

ไวร์เลสแอคเซสพอยท์มาตรฐาน IEEE 802.11b บนระบบปฏิบัติการลินุกซ์

Building a Wireless Access Point IEEE 802.11b on Linux

โดย

นาย สมเจต โพธิ์ทอง

รหัส 44067439



H002085

อาจารย์ที่ปรึกษา

ผศ.ดร. โชติพัทธ์ ภรณ์วลัย

| | |
|-------------------------------------|-----------------|
| วัน เดือน ปี..... | 26 ส.ค. 2550 |
| เลขทะเบียน..... | 02085 |
| เลขเรียกหนังสือ..... | วทว. ส236ว 2546 |
| "ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจธ." | |

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
ภาคเรียนที่ 2 ปีการศึกษา 2546
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

| | |
|------------------|--|
| ชื่อหัวข้อ | ไวร์เลสแอคเซสพอยท์มาตรฐาน IEEE 802.11b บนระบบปฏิบัติการลินุกซ์ |
| นักศึกษา | นาย สมเจ็ด โพธิ์ทอง |
| อาจารย์ที่ปรึกษา | ผศ.ดร. โชติพัชร ภรณ์วลัย |
| ระดับการศึกษา | วิทยาศาสตร์มหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ |
| แขนงวิชา | วิทยาการสารสนเทศ |
| ปีการศึกษา | 2546 |

บทคัดย่อ

ไวร์เลสแอคเซสพอยท์มาตรฐาน IEEE 802.11b บนระบบปฏิบัติการลินุกซ์ เป็นโอเพ่นซอร์สแวร์ไคร์เวอร์ HostAP ของการ์ดไวร์เลสชิป Intersil Prism2/2.5/3 ที่ใช้สำหรับติดตั้งลงในระบบปฏิบัติการลินุกซ์บนเครื่องคอมพิวเตอร์ที่ติดตั้งทั้งการ์ดไวร์เลสและการ์ดอีเทอร์เน็ตเมื่อติดตั้งซอร์สแวร์ไคร์เวอร์นี้แล้ว ระบบปฏิบัติการลินุกซ์จะสามารถทำงานเป็นไวร์เลสแอคเซสพอยท์ได้นั้นคือสามารถที่จะเชื่อมต่ออินเทอร์เน็ตทั้งสองเข้าด้วยกันและทำหน้าที่ส่งผ่านข้อมูลระหว่างอินเทอร์เน็ตได้ นอกจากนี้ยังมีระบบ การพิสูจน์ตัวตนจริง (Authentication) โดยใช้ NoCatAuth และโปรแกรมภาษา PHP โปรแกรมภาษา Perl ส่วนการจัดการฐานข้อมูลใช้โปรแกรม MySQL เว็บเซิร์ฟเวอร์ใช้โปรแกรม Apache Web Server เพื่อช่วย เพิ่มประสิทธิภาพให้กับการลงทะเบียนผ่านเว็บเบราว์เซอร์ที่แสดงผลเป็นภาษาไทย

| | |
|-----------------------|--|
| Title | Building a Wireless Access Point IEEE 802.11b on Linux |
| Student | Mr. Somjerd Pothong |
| Advisor | Asst.Prof.Dr. Chotipat Pornavalai |
| Level of Study | Master of Science in Information Technology |
| Major | Information Science |
| Academic Year | 2003 |

Abstract

Standard Wireless Access Point IEEE 802.11b on Linux Operation System is an Open Software Dirver HostAP of Intersil Prism 2/2.5/3 wireless chip card. It is setup on Linux Operation System of the compters which install both wireless card and Ethernet card. After being installed this software Dirver, Linux Operation System can work as Wireless Access Point ,i.e. it can connect two interfaces and transfer data between them. There is also the Authentication System run by NoCatAuth and PHP Programming Perl Programming. While Database System uses MySQL Web Server by Apache Web Server to increase efficiency of the registration on Web Browser that displays Thai language.

กิตติกรรมประกาศ

ผู้จัดทำโครงการได้รับความช่วยเหลือและสนับสนุนจากหลายฝ่ายในการศึกษาและพัฒนา
ระบบงาน ซึ่งถ้าไม่มีบุคคลเหล่านี้การศึกษาและพัฒนาระบบงานคงไม่สำเร็จลงได้ จึงใคร่
ขอขอบพระคุณ

ผศ.ดร. โชติพัชร ภรณวลัย ซึ่งเป็นอาจารย์ที่ปรึกษาโครงการ ที่ช่วยให้คำแนะนำในการ
จัดทำโครงการ ให้คำปรึกษาในด้านเนื้อหาที่เป็นประโยชน์

คุณสุจิน จันทร์หอมกุล ที่ให้คำปรึกษาเรื่องของระบบปฏิบัติการลินุกซ์

คุณสุรศักดิ์ สุขมาก ที่ให้คำแนะนำเรื่องโปรแกรมภาษา PHP และ PERL ที่กำลังศึกษา
ปริญญาโท คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คุณกาน มะลิหอม ที่ให้คำปรึกษาเรื่องของระบบเครือข่าย

ขอบคุณเพื่อนๆ ที่ให้คำแนะนำและกำลังใจที่ดีตลอดมา

สุดท้ายขอกราบขอบพระคุณ บิดา มารดา ผู้มีพระคุณสูงสุดที่ให้การสนับสนุนตลอด
ระยะเวลาที่ศึกษา

สมเจิด โพธิ์ทอง

สารบัญ

| | หน้า |
|--|------|
| บทคัดย่อภาษาไทย | I |
| บทคัดย่อภาษาอังกฤษ | II |
| กิตติกรรมประกาศ | III |
| สารบัญ | IV |
| สารบัญตาราง | VIII |
| สารบัญภาพ | IX |
| บทที่ | |
| 1.บทนำ | 1 |
| 1.1 ความเป็นมาของโครงการ | 1 |
| 1.2 วัตถุประสงค์ของการพัฒนาโครงการ | 1 |
| 1.3 ขอบเขตของการพัฒนาโครงการ | 1 |
| 1.4 ประโยชน์ที่คาดว่าจะได้รับ | 2 |
| 2.การพัฒนาระบบเครือข่ายไร้สาย | 3 |
| 2.1 ระบบเครือข่ายไร้สาย | 3 |
| 2.1.1 OSI Model (Open System Interconnection) | 3 |
| 2.1.2 บริคจ์ | 4 |
| 2.1.3 เราเตอร์ | 5 |
| 2.1.3 สนิฟเฟอร์ และการทำงานของสนิฟเฟอร์ | 5 |
| 2.1.4 มาตรฐานระบบเครือข่ายไร้สาย IEEE 802.11 | 6 |
| 2.1.5 มาตรฐาน IEEE 802.11b | 7 |
| 2.1.6 โครงสร้างการทำงานของระบบเครือข่ายไร้สาย | 8 |
| 2.1.7 รูปแบบการเชื่อมต่อของระบบเครือข่ายไร้สาย | 9 |
| 2.1.7.1 Peer-to-peer (ad hoc mode) | 11 |
| 2.1.7.2 Client/server (Infrastructure mode) | 11 |
| 2.1.7.3 Multiple access points and roaming | 12 |
| 2.1.7.4 Use of an Extension Point | 13 |

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

| | หน้า |
|---|-----------|
| 2.1.7.5 The Use of Directional Antennas | 13 |
| 2.1.8 เทคโนโลยีของระบบเครือข่ายไร้สาย (Wireless LANs Technology)..... | 14 |
| 2.1.8.1 Narrow Band Technology | 14 |
| 2.1.8.2 Spread Spectrum Technology..... | 14 |
| 2.1.8.3 Direct Sequence Spread Spectrum (DSSS) | 14 |
| 2.1.8.4 Frequency – Hopping Spread Spectrum (FHSS)..... | 15 |
| 2.1.8.5 Infrared Technology..... | 15 |
| 2.1.9 ระบบความปลอดภัยสำหรับมาตรฐาน IEEE 802.11..... | 17 |
| 2.1.9.1 Extended Service Set ID (ESSID)..... | 17 |
| 2.1.9.2 Access Lists | 17 |
| 2.1.9.3 Authentication and Association..... | 17 |
| 2.1.9.4 Wired Equivalent Privacy (WEP)..... | 19 |
| 2.1.10 คุณสมบัติของไวร์เลสแอสเซสพอยต์..... | 20 |
| 2.1.11 ประโยชน์ของระบบเครือข่ายไร้สาย..... | 23 |
| 3. การวิเคราะห์และออกแบบระบบ | 25 |
| 3.1 ปัญหาด้านความปลอดภัย..... | 25 |
| 3.2 การแก้ปัญหาด้านความปลอดภัย..... | 26 |
| 3.3 ขั้นตอนการทำงานระบบงานใหม่..... | 27 |
| 3.4 คอนเท็กซ์ไดอะแกรม ของระบบงานใหม่..... | 28 |
| 3.5 คาด้าโพลว์ ไดอะแกรม ของระบบงานใหม่..... | 29 |
| 3.3 การออกแบบฐานข้อมูลของระบบงาน..... | 30 |
| 4. การสร้าง ไวร์เลสแอสเซสพอยต์..... | 30 |
| 4.1 อุปกรณ์และเครื่องมือที่ต้องใช้..... | 33 |
| 4.1.1 ฮาร์ดแวร์..... | 33 |
| 4.1.2 เฟิร์มแวร์..... | 33 |
| 4.1.3 ซอฟต์แวร์..... | 34 |

สารบัญ (ต่อ)

หน้า

| | |
|---|-----------|
| 4.2 ขั้นตอนการอัปเดตเฟิร์มแวร์..... | 34 |
| 4.3 การติดตั้งซอฟต์แวร์ HostAP..... | 35 |
| 4.4 การติดตั้งซอฟต์แวร์ บริดจ์..... | 36 |
| 5.การพิสูจน์ตัวตนจริงและเกตเวย์..... | 41 |
| 5.1 อุปกรณ์และเครื่องมือที่ต้องใช้..... | 41 |
| 5.1.1 ซอฟต์แวร์..... | 41 |
| 5.1.2 ฮาร์ดแวร์..... | 42 |
| 5.2 ขั้นตอนการติดตั้ง..... | 42 |
| 5.2.1 การกำหนด DHCP ให้กับเครื่องลูกข่าย..... | 43 |
| 5.2.2 ขั้นตอนการติดตั้ง NoCatAuth..... | 43 |
| 5.2.3 ขั้นตอนการติดตั้งฐานข้อมูล MySQL..... | 45 |
| 5.2.4 ขั้นตอนการติดตั้ง iptables..... | 45 |
| 5.2.5 ขั้นตอนการติดตั้ง Apache กับ mod_ssl..... | 47 |
| 6. การพัฒนาระบบ..... | 48 |
| 6.1 ซอฟต์แวร์ที่ใช้ในส่วนของพัฒนาระบบ มีดังนี้..... | 48 |
| 6.2 การติดตั้งซอฟต์แวร์ Webmin..... | 48 |
| 6.3 โครงสร้างและพัฒนาระบบ..... | 50 |
| 6.3.1 ส่วนของผู้ดูแลระบบ Admin..... | 51 |
| 6.3.1 ส่วนของผู้ใช้ User..... | 51 |
| 7.ผลการทดลอง..... | 52 |
| 7.1 เริ่มต้นการใช้งานระบบ..... | 52 |
| 7.2 สรุปผลการทดลองการใช้งานระบบ..... | 63 |
| 8.สรุปผลการพัฒนาระบบงาน และข้อเสนอแนะ..... | 64 |
| 8.1 สรุปผลการพัฒนาระบบงาน..... | 64 |
| 8.2 ข้อเสนอแนะ..... | 64 |
| บรรณานุกรม..... | 65 |

สารบัญ (ต่อ)

| | หน้า |
|----------------------|------|
| ภาคผนวก..... | 68 |
| ประวัติผู้เขียน..... | 89 |



สารบัญตาราง

| ตารางที่ | | หน้า |
|----------|---|------|
| 2.1 | แสดงอัตราค่าส่งข้อมูลจำเพาะ ของ IEEE 802.11b..... | 8 |
| 3.1 | แสดงโครงสร้างและรายละเอียดของ Table Member..... | 31 |
| 3.2 | แสดงโครงสร้างและรายละเอียดของ Table Register..... | 32 |



สารบัญภาพ

| ภาพที่ | หน้า |
|---|------|
| 2.1 OSI Model..... | 3 |
| 2.2 แบบจำลองการทำงานของบริดจ์..... | 4 |
| 2.3 แบบจำลองการทำงานของเราเตอร์..... | 5 |
| 2.4 แสดงส่วนการทำงานของระบบเครือข่ายไร้สาย 802.11..... | 6 |
| 2.5 แสดงการเชื่อมต่อเป็นระบบเครือข่ายแบบชั่วคราว (Basic Service Set)..... | 10 |
| 2.6 แสดงการเชื่อมต่อกับระบบเครือข่ายเดิมโดยผ่านจุดเชื่อมต่อ (Extended Service Set)..... | 10 |
| 2.7 แสดงการทำงานแบบ Ac hoc mode..... | 11 |
| 2.8 แสดงการทำงานแบบ access point..... | 12 |
| 2.9 แสดงการทำงานแบบ Multiple access point and roaming..... | 12 |
| 2.10 แสดงการทำงาน แบบการใช้ Extension Point..... | 13 |
| 2.11 แสดงการทำงานแบบการใช้ Directional Antennas..... | 13 |
| 2.12 แสดงส่วนประกอบต่างๆ ในชั้นฟิสิกส์คอล..... | 16 |
| 2.13 แสดงระบบเปิด (Open System Authentication)..... | 18 |
| 2.14 แสดงระบบกุญแจร่วม (Shared Key Authentication)..... | 18 |
| 2.15 แสดงการทำงานของ Wired Equivalent Privacy (WEP)..... | 19 |
| 3.1 แสดงการทำงานระบบไวร์เลสแอสซอสายที่กับการพิสูจน์ตัวตนจริง..... | 26 |
| 3.2 แสดงการทำงานระบบใหม่..... | 28 |
| 3.3 แสดงคอนเท็กซ์ ไคอะแกรม ของระบบงานที่ออกแบบใหม่..... | 28 |
| 3.4 แสดงค่าตัวโพลว์ ไคอะแกรมของระบบงานใหม่..... | 29 |
| 3.5 แสดง E-R Diagram ของระบบงาน..... | 31 |
| 4.1 แสดงภาพ D-Link DWL-500..... | 33 |
| 4.2 แสดงภาพ WinUpdate-0-5-1-0..... | 34 |
| 4.3 แสดงภาพ แบบจำลองการทำงานของบริดจ์..... | 37 |
| 4.4 แสดงภาพ การทำงานของบริดจ์..... | 38 |
| 5.1 แสดงภาพ ของการทำงานระบบการพิสูจน์ตัวตนจริงกับเกตเวย์..... | 41 |
| 5.2 แสดงภาพ การกำหนด IP Address eth1 และ eth0..... | 42 |

สารบัญภาพ (ต่อ)

| ภาพที่ | หน้า |
|--------|---|
| 6.1 | แสดงหน้าจอล็อกอิน Webmin..... 49 |
| 6.2 | แสดงการติดตั้งโมดูล nocat-0.50.wbm และ nocat-0.51.wbm..... 49 |
| 6.3 | แสดงการทำงานและการพัฒนาระบบงาน..... 50 |
| 7.1 | แสดงภาพการทดสอบระบบไวร์เลสแอสเซมบลี..... 52 |
| 7.2 | แสดงหน้าจอเลือกตัวไวร์เลสแอสเซมบลี..... 53 |
| 7.3 | แสดงหน้าจอข้อความรายละเอียดโดยย่อในการเลือกตัวไวร์เลสแอสเซมบลี..... 53 |
| 7.4 | แสดงหน้าจอเครื่องลูกข่ายไวร์เลสแลนได้รับไอพี..... 54 |
| 7.5 | แสดงหน้าจอยืนยันการเข้ารหัส SSL เครื่องลูกข่ายไวร์เลสแลน..... 55 |
| 7.6 | แสดงหน้าจอล็อกอินเข้าสู่ระบบ..... 56 |
| 7.7 | แสดงหน้าจอลงทะเบียน..... 57 |
| 7.8 | แสดงหน้าจอลงทะเบียนเรียบร้อยแล้ว..... 57 |
| 7.9 | แสดงหน้าจอการล็อกอินของผู้ดูแลระบบ..... 58 |
| 7.10 | แสดงหน้าจอข้อมูลการลงทะเบียนของผู้ใช้เพื่อผู้ดูแลระบบทำการตรวจสอบ..... 59 |
| 7.11 | แสดงหน้าจอรหัสผู้ใช้งานที่ส่งมาทางอีเมลจากผู้ดูแลระบบ..... 60 |
| 7.12 | แสดงหน้าจอการเปลี่ยนรหัสผ่าน..... 60 |
| 7.13 | แสดงหน้าจอการล็อกอินเข้าใช้งานระบบ..... 61 |
| 7.14 | แสดงหน้าจอการล็อกอินเข้าใช้งานระบบผ่านแล้ว..... 61 |
| 7.15 | แสดงหน้าจอการใช้งานอินเทอร์เน็ตได้แล้ว..... 61 |
| 7.16 | แสดงหน้าจอการออกจากระบบ..... 63 |

บทที่ 1

บทนำ

1.1 ที่มาของโครงการ

เนื่องด้วยในยุคปัจจุบันนี้ เทคโนโลยีการสื่อสารแบบไร้สายได้เข้ามามีบทบาทในชีวิตประจำวันมากขึ้นเรื่อยๆ และเทคโนโลยีหนึ่งที่น่าจับตามองก็คือระบบเครือข่ายไร้สายเนื่องจากมีความสะดวกสบายในการใช้งานมากขึ้นและไม่ต้องคำนึงถึงข้อจำกัดทางด้านสถานที่ดังเช่นระบบเครือข่ายมีสายแบบเดิมแต่เนื่องจากผลิตภัณฑ์อุปกรณ์เครือข่ายแบบไร้สายนั้นมีข้อจำกัดคือเป็นระบบปิดซึ่งไม่อนุญาตให้บุคคลภายนอกเข้าไปปรับปรุงแก้ไขหรือแต่งเติมองค์ประกอบใดๆ ในผลิตภัณฑ์นั้นทั้งในด้านซอฟต์แวร์และฮาร์ดแวร์ นอกจากนี้ ซึ่งขาดความยืดหยุ่นในการรองรับการใช้งานที่ค่อนข้างหลากหลายในปัจจุบัน

ดังนั้น โครงการนี้จึงมุ่งเน้นในด้านการพัฒนาและออกแบบซอฟต์แวร์สำหรับการนำเครื่องคอมพิวเตอร์มาประยุกต์ให้สามารถทำงานแทนไวร์เลสแอ็คเซสพอยท์ได้ โดยการเชื่อมต่ออินเทอร์เน็ตทั้ง การ์ดไวร์เลสและการ์ดอีเทอร์เน็ตเข้ากับเครื่องคอมพิวเตอร์ โดยที่โปรแกรมจะทำหน้าที่ส่งผ่านข้อมูลระหว่างอินเทอร์เน็ตซึ่งโปรแกรมส่วนนี้จะถูกพัฒนามาให้ใช้งานสำหรับติดตั้งลงในระบบปฏิบัติการลินุกซ์ เนื่องจากมีความสะดวกต่อการติดตั้งและใช้งาน รวมถึงยังสามารถรองรับการพัฒนาในอนาคต

1.2 วัตถุประสงค์ของโครงการ

- เพื่อให้สามารถใช้งานระบบเครือข่ายไร้สายได้โดยใช้คอมพิวเตอร์ที่มีทรัพยากรไม่มากนักกับระบบปฏิบัติการลินุกซ์ให้ทำงานแทนไวร์เลสแอ็คเซสพอยท์
- เพื่อให้สามารถใช้งานระบบเครือข่ายไร้สายไวร์เลสแอ็คเซสพอยท์เชื่อมต่อกับระบบเครือข่ายอีเทอร์เน็ตและอินเทอร์เน็ตได้
- เพื่อให้สามารถใช้งานระบบการพิสูจน์ตัวตนจริง ในการลงทะเบียนขอรหัสผู้ใช้งานและรหัสผ่านด้วยเว็บเบราว์เซอร์ที่มีการเข้ารหัสรักษาความปลอดภัยได้

1.3 ขอบเขตของการพัฒนาโครงการ

เอกสารนี้เป็นเอกสารที่สร้างขึ้นเพื่อใช้ในการศึกษาเท่านั้น ไม่สามารถสร้างไวร์เลสแอ็คเซสพอยท์ บนระบบปฏิบัติการลินุกซ์ ด้วยซอฟต์แวร์ที่เขียนขึ้นด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- สามารถที่จะทำให้คอมพิวเตอร์ที่ติดตั้งอินเทอร์เน็ตเฟสทั้งการ์ด ไวร์เลสและการ์ดอีเทอร์เน็ต สามารถที่จะส่งผ่านข้อมูลระหว่างอินเทอร์เน็ตได้ในระดับชั้นเคทาถึงค์ให้สามารถใช้งานอินเทอร์เน็ตได้
- สามารถทำการพิสูจน์ตัวตนจริงของผู้ใช้งาน ผ่านเว็บเบราว์เซอร์ที่มีความปลอดภัยได้
- ผู้ดูแลระบบหรือเจ้าหน้าที่สามารถจัดการรหัสผู้ใช้งานผ่านเว็บเบราว์เซอร์ที่มีปลอดภัยได้
- ผู้ดูแลระบบสามารถทำการตรวจสอบอนุญาตให้ใช้งาน โดยทำการส่งรหัสผ่านทางอีเมล
- โปรแกรมจะได้รับการพัฒนา สามารถติดตั้งลงในระบบปฏิบัติการลินุกซ์ได้

1.4 ประโยชน์ที่คาดว่าจะได้รับ

สามารถนำระบบนี้ไปใช้งานได้จริงในปัจจุบัน ในคณะเทคโนโลยีสารสนเทศ เพื่อช่วยเพิ่มประสิทธิภาพการทำงานของระบบไวร์เลสแลน ให้สามารถทำการพิสูจน์ตัวตนจริงด้วยการรหัสผู้ใช้นักศึกษาและรหัสผ่านในการใช้งานอินเทอร์เน็ต

บทที่ 2

การพัฒนาระบบเครือข่ายไร้สาย

2.1 ระบบเครือข่ายไร้สาย

2.1.1 OSI Model (Open System Interconnection)

OSI Model คือ โมเดลอ้างอิงหนึ่งของ ISO (International Standard Organization) ที่ถูกออกแบบขึ้นเพื่อกำหนดรูปแบบการสื่อสารระหว่างคอมพิวเตอร์ในระบบเครือข่ายเป็นไปได้อย่างราบรื่นไม่ว่าจะมีสถาปัตยกรรมแบบเดียวกันหรือไม่ก็ตาม โดยที่ OSI Model จะถูกแบ่งส่วนการทำงานออกเป็นระดับชั้น (Layer) ดังรูปที่ 2.1



รูปที่ 2.1 OSI Model

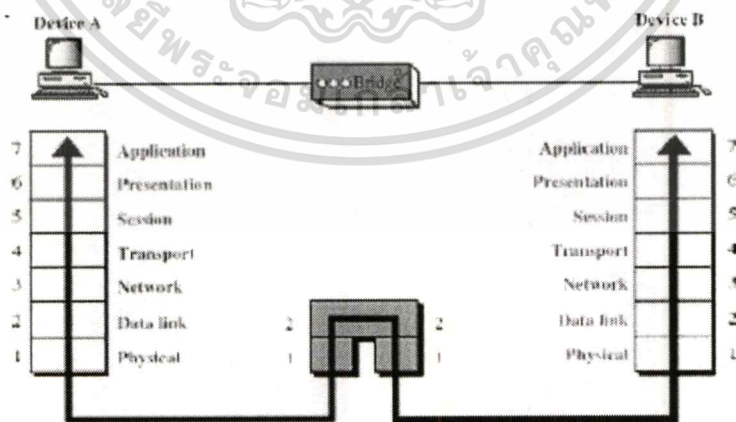
ในแต่ละชั้นของ OSI Model จะทำการติดต่อและส่งผ่านข้อมูลระหว่างชั้นที่อยู่ติดกันเท่านั้น โดยที่แต่ละชั้นก็ได้มีหน้าที่รับผิดชอบต่าง ๆ กันเพื่อให้เกิดการทำงานที่เป็นระบบและมีประสิทธิภาพ โดยที่รายละเอียดของแต่ละระดับชั้นมีดังนี้

- Physical Layer ทำหน้าที่จัดการกับข้อมูลในระดับบิต เป็นชั้นล่างสุดของ OSI Model โดยจะทำงานเกี่ยวกับ Media , Interface และ Hardware ที่ใช้ในการติดต่อกับระบบเครือข่าย

- Data Link Layer ทำหน้าที่จัดการกับข้อมูลในระดับเฟรม (Frame) โดยจะระบุเครื่องที่เป็นผู้รับและผู้ส่งข้อมูลโดยใช้ MAC Address ซึ่งจะเป็นการรับผิดชอบการส่งข้อมูลภายในเครือข่ายเท่านั้น นอกจากนี้จะยังควบคุมเกี่ยวกับอัตราการส่งข้อมูล (flow control) การควบคุมความผิดพลาด (error control) อีกด้วย
- Network Layer ทำหน้าที่เชื่อมต่อระหว่างเครือข่ายโดยใช้ IP Address นั่นคือหน้าที่หลักของระดับชั้นนี้จะเป็นการรับผิดชอบการส่งผ่านข้อมูลข้ามเครือข่ายในระดับแพ็คเกจ (packet) โดยมีการหาเส้นทาง (routing) เพื่อส่งข้อมูลไปยังเครือข่ายปลายทางเป็นหน้าที่สำคัญ
- Transport Layer รับผิดชอบการรับส่งข้อมูลระหว่างผู้รับและผู้ส่ง (end to end)
- Session Layer ควบคุมจังหวะ Start Stop ตลอดจนการ Synchronize ในขณะที่สื่อสาร
- Presentation Layer รับผิดชอบเกี่ยวกับการแปลความหมายของข้อมูล การบีบอัดข้อมูล ตลอดจนการเข้ารหัสข้อมูล
- Application Layer เป็นระดับชั้นที่จะทำการติดต่อกับผู้ใช้

2.1.2 บริดจ์

บริดจ์ (bridge) เป็นอุปกรณ์เครือข่ายที่ทำหน้าที่เชื่อมเครือข่ายย่อยสองเครือข่ายเข้าด้วยกัน บริดจ์จะทำงานในระดับชั้นเดทาลิงก์ จึงสามารถเชื่อมเครือข่ายประเภทเดียวกันหรือต่างกันเข้าด้วยกันได้ แบบจำลองการทำงานของบริดจ์จะแสดงได้ดังรูปที่ 2.2



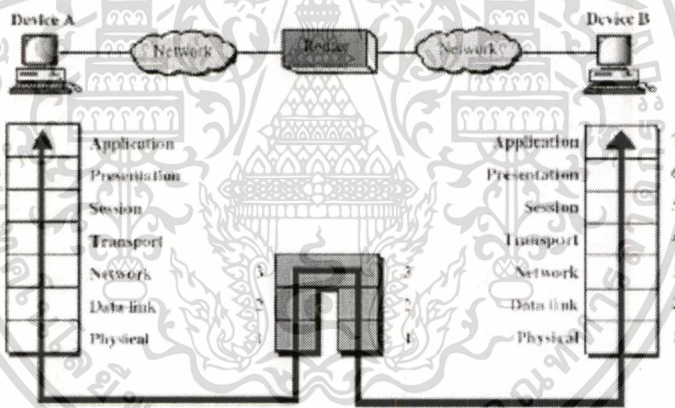
รูปที่ 2.2 แบบจำลองการทำงานของบริดจ์

ที่ระดับชั้นเดทาลิงก์ การทำงานของชั้นนี้จะรับข้อมูลที่ส่งลงมาจากระดับชั้นเน็ตเวิร์ก แล้วทำการเพิ่ม Header ของตัวเองเข้าไปก่อนที่จะส่งลงไปให้ระดับชั้นฟิสิคัลเพื่อส่งออกไปทางไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งยังมีให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การ์ดเน็ตเวิร์ก เมื่อข้อมูลถูกส่งไปถึงบริดจ์ บริดจ์จะทำงานที่ระดับชั้นเคทาลิงค์ นั่นคือจะส่งผ่านข้อมูลจากชั้นล่างสุดขึ้นไปเรื่อยๆ พร้อมกับทำการถอด Header ของแต่ละชั้นไปด้วย (Decapsulate) จนถึงระดับชั้นเคทาลิงค์ แล้วจึงตรวจสอบว่า MAC Address ของเครือข่ายปลายทางที่ระบุมาในเฟรมนั้นใช่เครือข่ายที่อยู่อีกอินเทอร์เฟซหนึ่งหรือไม่ ถ้าใช่ ก็จะทำการ Encapsulate ใหม่อีกครั้งด้วยสภาพแวดล้อมของเครือข่ายปลายทาง แล้วจึงส่งข้อมูลไปยังเครือข่ายปลายทาง

2.1.3 เราเตอร์

เราเตอร์ (Router) เป็นอุปกรณ์ที่ทำงานในระดับชั้นเน็ตเวิร์ก หน้าที่หลักของเราเตอร์คือจัดแบ่งเครือข่ายออกเป็นกลุ่มและเลือกเส้นทางที่เหมาะสมเพื่อนำส่ง Packet เราเตอร์จะประกอบด้วยหลายอินเทอร์เฟซเพื่อเชื่อมต่อเข้ากับเครือข่ายต่างชนิดเข้าด้วยกันได้ การทำงานของเราเตอร์จะพิจารณาที่ IP Address เป็นหลัก แบบจำลองการทำงานของเราเตอร์เทียบกับ OSI Model จะแสดงได้ดังรูปที่ 2.3



รูปที่ 2.3 แบบจำลองการทำงานของเราเตอร์

2.1.3 สนิฟเฟอร์ และการทำงานของสนิฟเฟอร์

การทำงานของอีเทอร์เน็ตการ์ดตามปกติแล้ว เมื่อการ์ดได้รับแพ็กเก็ตส่งเข้ามาตามสายสัญญาณ สิ่งที่การ์ดจะต้องทำทุกครั้งก็คือการตรวจสอบว่า ข้อมูลที่ส่งเข้ามานั้นเป็นข้อมูลของตัวเองหรือเปล่าโดยตรวจสอบจาก MAC Address ถ้าหากใช่ข้อมูลของเครื่องตัวเองก็จะเก็บข้อมูลนั้นไว้ แล้วจึงส่งให้กับ Layer ถัดไปทำงานตามปกติ หากไม่ใช่ข้อมูลของเครื่องตัวเองก็จะทิ้งข้อมูลนั้นไปเสีย

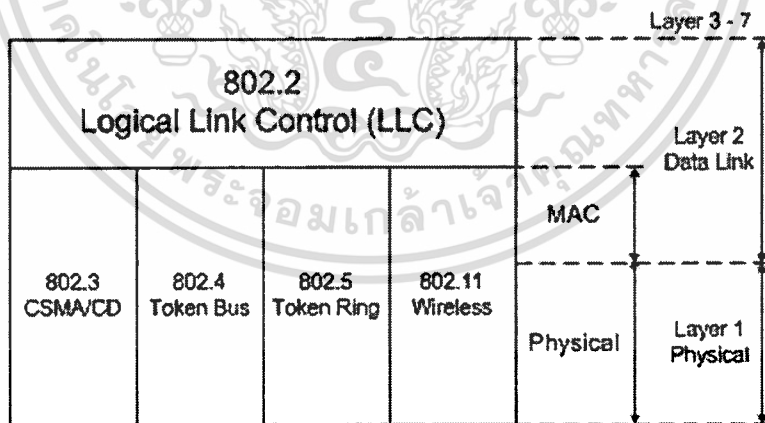
แต่ยังมีโปรแกรมอีกชนิดหนึ่งเรียกกันว่า สนิฟเฟอร์ (Sniffer) เป็นโปรแกรมที่จะจัดการให้เน็ตเวิร์กการ์ดไม่ทำการทิ้งเฟรมที่ไม่ใช่ของเครื่องตัวเอง แต่จะส่งข้อมูลขึ้นมาอย่างชั้นถัดๆ ไป โดยไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ที่ตัวสวิตช์เองจะเป็นโปรแกรมที่คอยทำงานในระดับชั้นแอปพลิเคชัน แล้วทำการแสดงข้อมูลนั้นให้กับผู้ใช้ สวิตช์เองจะมีประโยชน์มากสำหรับผู้ดูแลรักษาเครือข่ายหรือผู้ที่ต้องการที่จะศึกษาการส่งผ่านข้อมูลในระบบเครือข่าย แต่ในขณะเดียวกันก็ยังเป็นช่องทางสำหรับผู้ต้องการขโมยข้อมูลที่ไม่ใช่ของตัวเองอีกด้วย

การทำงานของสวิตช์ขั้นตอนแรกคือ ทำการเซตเน็ตเวิร์กการ์ดให้อยู่ในรูป Promiscuous mode เสียก่อน เพื่อไม่ให้เน็ตเวิร์กการ์ดทิ้งเฟรมที่ไม่ใช่ของตัวเองทิ้งไป

2.1.4 มาตรฐานระบบเครือข่ายไร้สาย IEEE 802.11

มาตรฐาน IEEE 802.11 เป็นมาตรฐานที่ใช้สำหรับการสื่อสารในระบบเครือข่ายไร้สาย มาตรฐาน IEEE 802.11 นี้จะทำงานในช่วงความถี่ระหว่าง 2.4 – 2.5 GHz ช่วงความถี่นี้เป็นช่วงความถี่อิสระที่สามารถใช้งานได้โดยไม่จำเป็นต้องจดทะเบียน มาตรฐาน IEEE 802.11 พัฒนามาจากการสื่อสารระบบเครือข่ายตามมาตรฐาน 802.3 ซึ่งเป็นมาตรฐานของการเชื่อมต่อเครือข่ายแบบใช้สายที่รู้จักกันในชื่อ อีเทอร์เน็ต โพรโตคอลที่มาตรฐาน IEEE 802.3 ใช้ในการสื่อสารคือ CSMA/CD (Carrier Sense Multiple Access / Collision Detection) ส่วนมาตรฐาน IEEE 802.11 ที่ได้พัฒนามาจาก IEEE 802.3 จะใช้โพรโตคอล CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) มาตรฐาน 802.11 มีการทำงานอยู่ในส่วนของ MAC layer และ Physical layer ดังแสดงในรูปที่ 2.4



รูปที่ 2.4 แสดงส่วนการทำงานของระบบเครือข่ายไร้สาย 802.11

มาตรฐาน IEEE 802.11 เหมือนกับมาตรฐาน IEEE 802.3 Ethernet ซึ่งใช้กับเครือข่าย LAN แบบใช้สาย และ IEEE 802.5 สำหรับเครือข่าย Token Ring ตรงที่ มาตรฐาน IEEE 802.11 จะมุ่งความสนใจไปที่ระดับล่างสุดสองระดับของ ISO model (คือ physical layer และ data link layer) เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่นิยมนำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ซึ่งจะทำให้ application, network OS, protocol, รวมทั้ง TCP/IP ใดๆก็ตามสามารถใช้งานบน 802.11 compliant ไร้สายได้เช่นเดียวกับใช้งานบน Ethernet โดยทั่วไป

มาตรฐาน 802.11 นี้ใช้การส่งสัญญาณแบบคลื่นวิทยุที่ความถี่ 2.4 GHz ซึ่งเป็นความถี่ ISM (Industrial, Scientific and Medical) band สามารถส่งข้อมูลได้ด้วยอัตราความเร็ว ก่อนข้างต่ำ คือ 1 และ 2 Mbps เท่านั้น โดยใช้เทคนิคการส่งสัญญาณหลักอยู่ 2 รูปแบบ คือ DSSS (Direct Sequence Spread Spectrum) และ FHSS (Frequency Hopping Spread Spectrum) ซึ่งถูกคิดค้นมาจากหน่วยงานทหาร การส่งสัญญาณทั้ง 2 รูปแบบจะใช้เวลาของช่องสัญญาณ (bandwidth) ที่มากกว่า การส่งสัญญาณแบบ narrow band แต่ทำให้สัญญาณมีความแรงมากกว่าซึ่งง่ายต่อการตรวจจับมากกว่า แบบ narrow band หน่วยงานทหารใช้วิธีการเหล่านี้ในการปิดกั้นการใช้งานจากอุปกรณ์อื่นๆที่จะมาทำให้ระบบเกิดปัญหา โดยการส่งสัญญาณแบบ FHSS สัญญาณจะกระโดดจากความถี่หนึ่งไปยังอีกความถี่หนึ่งในอัตราที่ได้กำหนดไว้แล้ว ซึ่งจะรู้กันเฉพาะตัวรับกับตัวส่งเท่านั้น ส่วนการส่งสัญญาณแบบ DSSS จะมีการส่ง chipping code ไปกับสัญญาณแต่ละครั้งด้วย ซึ่งจะมีเฉพาะตัวรับกับตัวส่งเท่านั้นที่จะรู้ลำดับของ chip สำหรับการใช้งานระบบเครือข่ายแบบไร้สายทุกวันนี้ DSSS มีคุณสมบัติที่โดดเด่นและให้ throughput ที่มากกว่า เมื่อเร็วๆนี้เองที่ได้มีการพัฒนาจนได้อัตราการส่งข้อมูล 11 Mbps ผ่านการส่งแบบ DSSS และเป็นมาตรฐานที่โดดเด่นของไร้สายแลนผลิตภัณฑ์ซึ่งรองรับมาตรฐาน 802.11b (อัตราส่งถ่ายข้อมูลสูง 11 Mbps) นี้สามารถทำงานร่วมกับผลิตภัณฑ์ซึ่งทำงานกับมาตรฐาน DSSS แบบเก่า 802.11 (อัตราส่งถ่ายข้อมูล 1 และ 2 Mbps) ได้ แต่ ระบบ FHSS จะถูกใช้กับอุปกรณ์ที่มีกำลังส่งต่ำ, เป็น application ที่ใช้งานในย่านต่ำๆ เช่น โทรศัพท์ไร้สายความถี่ 2.4 GHz แต่จะใช้งานร่วมกับผลิตภัณฑ์ DSSS ไม่ได้

2.1.5 มาตรฐาน IEEE 802.11b

มาตรฐาน IEEE 802.11b ซึ่งเป็นมาตรฐานระบบเครือข่ายไร้สายที่ได้รับการยอมรับมากที่สุดในโลก เพราะมีการเปิดตัวก่อนมาตรฐานอื่นและมีผลิตภัณฑ์ออกวางจำหน่ายแล้วมากและแพร่หลายที่สุด

มาตรฐาน IEEE 802.11b นั้นล่าสุดได้รับการตั้งชื่อใหม่ว่า Wi-Fi โดยได้รับการรับรองมาตรฐานและกำหนดรายละเอียดโดยกลุ่ม WECA หรือ wireless Ethernet Compatibility Alliance ที่ประกอบด้วยสมาชิกจากผู้ผลิตในอุตสาหกรรมคอมพิวเตอร์ชื่อดังอย่าง 3com, Cisco Systems, Intersil, Agere Systems, Nokia และ Symbol Technologies ซึ่งปัจจุบันก็ยังมีสมาชิกจากบริษัทต่างๆ อีกกว่า 110 บริษัทเข้าร่วมอยู่ในมาตรฐานนี้

สำหรับรายละเอียดด้านคุณสมบัติ ของ IEEE 802.11b จะสามารถรับ-ส่งข้อมูลได้ด้วยความเร็วสูงสุดที่ 11 Mbps โดยใช้ความถี่คลื่นวิทยุที่ 2.4 GHz ใช้เทคนิคการส่งสัญญาณแบบ DSSS

เอกสาร...
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โดยย่านความถี่ที่ใช้เป็น ISM (Industrial, Scientific and Medical) band จากระดับความเร็วที่ค่อนข้างต่ำ คือทำได้เพียง 11 Mbps เท่านั้น เมื่อเทียบกับ ระบบแลน แบบมีสาย ที่มาตรฐานปัจจุบันอยู่ที่ระดับ 100 Mbps และล่าสุดมาตรฐานความเร็ว 1 Gbps กำลังเป็นที่ยอมรับและนิยมใช้งานมากขึ้นเรื่อย ๆ ก็จะเห็นว่า IEEE 802.11b นั้นค่อนข้างช้ากว่ามาก ไม่เพียงเท่านั้น คลื่นความถี่วิทยุที่ 2.4 GHz ที่ IEEE 802.11b ใช้อยู่นั้นยังมีอุปกรณ์อื่นๆ ร่วมใช้งานอยู่ด้วยหลายชนิด เช่น เตาไมโครเวฟ หรือ โทรศัพท์มือถือ ซึ่งหากมีอุปกรณ์เหล่านี้ทำงานอยู่ใกล้ๆ กับเครือข่าย IEEE 802.11b ก็จะทำให้ความเร็วในการรับส่งข้อมูลช้าลง แต่จุดเด่นก็คือการใช้ความถี่คลื่นวิทยุที่ค่อนข้างต่ำ เพียง 2.4 GHz นั้นทำให้ IEEE 802.11b มีระยะทางในการติดต่อระหว่างอุปกรณ์ค่อนข้างไกล ทำให้ชุดเครือข่ายไร้สายแบบ IEEE 802.11b ไม่จำเป็นต้องมีจุด รับส่งสัญญาณ หรือที่เรียกกันว่า Access Point หรือ นะ Hot Spot มากนัก ซึ่งช่วยประหยัดค่าใช้จ่ายได้ดี

ตารางที่ 2.1 แสดงอัตราการส่งข้อมูลจำเพาะ ของ IEEE 802.11b

| Data Rate (Mbps) อัตราการส่งข้อมูล | Code Length ความยาวของรหัส ลำดับของบาร์เกอร์ | Modulation ชนิดของ การมอดูเลต | Symbol Rate (Mbps) อัตรา Symbol | Bits/Symbol |
|---------------------------------------|--|-------------------------------------|---------------------------------------|-------------|
| 1 | 11 (Barker sequence) ลำดับของบาร์เกอร์ | BPSK | 1 | 1 |
| 2 | 11 (Barker sequence) ลำดับของ บาร์เกอร์ | QPSK | 1 | 2 |
| 5.5 | 8(CCK) | QPSK | 1.375 | 4 |
| 11 | 8(CCK) | QPSK | 1.375 | 8 |

2.1.6 โครงสร้างการทำงานของระบบเครือข่ายไร้สาย

ในระบบเครือข่ายไร้สาย IEEE 802.11 นั้นจะแบ่งระดับชั้นของเทคโนโลยีออกเป็นสี่ระดับ นั่นคือ ชั้นกายภาพ (Physical Layer) ตัวควบคุมการเข้าถึงสื่อ (Media Access Controller) ระบบปฏิบัติการ (Operating System) และแอปพลิเคชัน (Application) โดยชั้นกายภาพคือ ส่วนของฮาร์ดแวร์ที่แบ่งมาตรฐานออกเป็น a, b และ g โดยหากเลือกต่างชนิดกันก็ไม่สามารถสื่อสารกัน

ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ได้รู้เรื่อง เพราะเป็นความถี่ที่ต่างกันจะติดต่อบ้างส่งข้อมูลกันไม่ได้ โดยปัจจุบันในส่วนของชั้นกายภาพนี้มีอยู่ทั้งสิ้น สี่ มาตรฐาน คือ a, b, g และอินฟราเรด (IR)

ส่วนต่อมาคือ ตัวควบคุมการเข้าถึงสื่อเป็นส่วนของการทำงานเกี่ยวกับระบบรักษาความปลอดภัยของเครือข่าย การจัดการ โครงสร้างหรือรูปแบบของข้อมูล การแปลงข้อมูล ซึ่งมาตรฐาน IEEE 802.11 นั้นใช้มาตรฐานตัวควบคุมการเข้าถึงสื่อเดียวกันทั้งหมด คือ ได้กำหนดทางเลือกของการเข้ารหัสไว้ก่อนทำการส่งข้อมูล โดยใช้อัลกอริธึมการเข้ารหัสแบบ 40 บิตซึ่งรู้จักกันในชื่อ RC4 นอกจากนี้ผู้ผลิตบางรายก็ยังเสนอให้มีการตรวจสอบก่อนใช้งาน โครงข่ายด้วยวิธีการที่เรียกว่า Wired Equivalent Privacy (WEP) shared-key อันเดียวกันจะใช้ในการตรวจสอบก่อนที่จะทำการเข้ารหัสหรือถอดรหัสข้อมูล ซึ่งจะมีเพียงผู้ใช้งานที่ถูกตั้งเท่านั้นจึงจะมี shared-key ที่ถูกต้องในการถอดรหัสข้อมูลออกมาได้ นอกจากนี้เรื่องความน่าเชื่อถือกับเรื่องความปลอดภัยแล้ว มาตรฐาน 802.11 ในส่วนตัวควบคุมการเข้าถึงสื่อยังมีโหมดสนับสนุนการจัดการพลังงานอีก สอง รูปแบบ คือ Continuous Aware Mode และ Power Saving Polling Mode โดยโหมดแรกสัญญาณวิทยุจะส่งอยู่ตลอดและทำให้สูญเสียพลังงาน ในขณะที่โหมดต่อมาสัญญาณวิทยุจะอยู่ในสถานะนอนหลับหรือ sleep เพื่อที่จะลดการสิ้นเปลืองพลังงาน

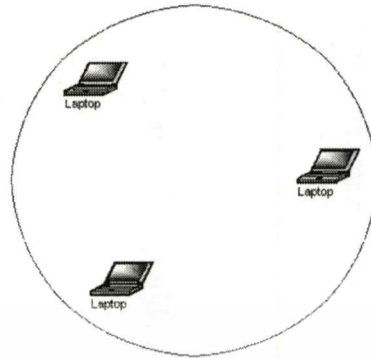
ส่วนของระบบปฏิบัติการและแอปพลิเคชันคือ ระบบปฏิบัติการภายในเครื่องและแอปพลิเคชันควบคุมการสื่อสาร ซึ่งใช้งานเหมือนกับเครือข่ายแบบมีสายในปัจจุบัน

2.1.7 รูปแบบการเชื่อมต่อของระบบเครือข่ายไร้สาย

รูปแบบการเชื่อมต่อของมาตรฐาน 802.11 สามารถทำได้สองรูปแบบ คือ

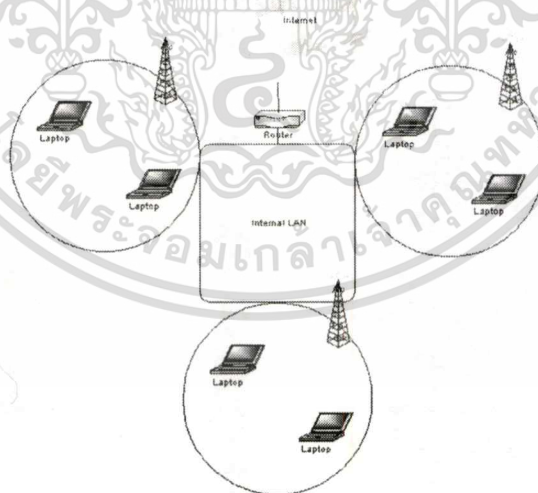
- การเชื่อมต่อเป็นระบบเครือข่ายแบบชั่วคราว (Basic Service Set)
- การเชื่อมต่อกับระบบเครือข่ายเดิมโดยผ่านจุดเชื่อมต่อ (Extended Service Set)

ในการเชื่อมต่อเป็นระบบเครือข่ายแบบชั่วคราวหรือที่เรียกว่าการเชื่อมต่อแบบ Ad hoc นั้นสามารถทำได้โดยการสร้างวงเครือข่ายโดยวิธีการติดต่อกันโดยตรงระหว่างเครื่องที่ต้องการสื่อสารกันในวงเครือข่ายชั่วคราวนั้นๆ เหมาะสำหรับการนำไปใช้ในการสร้างระบบเครือข่ายแบบชั่วคราว มีรูปแบบในการเชื่อมต่อแสดงได้ดังรูปที่ 2.5



รูปที่ 2.5 แสดงการเชื่อมต่อเป็นระบบเครือข่ายแบบชั่วคราว (Basic Service Set)

การเชื่อมต่อกับระบบเครือข่ายเดิมนั้นจะต้องใช้อุปกรณ์จุดเชื่อมต่อ (Access Point) เพื่อทำหน้าที่เป็นตัวเชื่อมต่อระบบส่วนที่เป็นการเชื่อมต่อแบบไร้สายเข้ากับเครือข่ายเดิม โดยจุดที่เชื่อมต่อนี้จะเป็นเสมือนช่องทางที่ใช้ในการสื่อสารระหว่างส่วนที่เป็นการสื่อสารแบบไร้สายกับส่วนที่เป็นการสื่อสารโดยใช้สาย มีรูปแบบการเชื่อมต่อดังแสดงในรูปที่ 2.6



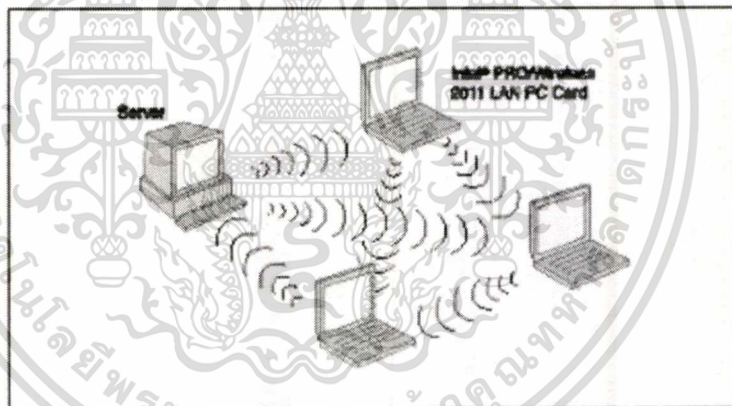
รูปที่ 2.6 แสดงการเชื่อมต่อกับระบบเครือข่ายเดิมโดยผ่านจุดเชื่อมต่อ (Extended Service Set)

ระบบเครือข่ายไร้สาย เป็นระบบเครือข่ายคอมพิวเตอร์ขนาดเล็ก ที่ประกอบไปด้วยอุปกรณ์
 ไม่นานนัก และมักจำกัดอยู่ในอาคารหลังเดียวหรืออาคารในบริเวณเดียวกัน การใช้งานที่น่าสนใจ
 เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้ในเพื่อการศึกษเท่านั้น เมื่อผู้เอาไปใช้ประโยชน์ในการค้า
 ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ที่สุดของเครือข่ายไร้สายก็คือ ความสะดวกสบายที่ไม่ต้องติดอยู่กับที่ ผู้ใช้สามารถเคลื่อนที่ไปมาได้ โดยที่ยังสื่อสารอยู่ในระบบเครือข่าย โดยรูปแบบการเชื่อมต่อของระบบเครือข่ายไร้สายทั้งสองแบบที่กล่าวมาข้างต้นสามารถแบ่งได้เป็น 5 แบบดังนี้

2.1.7.1 Peer-to-peer (ad hoc mode)

รูปแบบการเชื่อมต่อระบบแลนไร้สายแบบ Peer to Peer เป็นลักษณะ การเชื่อมต่อแบบ โครงข่ายโดยตรงระหว่างเครื่องคอมพิวเตอร์ จำนวนสอง เครื่องหรือมากกว่านั้น เป็นการใช้งาน ร่วมกันของ การ์ด ไร้เลสแลน โดยไม่ได้มีการเชื่อมต่อกับเครือข่ายแบบใช้สายเลย โดยที่เครื่อง คอมพิวเตอร์แต่ละเครื่องจะมีความเท่าเทียมกัน สามารถทำงานของตนเองได้และขอใช้บริการ เครื่องอื่นได้ เหมาะสำหรับการนำมาใช้งานเพื่อจุดประสงค์ในด้านความรวดเร็วหรือติดตั้งได้ โดยง่ายเมื่อไม่มีโครงสร้างพื้นฐานที่จะรองรับ ยกตัวอย่างเช่น ในศูนย์ประชุม หรือการประชุมที่จัด ขึ้นนอกสถานที่

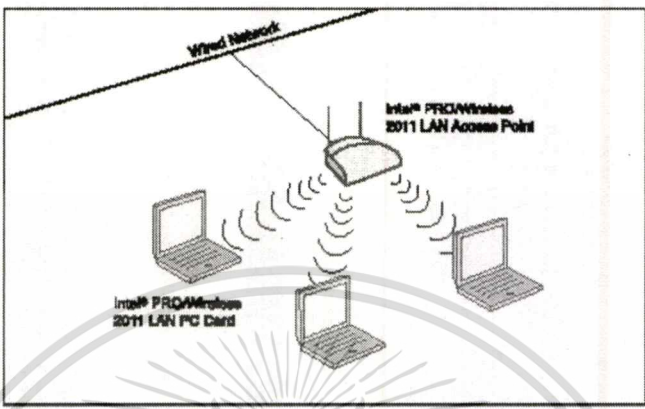


รูปที่ 2.7 แสดงการทำงานแบบ Ac hoc mode

2.1.7.2 Client/server (Infrastructure mode)

ระบบเครือข่ายไร้สายแบบ Client / server หรือ Infrastructure mode เป็นลักษณะการรับส่ง ข้อมูลโดยอาศัย Access Point (AP) หรือเรียกว่า Hot spot ทำหน้าที่เป็นสะพานเชื่อมต่อระหว่าง ระบบเครือข่ายแบบใช้สายกับเครื่องคอมพิวเตอร์ลูกข่าย (client) โดยจะกระจายสัญญาณคลื่นวิทยุ เพื่อ รับ-ส่งข้อมูลเป็นรัศมีโดยรอบ เครื่องคอมพิวเตอร์ที่อยู่ในรัศมีของ AP จะกลายเป็น เครือข่าย กลุ่มเดียวกันทันที โดยเครื่องคอมพิวเตอร์ จะสามารถติดต่อกัน หรือติดต่อกับ Server เพื่อ แลกเปลี่ยนและค้นหาข้อมูลได้ โดยต้องติดต่อผ่าน AP เท่านั้น ซึ่ง AP 1 จุด สามารถให้บริการเครื่อง ลูกข่ายได้ถึง 15-50 อุปกรณ์ ของเครื่องลูกข่าย เหมาะสำหรับการนำไปขยายเครือข่ายหรือใช้ร่วมกับ ไม่ว่างกรณีใดทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

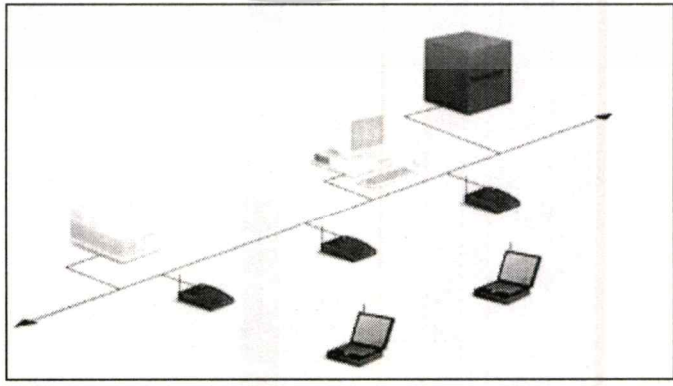
ระบบเครือข่ายแบบใช้สายเดิมในออฟฟิศ, ห้องสมุด หรือในห้องประชุม เพื่อเพิ่มประสิทธิภาพในการทำงานให้มากขึ้น



รูปที่ 2.8 แสดงการทำงานแบบ access point

2.1.7.3 Multiple access points and roaming

โดยทั่วไปแล้ว การเชื่อมต่อสัญญาณระหว่างเครื่องคอมพิวเตอร์ กับ Access Point ของเครือข่ายไร้สายจะอยู่ในรัศมีประมาณ 500 ฟุต ภายในอาคาร และ 1000 ฟุต ภายนอกอาคาร หากสถานที่ที่ติดตั้งมีขนาดกว้าง มากๆ เช่นคลังสินค้า บริเวณภายในมหาวิทยาลัย สนามบิน จะต้องมีการเพิ่มจุดการติดตั้ง AP ให้มากขึ้น เพื่อให้การรับส่งสัญญาณในบริเวณของเครือข่ายขนาดใหญ่ เป็นไปอย่างครอบคลุมทั่วถึง

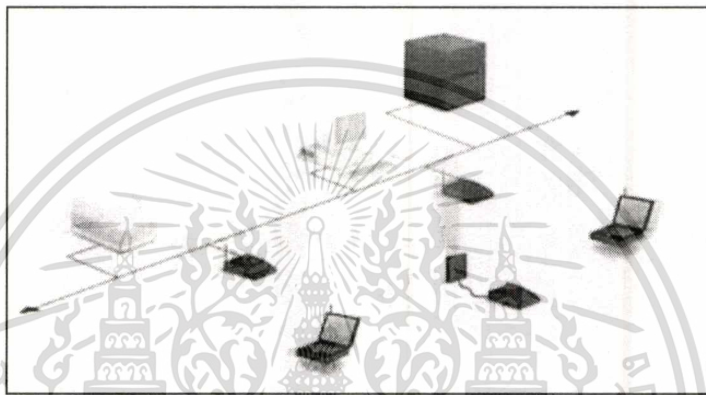


รูปที่ 2.9 แสดงการทำงานแบบ Multiple access point and roaming

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับเอาไว้ใช้เพื่อการศึกษาเท่านั้น ไปจนกระทั่งให้ไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.7.4 Use of an Extension Point

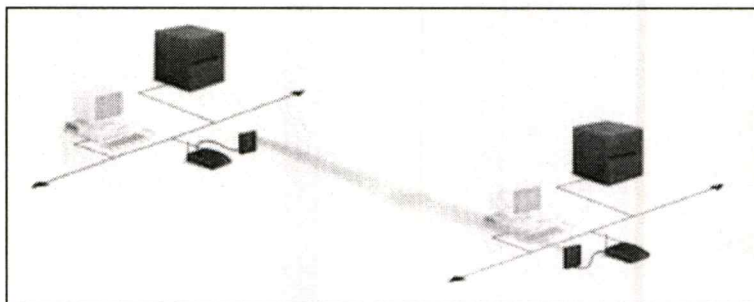
กรณีทีโครงสร้างของสถานที่ติดตั้งเครือข่ายแบบไร้สายมีปัญหาผู้ออกแบบระบบอาจจะใช้ Extension Points ที่มีคุณสมบัติเหมือนกับ Access Point แต่ไม่ต้องผูกติดไว้กับเครือข่ายไร้สาย เป็นส่วนที่ใช้เพิ่มเติมในการรับส่งสัญญาณ



รูปที่ 2.10 แสดงการทำงาน แบบการใช้ Extension Point

2.1.7.5 The Use of Directional Antennas

ระบบแลนไร้สายแบบนี้เป็นแบบใช้เสาอากาศในการรับส่งสัญญาณระหว่างอาคารที่อยู่ห่างกัน โดยการติดตั้งเสาอากาศที่แต่ละอาคาร เพื่อส่งและรับสัญญาณระหว่างกัน



รูปที่ 2.11 แสดงการทำงานแบบการใช้ Directional Antennas

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.8 เทคโนโลยีของระบบเครือข่ายไร้สาย (Wireless LANs Technology)

โดยทั่วไปแล้วระบบเครือข่ายไร้สายจะใช้เทคโนโลยีในการส่งสัญญาณอยู่ สอง ประเภท คือ ประเภทที่ใช้สัญญาณคลื่นความถี่วิทยุซึ่งแบ่งเป็น สอง แบบ คือ Narrow Band และ Spread Spectrum และประเภทที่ใช้สัญญาณอินฟราเรดในการติดต่อรับ - ส่งข้อมูล โดยมีรายละเอียดดังต่อไปนี้

2.1.8.1 Narrow Band Technology

ระบบวิทยุแบบความถี่แคบ เป็นการรับ - ส่งสัญญาณคลื่นวิทยุบนความถี่เฉพาะ โดยคลื่นความถี่ดังกล่าว เป็นที่รู้จักในชื่อของแถบความถี่ ISM (Industrial Scientific / Medical) ที่มีความถี่แบ่งเป็น สาม ช่วง ได้แก่ 902 MHz ถึง 928 MHz, 2.4 MHz ถึง 2.484 และ 5.725 MHz ถึง 5.850 MHz สัญญาณจะมีกำลังต่ำ (โดยทั่วไปประมาณ 1 มิลลิวัตต์) และใช้ในการรับ-ส่งข้อมูลระหว่างต้นทางกับปลายทางเพียง 1 คู่เท่านั้น และไม่สามารถส่งสัญญาณข้ามโหนดไปมาได้ การส่งข้อมูลแบบนี้เปรียบได้กับคู่สายโทรศัพท์ที่สามารถคุยได้เฉพาะต้นทางกับปลายทาง แต่ไม่สามารถคุยพร้อมกันได้เลยหลาย ๆ คน ข้อจำกัดของการใช้สัญญาณแบบนี้ คือจะต้องขออนุญาตจาก FCC (Federal Communication Committee) ซึ่งเป็นหน่วยงานที่กำหนดความถี่ในการใช้สัญญาณคลื่นวิทยุแบบ Narrow band นี้

2.1.8.2 Spread Spectrum Technology

ระบบเครือข่ายไร้สายส่วนใหญ่นิยมใช้เทคนิค Spread Spectrum Technology ซึ่งใช้ความถี่ที่กว้างกว่า Narrow Band Technology ซึ่ง Spread Spectrum คือ วิธีการเปลี่ยนแปลงสัญญาณข้อมูลเพื่อให้ครอบคลุมพื้นที่ความถี่วิทยุมากเกินความจำเป็น ระบบนี้เป็นการส่งสัญญาณออกไปหลายความถี่พร้อมกัน ทำให้สามารถป้องกันการรบกวนการสื่อสาร เพราะจะต้องค้นหาคลื่นความถี่ทั้งหมดให้ได้ โดยการส่งสัญญาณจะใช้แถบความถี่ ISM ที่ช่วงความถี่ ระหว่าง 902-928 MHz และ 2.4-2.484 GHz เทคนิค Spread Spectrum สามารถแบ่งได้ เป็น สอง แบบ คือ Direct Sequence และ Frequency - Hopping

2.1.8.3 Direct Sequence Spread Spectrum (DSSS)

Direct Sequence Spread Spectrum เป็นเทคนิคที่ยังใช้คลื่นพาหะที่ต้องระบุความถี่ที่ใช้สามารถส่งข้อมูลได้มากกว่าแบบ Narrow Band ข้อมูลจะถูกกระจายให้ช่วงความถี่กว้างขึ้น ในรูปแบบของรหัสเฉพาะ รูปแบบของรหัสเฉพาะที่เป็นที่รู้จักกันดีคือ Pseudo-Noise Sequence หรือ PN Sequence รูปแบบนี้จะใช้การเข้ารหัสในวิธีพิเศษ โดยการแปลงเลขฐานสองแต่ละบิตในข้อมูลดั้งเดิมที่จะส่งไปให้อยู่ในรูปแบบเลขฐานสองที่มีความยาวเพิ่มมากขึ้น ตัวอย่างเช่น ข้อมูล

เลขฐานสอง 1 อาจจะถูกละเปลี่ยนเป็น 0010010101 และข้อมูล 0 จะถูกละเปลี่ยนเป็น Inverse ของ 1 คือ 0
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้คัดลอกเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1101101010 ข้อมูลที่แปลงแล้วจะถูกส่งไปพร้อมๆกันในลักษณะขนาน ซึ่งหากผู้รับสามารถจดจำรูปแบบการแปลงข้อมูลได้ข้อมูลก็จะถูกส่งไป โดยที่สัญญาณรบกวนไม่สามารถทำให้ข้อมูลเสียหายไปได้ หรือหากรูปแบบที่ส่งไปเกิดผิดพลาดไปไม่ว่าจะด้วยสาเหตุใดก็ตาม ทางฝ่ายรับก็สามารถที่จะใช้เทคนิคในทางสถิติเพื่อกู้ข้อมูลที่ผิดพลาดไปให้กลับคืนมาได้ โดยวิธีนี้จะใช้ในมาตรฐาน IEEE802.11 และ IEEE 802.11b

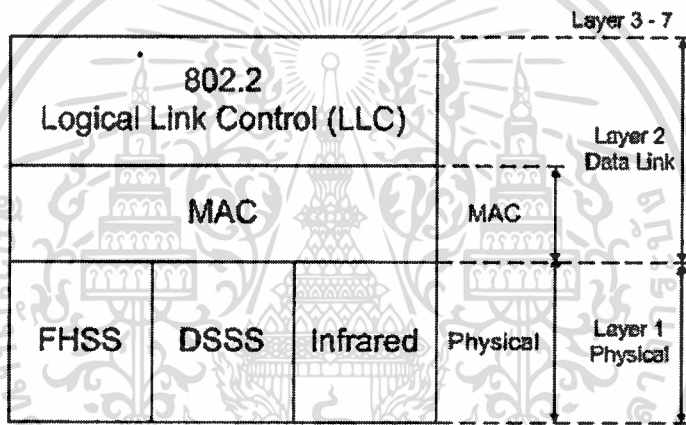
2.1.8.4 Frequency – Hopping Spread Spectrum (FHSS)

การส่งสัญญาณรูปแบบนี้จะใช้ความถี่แคบพาหะเพียงความถี่เดียว (Narrow Band) และจะเปลี่ยนแปลงความถี่ (กระโดด) ไปมาอย่างต่อเนื่อง ในลักษณะที่เครื่องส่งกับเครื่องรับสามารถทำงานประสานกัน วิธีการส่งแบบนี้ป้องกันสัญญาณรบกวนที่เกิดจากความถี่ข้างเคียง ได้เป็นอย่างดี เพราะว่าความถี่จะมีการเปลี่ยนแปลงตลอดเวลา โดยการส่งและรับแต่ละครั้งที่ส่วนหัวของแพคเกจข้อมูลจะบอก ทำให้เกิดความปลอดภัยของข้อมูลสูงมากขึ้น การส่งข้อมูลวิธีนี้สามารถส่งข้อมูลไปพร้อมๆกันหลายช่องสัญญาณได้ด้วยการกำหนดให้มีรูปแบบของการเปลี่ยนแปลงหลายๆรูปแบบทำงานไปพร้อมกัน ซึ่งจะสามารถใช้ประโยชน์แถบความถี่ได้ดีกว่าและทำให้เครือข่ายมีประสิทธิภาพสูงกว่า

2.1.8.5 Infrared Technology

ลำแสงอินฟราเรด (Infrared : IR) เป็นส่วนหนึ่งของสเปกตรัมแม่เหล็กไฟฟ้าอยู่ในย่านความถี่ของแสงที่อยู่ต่ำกว่าแสงสีแดงที่ตาของพวกเราสามารถมองเห็นได้ เป็นลำแสงอีกชนิดหนึ่งที่ถูกนำมาใช้เพื่อการสื่อสารที่ใช้ในระยะใกล้ ตัวอย่างของการใช้ลำแสงอินฟราเรดที่พบได้ในชีวิตประจำวันได้แก่ อุปกรณ์ควบคุมระยะไกลแบบไร้สาย (Wireless Remote Control) ที่ใช้ควบคุมเครื่องรับโทรทัศน์ เครื่องเล่นวีดีโอ เครื่องเสียงและอุปกรณ์ไฟฟ้าต่างๆ ในระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์และอุปกรณ์บางชนิดได้ใช้ลำแสงอินฟราเรดเพื่อการติดต่อสื่อสารระหว่างกันแบบจุดต่อจุดเช่น คอมพิวเตอร์โน้ตบุ๊ก เครื่องคอมพิวเตอร์มือถือ (Hand held) จะมีพอร์ตอินฟราเรดเพื่อรับส่งข้อมูลออกไปยังเครื่องพิมพ์ซึ่งเครื่องพิมพ์แบบเลเซอร์สำหรับสำนักงานบางรุ่นจะรับข้อมูลผ่านทางพอร์ตอินฟราเรด คุณสมบัติเด่นของคลื่นอินฟราเรดและคลื่นสั้น คือเดินทางเป็นแนวตรง ราคาถูก และง่ายต่อการผลิตใช้งาน แต่คลื่นประเภทนี้ไม่สามารถเดินทางผ่านวัตถุหรือสิ่งกีดขวางได้ ซึ่งเป็นข้อดีคือสามารถนำอุปกรณ์ที่ใช้คลื่นอินฟราเรดมาใช้ในห้องทำงานที่อยู่ติดกันได้แม้ว่าอุปกรณ์ทั้งสองชิ้นนั้นจะใช้ความถี่เดียวกันนอกจากนี้อุปกรณ์ที่ใช้คลื่นอินฟราเรดยังปลอดภัยจากการถูกลักลอบดักสัญญาณด้วย คุณสมบัติเหล่านี้ทำให้คลื่นอินฟราเรดสามารถนำมาใช้ในการสื่อสารในระบบเครือข่ายเฉพาะบริเวณได้เป็นอย่างดี

มาตรฐานระบบเครือข่ายแบบไร้สาย 802.11 ใช้ตัวกลางในการสื่อสารเป็นอากาศ เช่นเดียวกับที่มาตรฐาน 802.3 อนุญาตให้ใช้สายคู่ตีเกลียวหรือสายโคแอกเชียลเป็นตัวกลางในการสื่อสารข้อมูล ตัวกลางที่มาตรฐาน 802.11 ใช้จะแบ่งเป็นแสงอินฟราเรดที่สามารถนำมาประยุกต์ใช้ได้โดยที่ไม่จำเป็นต้องขออนุญาต และคลื่นวิทยุอีก 2 รูปแบบที่ใช้งานอยู่ในช่วงความถี่ 2.4-GHz ช่วงความถี่ในช่วงนี้เป็นช่วงความถี่ที่สามารถนำมาใช้ได้โดยที่ไม่ต้องขออนุญาตเช่นกัน รูปแบบของคลื่นวิทยุที่ใช้งานประกอบด้วยแบบ Frequency hopping spread spectrum (FHSS) และ Direct sequence spread spectrum (DSSS) ซึ่งทั้งหมดจะถูกกำหนดไว้ในส่วนของชั้นกายภาพ (Physical layer) ดังแสดงในรูปที่ รูปที่ 2.12



รูปที่ 2.12 แสดงส่วนประกอบต่างๆ ในชั้นฟิสิกส์คอล

เทคโนโลยีการกระจายระยะคลื่น (Spread spectrum) นี้เป็นเทคนิคในการมอดดูเลตสัญญาณที่ได้มีการพัฒนาขึ้นในช่วง 1940 โดยที่จะทำการกระจายสัญญาณที่จะส่งออกไปให้กระจายอยู่ในช่วงความถี่วิทยุต่างๆ กัน เทคนิคนี้จะดีสำหรับการนำมาใช้กับการสื่อสารข้อมูล เพราะว่าจะสามารถทนต่อสัญญาณรบกวนได้ดี

การทำงานของ FHSS จะใช้วิธีการเปลี่ยนช่วงความถี่ในการสื่อสาร ความถี่จะถูกแบ่งเป็นช่วงๆ เพื่อใช้งาน ช่วงเวลาของความถี่ที่แบ่ง จะมีค่าเท่ากันในทุกๆ ช่วง (dwell time) เมื่อทำการสื่อสาร ข้อมูลจะถูกส่งโดยใช้ช่วงความถี่ที่แบ่งไว้ตามเวลาที่กำหนดและตามลำดับการใช้งานตามช่วงความถี่ที่แน่นอน ส่วนการทำงานของ DSSS ใช้วิธีการการเปลี่ยนเฟสของคลื่นความถี่เพื่อสร้างชุดของบิตของข้อมูล ชุดของบิตของข้อมูลนี้จะใช้แทนข้อมูลจริงที่ต้องการส่งผ่านระบบเครือข่าย เมื่อเปรียบเทียบลักษณะ ประสิทธิภาพของ FHSS และ DSSS แล้ว การทำงานทั้งสองแบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น เมื่ออนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

มีข้อดีที่แตกต่างกัน กล่าวคือ FHSS จะมีความทนทานต่อการรบกวนสูงกว่า DSSS แต่ DSSS จะมีความเร็วในการเชื่อมต่อที่ดีกว่า มีความสามารถในการส่งได้ไกลมากกว่า FHSS

การใช้งานในรูปแบบของ FHSS จะมีความเร็วในการสื่อสารข้อมูลจำกัดอยู่ที่ 2-Mbps และมีการแนะนำให้นำมาใช้สำหรับงานเฉพาะทางเท่านั้น ส่วนในการนำระบบเครือข่ายไร้สายมาประยุกต์ใช้งานโดยทั่วๆ ไปแล้ว จะใช้รูปแบบของ DSSS เพราะเป็นตัวเลือกที่ดีกว่า มาตรฐานสำหรับระบบเครือข่ายแบบไร้สายที่ได้ถูกกำหนดมาล่าสุดคือมาตรฐาน IEEE 802.11b สามารถทำงานได้ที่ความเร็ว 11 Mbps เทียบเท่ากับการทำงานของอินเทอร์เน็ต โดยใช้รูปแบบการทำงานแบบ DSSS

2.1.9 ระบบความปลอดภัยสำหรับมาตรฐาน IEEE 802.11

ระบบความปลอดภัยสำหรับระบบเครือข่ายไร้สายตามมาตรฐาน IEEE 802.11 นั้น มีอยู่ด้วยกันหลายส่วน ที่จะทำงานร่วมกัน โดยแบ่งออกได้ดังต่อไปนี้ คือ

- Extended Service Set ID (ESSID)
- Access Lists
- Authentication and Association
- Wired Equivalent Privacy (WEP)

2.1.9.1 Extended Service Set ID (ESSID)

หลักการการทำงานของ ESSID คือ การให้หมายเลขประจำตัวสำหรับทุกจุดเชื่อมต่อ (Access Point) และไคลเอนต์ทั้งหมดที่อยู่ในระบบเครือข่ายไร้สาย โดยการกำหนดในลักษณะนี้ จะเหมือนกับการกำหนดชื่อของระบบเครือข่ายนั่นเอง แต่โดยทั่วไปแล้วผู้ผลิตอุปกรณ์ระบบเครือข่ายแบบไร้สายจะกำหนดค่ามาตรฐานไว้ ดังนั้นเมื่อนำมาใช้งาน จึงควรเปลี่ยนค่าของ ESSID โดยทันที

2.1.9.2 Access Lists

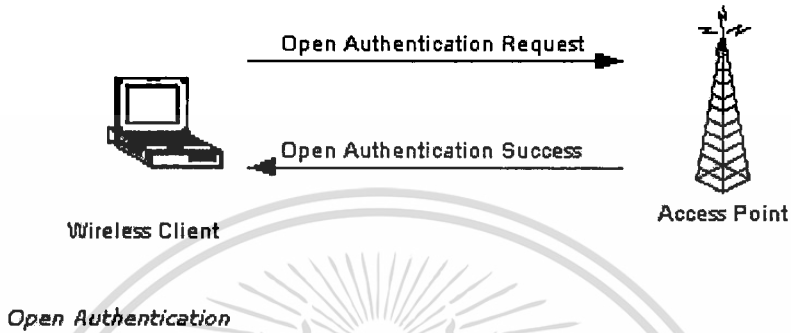
การใช้งาน Access Lists นี้จะกระทำที่จุดเชื่อมต่อ (Access Point) โดยที่จะกำหนดรายการของค่า MAC address ของไคลเอนต์แบบไร้สาย ที่ได้รับอนุญาตให้สามารถเชื่อมต่อกับระบบได้ ถ้า MAC address ของไคลเอนต์ใดที่ไม่อยู่ในรายการของจุดเชื่อมต่อ ก็จะไม่สามารถเชื่อมต่อเข้ากับระบบเครือข่ายได้

2.1.9.3 Authentication and Association

กระบวนการในการรับรองสิทธิ์และการเข้าใช้งานในระบบเครือข่ายไร้สายตามมาตรฐาน IEEE 802.11 นี้จะแบ่งออกเป็น สอง รูปแบบ คือ

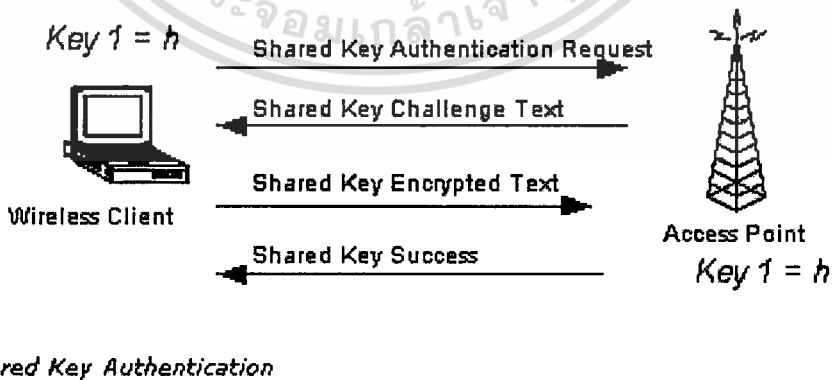
- ระบบเปิด (Open System Authentication)
- กุญแจร่วม (Shared Key Authentication)

การใช้กระบวนการรับรองสิทธิ์แบบระบบเปิดจะเป็นกระบวนการพื้นฐานที่สุด กล่าวคือ จะไม่มีการใช้กุญแจในขั้นตอนการรับรองสิทธิ์ และมีขั้นตอนทั้งหมดในการแสดงสิทธิ์เพียง สอง ขั้นตอนเท่านั้น ดังแสดงในรูปที่ 2.13



รูปที่ 2.13 แสดงระบบเปิด (Open System Authentication)

การใช้กระบวนการรับรองสิทธิ์แบบใช้กุญแจร่วมกันนี้ จะต้องมีการใช้งานกุญแจที่ใช้งานร่วมกันระหว่างไคลเอนต์และจุดเชื่อมต่อ โดยกุญแจดังกล่าวนี้จะใช้เป็นเครื่องมือในการเข้าและถอดรหัสข้อความที่ใช้แสดงตัวของไคลเอนต์ ดังนั้นจะมีเพียงไคลเอนต์ที่มีกุญแจที่ถูกต้องเท่านั้น ที่จะสามารถทำการถอดรหัสได้ โดยขั้นตอนดังกล่าวจะอยู่ในช่วงขั้นตอนที่ สอง และ สาม ของกระบวนการในการรับรองสิทธิ์ ดังแสดงในรูปที่ 2.14

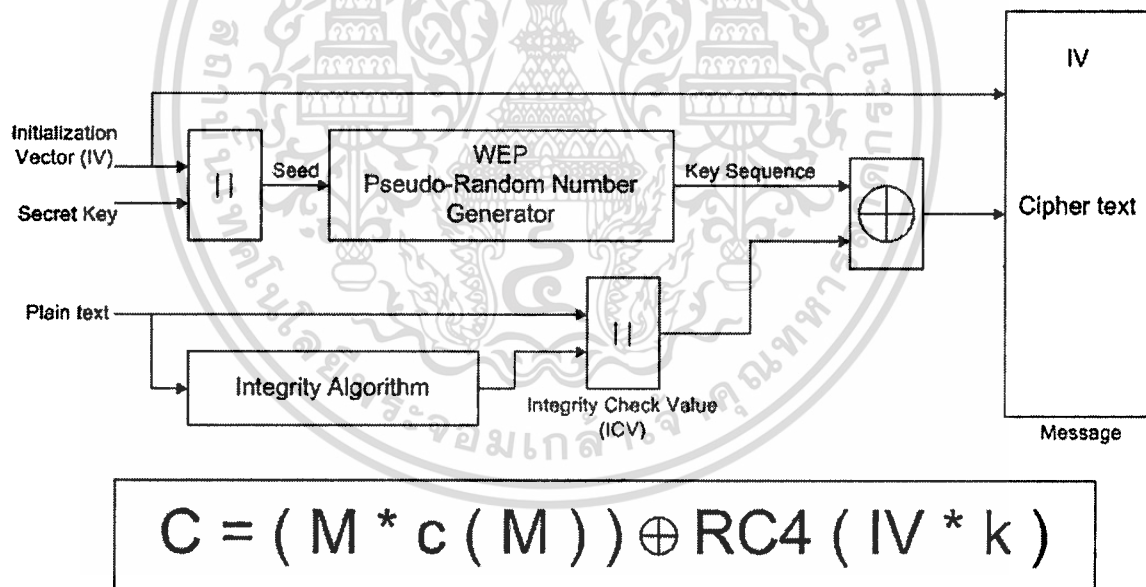


รูปที่ 2.14 แสดงระบบกุญแจร่วม (Shared Key Authentication)

กระบวนการในการรับรองสิทธิ์แบบใช้กุญแจร่วมกัน จะใช้ Wired Equivalent Privacy (WEP) ซึ่งถูกกำหนดไว้ในมาตรฐานการเชื่อมต่อระบบเครือข่ายไร้สาย IEEE 802.11 โดยใช้เป็นเครื่องมือในการเข้าและถอดรหัสของข้อมูลที่สื่อสารกันผ่านระบบเครือข่ายไร้สาย การใช้งานระบบกุญแจร่วมกัน จะเป็นตัวเลือกให้ใช้งาน ไม่ได้ถูกกำหนดมาเป็นค่ามาตรฐานในการเชื่อมต่อ ดังนั้น ถ้าต้องการที่จะใช้งานระบบแบบกุญแจร่วมกันแล้ว จะต้องทำการกำหนดตัวเลือกในการใช้งานให้ถูกต้องด้วย

2.1.9.4 Wired Equivalent Privacy (WEP)

กลไกการทำงานของโปรโตคอล WEP นี้จะเป็นกระบวนการที่ใช้ในการเข้าและถอดรหัสข้อมูลที่ผู้รับและผู้ส่งสื่อสารกัน เพื่อทำการเพิ่มความปลอดภัยให้กับข้อมูล โดยที่มีจุดประสงค์ให้มีลักษณะและประสิทธิภาพการทำงานได้เช่นเดียวกันกับที่ใช้ในระบบเครือข่ายแบบใช้สาย ซึ่งจะมีการทำงาน ดังแสดงในรูปที่ 2.15



รูปที่ 2.15 แสดงการทำงานของ Wired Equivalent Privacy (WEP)

ขั้นตอนการทำงานของ WEP ที่มาตรฐาน IEEE 802.11 ใช้นั้นจะใช้กลไกการเข้าและถอดรหัสแบบอาร์ซีไฟร์ โดยที่อาร์ซีไฟร์นี้จะมีส่วนประกอบอยู่ด้วยกัน สอง ส่วนคือ

- ส่วนที่ใช้ในการกำหนดกุญแจที่จะใช้งาน (Key Scheduling Algorithm)
- ส่วนที่ใช้ในการสร้างผลลัพธ์ (Output Generator)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ส่วนการกำหนดคกุญแจขึ้นมาใช้งานนั้น WEP ที่มีใช้อยู่ในปัจจุบันจะมีรูปแบบการทำงานในส่วนนี้อยู่สองรูปแบบคือ การใช้ 64-bit packet key (40-bit secret key + 24-bit IV) และ 128-bit packet key (104-bit secret key + 24-bit IV) ซึ่งถ้าจำนวนบิตที่ใช้ในการสร้างคกุญแจยิ่งมากก็จะทำให้ระบบมีความปลอดภัยมากขึ้นด้วย ส่วนการทำงานในส่วนของการสร้างผลลัพธ์นั้นจะใช้วิธีการเรียงสับเปลี่ยน (Permutation) ซึ่งจะได้ผลลัพธ์เป็นลำดับของข้อมูลที่ถูกเรียงสับเปลี่ยนแล้ว จากรูปที่ 2.15 ข้างต้นจะอธิบายขั้นตอนการทำงานของ WEP ได้ดังนี้คือ นำเอาข้อมูลที่ต้องการส่งมาทำการเข้ารหัสโดยการเข้ารหัสเพื่อตรวจสอบความถูกต้องของข้อมูลระหว่างผู้รับกับผู้ส่ง (Integrity Check Value) จะได้ผลลัพธ์เป็น $M * c(M)$ จากสมการข้างต้น M คือข้อมูลที่ต้องการส่ง นำมาต่อกับ $c(M)$ ซึ่งคือการสร้าง ICV เพื่อทำการตรวจสอบ ทำการสร้างลำดับของคกุญแจ (Key Sequence) จากสมการข้างต้นโดยการใช้คกุญแจ k และค่า IV (Initialization vector) มาเชื่อมต่อกันและทำการเรียงสับเปลี่ยนโดยใช้วิธีการของอาร์ซีโพรและมีความยาวของข้อมูลเท่ากับส่วนของ $M * c(M)$ โดยที่ค่า IV ที่ใช้จะเป็นค่าที่ได้จากการสุ่มและไม่ซ้ำกันในการส่งแต่ละครั้ง ทำการเข้ารหัสข้อมูลโดยการนำข้อมูลที่ได้ทั้งสองส่วนมาทำการ XOR กัน แล้วส่งไปยังผู้รับ เมื่อผู้รับได้รับข้อมูลแล้วจะทำการถอดรหัสโดยใช้คกุญแจร่วมและจะสามารถทำการตรวจสอบผู้ส่งได้จากค่า ICV ที่ได้เพิ่มไปในตอนต้นด้วย

2.1.10 คุณสมบัติของไวร์เลสแอสเซสพอยต์

2.1.10.1 Range and Coverage

ระยะทางและเส้นทางการแพร่กระจายของคลื่น ซึ่งขึ้นอยู่กับสิ่งแวดล้อม เช่น กำแพงโลหะ เป็นต้น วัตถุที่เป็นของแข็งจะกั้นสัญญาณอินฟราเรดซึ่งเป็นการจำกัดพื้นที่ครอบคลุมของระบบเครือข่ายไร้สาย ระยะหรือรัศมีการครอบคลุมของสัญญาณสำหรับระบบเครือข่ายไร้สายโดยทั่วไปจะมีค่าในช่วง 100 ฟุต จนถึง 300 ฟุต การครอบคลุมของสัญญาณสามารถขยายออกและมีอิสระในการเคลื่อนย้ายไปยังที่ต่างๆ ได้

2.1.10.2 Throughput

คืออัตราการส่งข้อมูลเข้าสู่ระบบเครือข่าย ไร้สายปัจจัยที่มีผลต่ออัตราการส่งข้อมูลเข้าประกอบด้วย จำนวนของผู้ใช้ ระยะทางและเส้นทางการแพร่กระจายของคลื่น ชนิดของระบบเครือข่ายไร้สายที่ใช้ อัตราการส่งข้อมูลในระบบเครือข่ายไร้สายจะมีค่าประมาณ 1.6 เมกะบิตต่อวินาที ซึ่งสามารถนำไปใช้เปรียบเทียบการส่งข้อมูล โดยพิจารณาจากอัตราการส่งข้อมูล เช่น โมเด็มรุ่น State-of-Art V.90 มีอัตราการส่งข้อมูล 56.6 กิโลบิตต่อวินาที ซึ่งแสดงถึงอัตราการส่งข้อมูลที่ช้ากว่าอัตราการส่งข้อมูล 1.6 เมกะบิตต่อวินาทีถึง 30 เท่า

2.1.10.3 Integrity and Reliability

เทคโนโลยีระบบเครือข่ายไร้สายมีความมั่นคงและความน่าเชื่อถือสูง เพราะเมื่อคลื่นวิทยุถูกรบกวนระบบจะลดอัตราการส่งข้อมูลเข้าลงเพื่อลดความผิดพลาดที่อาจเกิดจากการรบกวนได้ นอกจากนี้การออกแบบให้ระบบเครือข่ายไร้สายมีพื้นที่ครอบคลุมที่จำกัดทำให้ความถูกต้องของข้อมูลสูงกว่าการเชื่อมต่อด้วยระบบเครือข่ายมีสายเพราะระยะทางที่จำกัดและการสื่อสารแบบจุดต่อจุดทำให้โอกาสผิดพลาดต่ำ

2.1.10.4 Compatibility with the Existing Network

ระบบเครือข่ายแลนไร้สายส่วนใหญ่จะมีมาตรฐานอุตสาหกรรมในการติดต่อกับเครือข่ายมีสาย เช่น ethernet หรือ Token Ring เครื่องคอมพิวเตอร์ในเครือข่ายแลนไร้สายจะถูกสนับสนุนโดยระบบปฏิบัติการเครือข่ายเหมือนกันกับเครื่องคอมพิวเตอร์ในเครือข่ายอื่นๆ โดยพิจารณาใช้ไครฟ์เวอร์ที่เหมาะสม การติดตั้ง เพียงครั้งเดียวเครื่องคอมพิวเตอร์ในการปฏิบัติการเครือข่ายไร้สายจะเหมือนกับส่วนประกอบของเครือข่ายอื่นๆ

2.1.10.5 Interoperability of Wireless Devices

ผู้ซื้อควรจะทราบว่าระบบเครือข่าย LAN ไร้สายจากผู้ขายที่แตกต่างกันนั้นจะไม่ทำงานร่วมกันได้ มีเหตุผล สาม ข้อคือ

- เทคโนโลยีที่แตกต่างกันจะทำงานร่วมกันไม่ได้ระบบพื้นฐานบนเทคโนโลยีการเผยแพร่สเปกตรัมความถี่แบบกระโดด FSSHจะไม่สื่อสารกับระบบพื้นฐานอื่นบนเทคโนโลยีการเผยแพร่ความถี่โดยตรงแบบลำดับ DSSS
- ระบบใช้ความกว้างของความถี่ต่างกันจะไม่ทำงานร่วมกันแม้ว่าจะใช้เทคโนโลยีที่เหมือนกันก็ตาม
- ระบบจากผู้ขายที่ต่างกันจะไม่ทำงานร่วมกันแม้ว่าจะมีเทคโนโลยีหรือความกว้างที่เหมือนกับรวมกับการดูแลของแต่ละผู้ขายต่างกัน

2.1.10.6 Interference and Coexistence

ลักษณะที่ไม่ได้รับอนุญาตฐานคลื่นวิทยุระบบเครือข่ายแลนไร้สาย หมายถึงสินค้าอื่นซึ่งส่งพลังงานในความถี่เดียวกัน สามารถทำให้ระดับความดันไฟฟ้าบางขนาดรบกวนถึงระบบเครือข่ายแลน ไร้สายได้ เตาอบไมโครเวฟเป็นพลังงานที่เกี่ยวข้องด้วยแต่ระบบเครือข่ายแลนไร้สายส่วนใหญ่ออกแบบสินค้าของพวกเขาให้รับผิดชอบสำหรับการรบกวนคลื่นไมโครเวฟ ส่วนอื่นๆที่เกี่ยวข้องคือสถานที่ที่ระบบเครือข่ายแลนไร้สายสามารถรวมกันขณะที่เครือข่ายแลนไร้สายจากบางผู้ผลิตรบกวนเครือข่าย แลน ไร้สายอยู่ การรวมกันของคลื่นจะไม่ ถูกรบกวน แต่ก็ขึ้นอยู่กับกำหนัด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.10.7 Licensing Issues

ในสหรัฐอเมริกา the Federal Communications commission(FCC) เป็นคณะกรรมการควบคุมการส่งคลื่นวิทยุ ประกอบด้วยการทำงานในระบบเครือข่ายแลนไร้สาย ชาติอื่นๆก็มีตัวแทนควบคุมเช่นกัน ระบบเครือข่าย LANไร้สายถูกออกแบบให้ปฏิบัติการในส่วนของสเปกตรัมวิทยุที่ซึ่ง FCC ไม่ต้องการให้ผู้ใช้สุดท้ายซื้อลิขสิทธิ์ที่ใช้คลื่นอากาศ ในสหรัฐอเมริการะบบเครือข่าย LANไร้สายส่วนใหญ่ขยายช่วงกว้างในการใช้เครื่องมือมากขึ้น ประกอบด้วย 902-928 MHz, 2.4-2.483 GHz, 5.15-5.35GHz และ 5.725-5.875GHz สำหรับระบบเครือข่ายแลนไร้สาย ถูกขายในประเทศโดยเฉพาะ การผลิตของระบบเครือข่ายLANไร้สาย ต้องได้รับประกันโคเนตตัวแทนที่เหมาะสมในประเทศนั้นๆ

2.1.10.8 Simplicity/Ease of use

ผู้ใช้งานเป็นที่ต้องการข่าวสารใหม่ ๆ เล็กน้อยเพื่อการใช้ประโยชน์ของระบบเครือข่ายแลนไร้สาย เพราะธรรมชาติของกรไร้สายของระบบเครือข่ายแลนไร้สายจะโปร่งแสงถึงผู้ใช้ของ NOP การทำงานของแอปพลิเคชันเหมือนกับระบบเครือข่ายแลนมีสาย สิ้นค้าเครือข่ายแลนไร้สายจะรวบรวมความหลากหลายของเครื่องมือวินิจฉัยถึงที่อยู่จะมีความสัมพันธ์กับส่วนประกอบมีสายของระบบ อย่างไรก็ตาม สิ้นค้าถูกออกแบบมาเพื่อให้ผู้ใช้ส่วนใหญ่ใช้เครื่องมือที่จำเป็น

ระบบเครือข่ายแลนไร้สายมีหลายอย่างที่ง่ายต่อการติดตั้ง และองค์ประกอบพื้นฐานที่จัดการสิ่งที่มารบกวนเครือข่าย ตั้งแต่การเข้าถึงจุดของระบบเครือข่ายแลนไร้สายต้องการการเคเบิล การจัดการเครือข่ายเป็นอิสระจากการตั้งสายเคเบิลสำหรับระบบเครือข่ายแลนไร้สาย การขาดแคลนเคเบิลก็ยังสามารถเคลื่อนที่ การเพิ่มและการเปลี่ยนการดำเนินการเล็ก ๆ น้อย ๆ สำหรับระบบเครือข่ายแลนไร้สาย สุดท้าย ธรรมชาติการเคลื่อนย้ายของระบบเครือข่ายแลนไร้สาย ปล่อยให้มีการจัดการเครือข่ายและมีผู้เชี่ยวชาญในการแก้ปัญหาเครือข่ายก่อนการติดตั้ง ที่ตำแหน่งที่ตั้งไกล ระบบเครือข่ายแลนไร้สายสามารถเคลื่อนที่จากสถานที่หนึ่งไปยังอีกที่

2.1.10.9 Security

เพราะเทคโนโลยีเครือข่ายไร้สายมีรากในแอปพลิเคชัน ระบบความปลอดภัยถูกออกแบบให้มีมาตรฐานสำหรับอุปกรณ์ไร้สายข้อกำหนดความปลอดภัยถูกสร้างไปยังระบบเครือข่ายแลนไร้สายทำให้มีความปลอดภัยมากกว่าระบบเครือข่ายแลนมีสายมันเป็นการยากมากสำหรับผู้ที่ไม่ได้มุ่งหมายจะฟังในการจรรยาบรรณเครือข่ายแลนไร้สาย เทคนิคการสร้างรหัสลับที่ซับซ้อนมันเป็นไปไม่ได้สำหรับทั้งหมดแต่ส่วนใหญ่จะไม่ได้รับอนุญาตให้เข้าถึงการจรรยาบรรณนี้ได้ในทุกๆ คอมพิวเตอร์เครือข่าย

ข่าย ต้องมีระบบความปลอดภัยก่อนที่จะได้รับอนุญาตให้เข้าไปในการจรรยาบรรณเครือข่าย โยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.10.10 Cost

เครื่องมือระบบเครือข่ายแลนไร้สายประกอบด้วยราคาโครงสร้างพื้นฐานสำหรับการเข้าถึง และราคาผู้ใช้สำหรับอุปกรณ์ต่อเชื่อมเครือข่ายแลนไร้สายขึ้นอยู่กับความสำคัญบนจำนวนของจุดเข้าถึงอย่างเหมาะสมโดยจุดเข้าถึงอยู่ในช่วงราคา \$1000-\$ 2000 จำนวน จุดเข้าถึงจะขึ้นอยู่กับพื้นที่ที่ครอบคลุมบริเวณ ชนิดของบริการ การครอบคลุมพื้นที่ คือส่วนของสี่เหลี่ยมของระยะสินค้า อุปกรณ์เชื่อมต่อเครือข่ายไร้สายมีราคาในช่วง \$300-\$1000 ราคาของการติดตั้งและดูแลระบบเครือข่ายไร้สายจะถูกกว่าแบบระบบเครือข่ายLANมีสายด้วย สอง เหตุผลคือ

- ระบบเครือข่ายแลนไร้สายปราศจากราคาของการเคเบิลและการมีส่วนร่วมในการติดตั้งและดูแล
- ระบบเครือข่ายแลนไร้สายง่ายต่อการเคลื่อนที่ เพิ่มและเปลี่ยน พวกมันจะลดราคาโดยอ้อมของเวลาที่ลดลงและเกี่ยวกับการจัดการบริหาร

2.1.10.11 Scalability

เครือข่ายไร้สายสามารถถูกออกแบบให้ง่ายอย่างมากหรือมีความซับซ้อนได้ เครือข่ายไร้สายสามารถสนับสนุนเครื่องปลายทางจำนวนมากและหรือพื้นที่ทางกายภาพ โดยการเข้าถึงจุดที่ส่งหรือขยายการครอบคลุม

2.1.10.12 Battery Life for Mobile Platforms

สินค้าไร้สายถูกออกแบบให้ปราศจากไฟกระแสดตรง คือให้ใช้แบตเตอรี่จากตัวโน้ตบุคหรือคอมพิวเตอร์มือถือ ผู้จำหน่ายจึงใช้เทคนิคพิเศษในการออกแบบเพื่อให้มีการใช้พลังงานของคอมพิวเตอร์และแบตเตอรี่ให้นานที่สุด

2.1.10.13 Safety

พลังงานที่ออกมาจากระบบเครือข่ายแลนไร้สายนั้นต่ำมากซึ่งมีค่าน้อยกว่า โทรศัพท์มือถือ CELLULAR ตั้งแต่คลื่นวิทยุมีความไวเหนือระยะทาง มีการเปิดโอกาสน้อยมากถึงคลื่น RF ที่จัดให้ในพื้นที่ระบบเครือข่ายแลนไร้สาย ระบบเครือข่ายแลนไร้สายต้องพบกับการควบคุมที่แข็งแกร่งและอุตสาหกรรมที่มีความปลอดภัยไม่เป็นอันตรายต่อผู้ใช้จากระบบเครือข่ายแลนไร้สาย

2.1.11 ประโยชน์ของระบบเครือข่ายไร้สาย

- Mobility improves productivity & service มีความคล่องตัวสูง ดังนั้นไม่ว่าเราจะเคลื่อนที่ไปที่ ไหนหรือเคลื่อนย้ายคอมพิวเตอร์ไปตำแหน่งใด ก็ยังมีการเชื่อมต่อ กับเครือข่าย ตลอดเวลา トラบไคที่ยังอยู่ในระยะการส่งข้อมูล
- Installation speed and simplicity สามารถติดตั้งได้ง่ายและรวดเร็ว เพราะไม่ต้องเสียเวลา

เอกสารนี้เป็นแค่ต้นแบบและไม่ได้กรังรัง เพื่อการศึกษาเท่านั้น ไม่นิยามให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Installation flexibility สามารถขยายระบบเครือข่ายได้ง่าย เพราะเพียงแค่มิ พีซีการ์ดมาต่อเข้ากับ โน้ตบุ๊ก หรือพีซี ก็เข้าสู่เครือข่ายได้ทันที
- Reduced cost- of-ownership ลดค่าใช้จ่ายโดยรวม ที่ผู้ลงทุนต้องลงทุน ซึ่งมีราคาสูง เพราะในระยะยาวแล้ว ระบบเครือข่ายไร้สายไม่จำเป็นต้องเสียค่าบำรุงรักษา และการขยายเครือข่ายก็ลงทุนน้อยกว่าเดิม หลายเท่า เนื่องด้วยความสะดวกในการติดตั้ง
- Scalability เครือข่ายไร้สายทำให้องค์กรสามารถปรับขนาดและความเหมาะสมได้ง่ายไม่ยุ่งยาก เพราะสามารถโยกย้ายตำแหน่งการใช้งาน โดยเฉพาะระบบที่มีการเชื่อมระหว่างจุดต่อจุด เช่นระหว่างตึกระบบ ไวร์เลสแลนสามารถถูกกำหนดมาใช้ในลักษณะของ Topology ได้หลายรูปแบบ เพื่อการประชุม



บทที่ 3

การวิเคราะห์และออกแบบระบบ

3.1 ปัญหาด้านความปลอดภัย

ปัญหาทางด้านความปลอดภัยที่เกิดขึ้นก็คือระบบไวร์เลสแลนนั้นจะใช้ SSID (Service Set Identifier) ความยาวไม่เกิน 32 ตัวอักษร ในการกำหนดเป็นชื่อของ Network Name ที่เป็นไวร์เลสแลนดังนั้นเครื่องลูกข่ายไวร์เลสแลนทุกตัวที่ต้องการต่อเชื่อมกับไวร์เลสแลนต้องอ้างอิง SSID ค่าเดียวกันทั้งหมด ค่า SSID สามารถถูกโปรแกรม Sniffer แบบไวร์เลสแลนดักจับได้ง่ายเพราะค่า SSID นั้นเป็น Plain Text ที่ไม่ได้เข้ารหัสแต่อย่างใด จริงๆแล้วไวร์เลสแลนนั้นมีโปรโตคอลในการเข้ารหัสข้อมูลที่เรียกว่า WEP (Wired Equivalent Privacy) แต่พบว่ามีแค่เพียง 25 เปอร์เซนต์ เท่านั้นที่ใช้ WEP นอกนั้นก็ใช้แบบ Plain Text ธรรมดาแถมยังใช้ค่า Default SSID ที่มากับอุปกรณ์ไวร์เลสแลนแฮคเซอร์ที่ต่างหาก เช่นค่า Default SSID ของ CISCO Aironet ไวร์เลสแลนแฮคเซอร์คือ Tsunami ทำให้แฮกเกอร์สามารถสแกนพบได้โดยง่าย

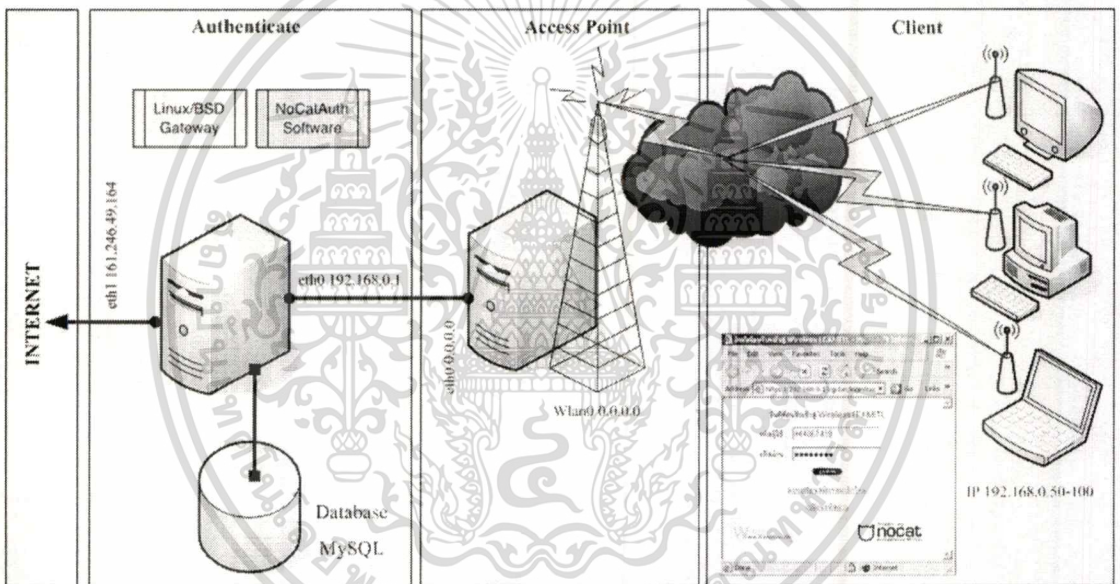
ถึงแม้ว่าเราจะใช้ WEP ในการเข้ารหัสแต่ WEP มีการเข้ารหัสบนพื้นฐาน RC4 Algorithm การเข้ารหัสแบบ RC4 นั้นมีช่องโหว่ (Vulnerability) ที่แฮกเกอร์สามารถเจาะได้ (WEP ใช้ 40 Bit Secret Key ในการเข้ารหัส) โดยใช้เทคนิคที่เรียกว่า Known Plain Text Attack หลักการก็คือ แฮกเกอร์จะใช้ Sniffer ดักจับ Packet ข้อมูลที่ถูกเข้ารหัสโดย WEP จำนวนหนึ่งซึ่งมากพอที่จะ Crack WEP ได้ ตัวอย่างโปรแกรม Sniffer ที่ใช้ในการ Crack WEP ได้แก่ AirSnort และ Wepcrack ซึ่งสามารถที่จะถอดรหัส WEP ได้

กลยุทธ์ของแฮกเกอร์ที่จะแอบใช้งานระบบไวร์เลสแลนของเราก็คือ Wardriving และ Warchalking ถ้าพูดถึงกลุ่มของแฮกเกอร์ ในเมือง Pittsburgh ใช้เทคนิคนี้ในการเจาะระบบไวร์เลสแลนกล่าวคือ แฮกเกอร์จะขับรถไปในเมืองผ่านบริเวณที่มีการใช้งานไวร์เลสแลน แล้วแฮกเกอร์จะใช้ Notebook ที่ต่อกับ การ์ดไวร์เลสแลน ที่ Support IEEE 802.11b จากนั้นก็จะใช้โปรแกรมชื่อ Netstrumbler ตรวจสอบระบบ ไวร์เลสแลน ที่แฮกเกอร์ ได้ขับรถผ่านเข้าไปใกล้รัศมีการทำงานของแฮคเซอร์ จากนั้นก็จะ Mark ตำแหน่งของจุดที่มี WLAN เปิดใช้งานอยู่เรียกว่า Warchalking ในเมือง Pittsburgh นั้น กลุ่มของแฮกเกอร์ได้สร้างแผนที่ของเมืองแสดงตำแหน่งของ ไวร์เลสแลนแล้วแฮกเกอร์

ก็สามารถเข้ามาในระบบแลนของเราที่ แอคเซสพอยท์ เชื่อมต่ออยู่ได้โดยง่ายโดยเฉพาะเครือข่ายที่ไม่ได้เปลี่ยนค่า Default SSID หรือ ไม่ได้เข้ารหัสด้วย WEP ถึงเข้ารหัสด้วย WEP ก็ยังถูกถอดรหัสได้อยู่ดี ดังนั้นจะเห็นว่าไวร์เลสแลนนั้นมีจุดอ่อนด้าน Security อยู่พอสมควร

3.2 การแก้ปัญหาด้านความปลอดภัย

การแก้ปัญหาด้านความปลอดภัยของไวร์เลสแลนนั้นสามารถทำได้โดยกำหนดให้มีการพิสูจน์ตัวตน (Authentication) ของเครื่องลูกข่ายไวร์เลสแลนก่อนที่จะสามารถมีสิทธิเข้ามาใช้งานระบบอินเทอร์เน็ต โดยโครงงานนี้จะใช้เครื่องมือ NoCatAuth PGP และ SSL



รูปที่ 3.1 แสดงการทำงานของระบบไวร์เลสแอคเซสพอยท์กับการพิสูจน์ตัวตน

เป็นการลดปัญหาการติดตั้งโปรแกรมกับเครื่องลูกข่าย โดยใช้เว็บเบราว์เซอร์ที่มาพร้อมกับระบบปฏิบัติการแล้วโดยไม่จำเป็นต้องลงเพิ่มเติมอีกทั้งยังเป็นมาตรฐานเดียวกัน

NoCatAuth เปรียบเสมือนตัวกลาง ในการควบคุมการทำงานของระบบ โดยอาศัยโปรแกรมต่างๆ เช่น ใช้โปรแกรม iptables เข้ามาทำเป็นไฟล้วอลท่า NAT เป็นตัวกลางในการทำการพิสูจน์ตัวตน

PGP นำมาเข้ารหัสระหว่าง การพิสูจน์ตัวตน กับ เกตเวย์ เพื่อการตรวจสอบทั้งสองฝ่าย เซิร์ฟเวอร์ที่ทำหน้าเป็นเกตเวย์กับเซิร์ฟเวอร์ที่ทำหน้าที่เป็นตัวการพิสูจน์ตัวตน ว่าเป็นตัวจริงทั้ง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สองฝ่าย เป็นการป้องกันการเซิร์ฟเวอร์ปลอม โดยมีการเข้ารหัส 1024 บิต ทั้งสองฝ่ายจะต้องมีคีย์ ส่วนตัว ตัวเดียวกันในการถอดรหัส

SSL ทำหน้าที่เข้ารหัสระหว่าง เว็บเซิร์ฟเวอร์กับ เว็บเบราว์เซอร์ โดยทำการเข้ารหัส 128 บิต เพื่อป้องกันการดักจับข้อมูลรหัสผ่าน

3.3 ขั้นตอนการทำงานระบบงานใหม่

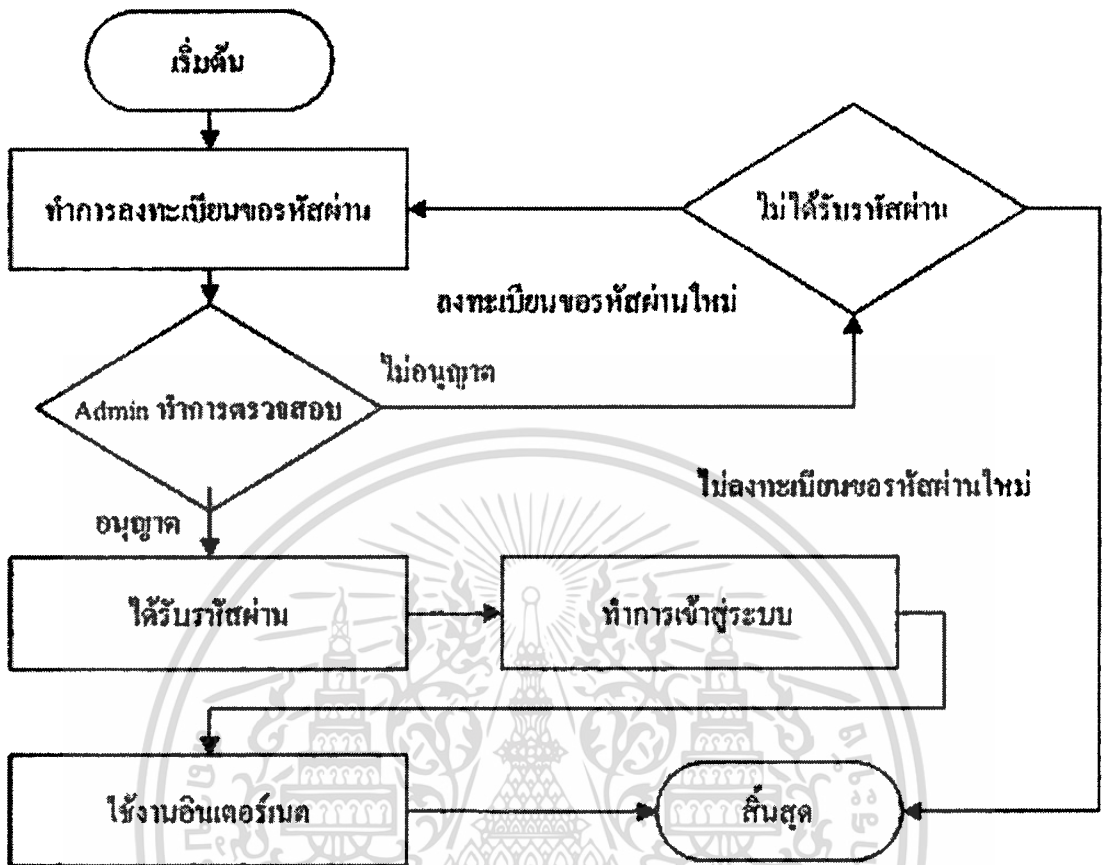
ขั้นตอนที่ 1 ผู้ใช้บริการจะทำการเข้าสู่ระบบ ได้จะต้องทำการลงทะเบียนก่อน นอกเสียจาก ผู้ดูแลระบบทำการลงทะเบียนให้ โดยในขั้นตอนนี้ผู้บริการจะต้องทำการป้อนข้อมูลที่เป็นความจริงและข้อมูลที่สำคัญ ให้ครบ

ขั้นตอนที่ 2 ผู้ดูแลระบบจะทำการตรวจสอบผู้ขอใช้งานนั้นว่าป้อนข้อมูลตรงกับความจริงไหมเมื่อถูกต้องตรงตามความจริงก็จะข้ามไปยังขั้นตอนที่ 4

ขั้นตอนที่ 3 เมื่อป้อนข้อมูลแล้วไม่ถูกต้องตามความจริง ผู้ดูแลระบบจะทำการลบผู้ใช้นั้นออกเมื่อให้ผู้บริการสมัครเข้ามาใหม่ หรือ ไม่ก็จบ

ขั้นตอนที่ 4 เมื่อถูกต้องตามความจริงที่ป้อนข้อมูลลงทะเบียนไปแล้วนั้น ผู้ดูแลระบบจะทำการส่งรหัสผ่านโดยการสุ่มรหัสผ่านแปดตัวไปทางเมลล์

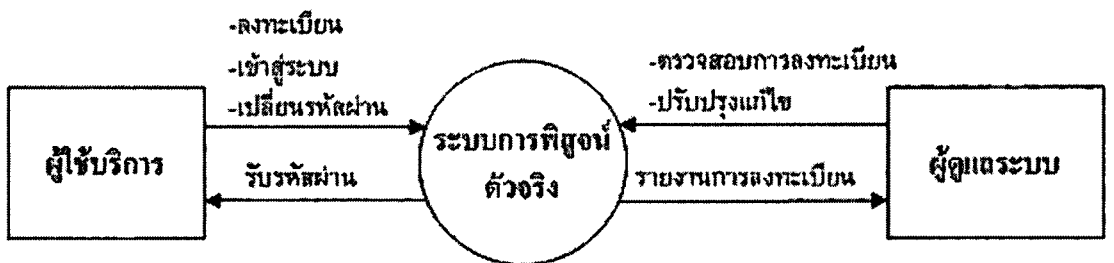
ขั้นตอนที่ 5 เมื่อผู้ใช้ได้รับรหัสผ่านทางเมลล์แล้ว ขั้นตอนต่อไปผู้ใช้งานสามารถเข้าสู่ระบบใช้งานอินเตอร์ได้แล้ว



รูปที่ 3.2 แสดงการทำงานของระบบใหม่

3.4 คอนเท็กซ์ไดอะแกรม ของระบบงานใหม่

การออกแบบโครงสร้างของระบบงานการพิสูจน์ตัวตนจริง สามารถเขียนให้อยู่ในรูปของคอนเท็กซ์ ไดอะแกรม ที่จะแสดงถึงขอบเขตของระบบงาน แสดงถึงสิ่งต่างๆ ที่เกี่ยวข้องกับระบบ และแสดงถึงการไหลของข้อมูลที่สัมพันธ์กันทั้งข้อมูลเข้าและออกจากระบบงาน ดังแสดงตามรูปที่ 3.3



รูปที่ 3.3 แสดงคอนเท็กซ์ ไดอะแกรม ของระบบงานที่ออกแบบใหม่

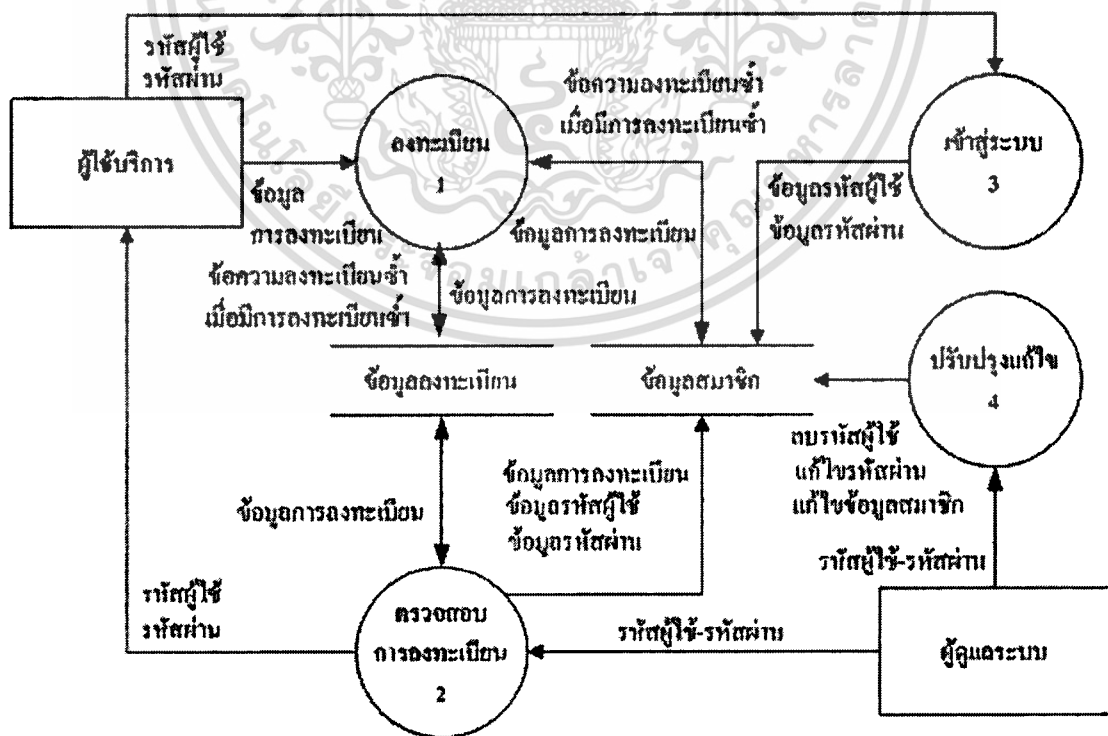
คอนเท็กซ์ โคอะแกรม ดังรูปที่ 3.3 แสดงให้เห็นว่า มีผู้ให้บริการและผู้ดูแลระบบที่มีส่วนเกี่ยวข้องกับระบบงาน ซึ่งอธิบายได้ดังนี้

ผู้ให้บริการ เป็นส่วนของผู้ใช้งานที่จะทำการร้องขอการรับบริการในการเข้าสู่ระบบงาน ซึ่งอาจจะใช้วิธีการลงทะเบียนเพื่อรหัสผ่านระบบ

ผู้ดูแลระบบ เป็นส่วนของผู้หน้าที่ที่คอยทำการตรวจสอบการลงทะเบียนเพื่ออนุญาตให้เข้าใช้งานระบบโดยทำการส่งรหัสผู้ใช้งานกับรหัสผ่าน ไปทางเมลล์ที่ผู้ให้บริการเคยลงทะเบียนขอใช้บริการไว้ครั้งแรกและทำหน้าที่ควบคุมและจัดการกำหนดค่าการทำงานต่างๆ ให้กับระบบไม่ว่าจะเป็นการเปลี่ยนแปลงแก้ไขค่าการทำงานต่างๆ ของระบบงาน

3.5 คาด้าโฟลว์ โคอะแกรม ของระบบงานใหม่

สำหรับภาพรวมการทำงานของทั้งระบบที่เป็นส่วนงานย่อย ที่แสดงถึงความสัมพันธ์โดยรวมระหว่างโพเรสเซส กระแสข้อมูล และการจัดเก็บข้อมูล จากแผนภาพคอนเท็กซ์ โคอะแกรม ของระบบงานที่ออกแบบใหม่ สามารถแสดงภาพการทำงานเป็นคาด้าโฟลว์ โคอะแกรม ได้ ดังรูปที่ 3.4



รูปที่ 3.4 แสดงคาด้าโฟลว์ โคอะแกรมของระบบงานใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น เมื่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รายละเอียดของงานย่อยในแต่ละโพรเซส จากดาต้าโฟลว์ ไดอะแกรมของระบบงาน สามารถแสดงและอธิบายหน้าที่การทำงาน ได้ดังนี้

ลงทะเบียน ทำหน้าที่ในการบันทึกรับรายละเอียดข้อมูลการลงทะเบียนจากผู้ให้บริการ โดยทำการตรวจสอบการลงทะเบียนของผู้ให้บริการก่อนว่าทำการลงทะเบียนซ้ำหรือไม่ ทำการตรวจสอบที่ข้อมูลลงทะเบียนกับข้อมูลสมาชิก

ตรวจสอบการลงทะเบียน ทำหน้าที่ในการตรวจสอบการลงทะเบียนของผู้ขอใช้บริการ โดยผู้ดูแลระบบจะเป็นผู้ตรวจสอบตรงจุดนี้เพื่อทำการอนุญาตแล้วทำการส่งรหัสผู้ให้บริการกับรหัสผ่านให้แก่ผู้ให้บริการที่ได้รับการอนุญาตให้ใช้ระบบแล้ว ไปทางเมลล์ของผู้ให้บริการที่เคยลงทะเบียนไว้ครั้งแรก และจะทำการย้ายข้อมูลที่อยู่ในข้อมูลการลงทะเบียนมาไว้ในข้อมูลสมาชิก

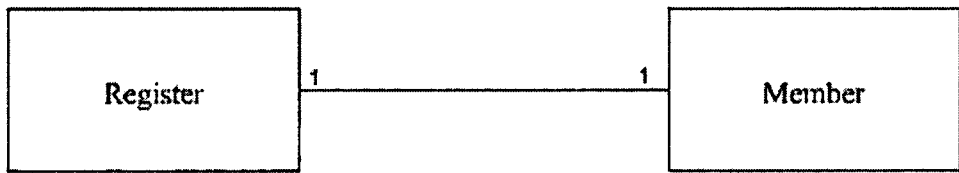
เข้าสู่ระบบ ทำหน้าที่ในการตรวจสอบการเข้าสู่ระบบของผู้ให้บริการจากที่ผู้ให้บริการทำการป้อนข้อมูลเพื่อต้องการเข้าสู่ระบบ โดยทำการตรวจสอบจากข้อมูลสมาชิกว่ามีรหัสผู้ให้บริการกับรหัสผ่านตรงกันหรือไม่ ถ้าตรงกันจึงจะสามารถเข้าสู่ระบบได้

ปรับปรุงแก้ไข ทำหน้าที่ในการแก้ไขหรือปรับปรุงรายละเอียดข้อมูลที่ทำกรลงทะเบียนมาแล้ว โดยผู้ดูแลระบบสามารถที่จะแก้ไขข้อมูลผู้ให้บริการ ทำการลบข้อมูลผู้ให้บริการ หรือ ทำการเพิ่มผู้ให้บริการ

3.6 การออกแบบฐานข้อมูลของระบบงาน

จากการออกแบบภาพรวมของระบบงาน (Context Diagram) และการออกแบบความสัมพันธ์และการไหลของข้อมูลในระบบงาน (Data Flow Diagram) ที่ได้นำเสนอไป สามารถวิเคราะห์ห่ออกแบบความสัมพันธ์ของข้อมูลภายในระบบงาน โดยนำเสนอในลักษณะที่เป็นแผนภาพรวมที่เรียกว่า แบบจำลอง E-R Model ได้ดังรูปที่ 3.5 ซึ่งแผนภาพ E-R Diagram ที่แสดงประกอบไปด้วยความสัมพันธ์ของเอนทิตี (Entity) ต่างๆ ซึ่งสามารถอธิบายรายละเอียดได้ดังนี้

ความสัมพันธ์ระหว่างการลงทะเบียนผู้ให้บริการ กับ สมาชิกผู้ให้บริการ เป็นแบบ one to one โดยสมาชิกจะต้องมีได้ไม่ซ้ำกันเพียงหนึ่งเดียว เมื่อมีข้อมูลสมาชิกข้อมูลในการลงทะเบียนจะถูกย้ายมายังข้อมูลสมาชิก



รูปที่ 3.5 แสดง E-R Diagram ของระบบงาน

เมื่อทำการติดตั้งโปรแกรม NoCat และทำการนำเข้าฐานข้อมูลเข้าสู่ฐานข้อมูล MySQL โดยทำการสร้างคาต้าเบสชื่อ nocat โดยมีตารางฐานข้อมูลมาให้ ทั้งหมด 5 ตาราง และนำมาใช้งานจริงเพียง 1 ตารางเท่านั้นคือ Member และทำการเพิ่มตารางใหม่คือ Register

| ลำดับที่ | ชื่อ Table | รายละเอียด |
|----------|------------|--|
| 1 | Member | เก็บข้อมูลรายละเอียดของผู้ใช้บริการเป็นสมาชิก |
| 2 | Register | เก็บข้อมูลรายละเอียดของ ผู้ใช้บริการทำการลงทะเบียน |

ตารางที่ 3.1 แสดง โครงสร้างและรายละเอียดของ Table Member

| Field | Type | Length | Key | Description |
|-------------|------------------|--------|-----|----------------------------|
| url | varchar | 255 | | ยูอาร์แอล |
| description | text | 255 | | รายละเอียด |
| created | datetime | | | รับการอนุญาตเมื่อไร |
| modified | timestamp | 14 | | ทำการปรับปรุงเมื่อไร |
| status | tinyint unsigned | 3 | | สถานะ |
| login | varchar | 10 | PRI | Login Name ของผู้ให้บริการ |
| pass | varchar | 255 | | รหัสผ่าน |
| name | varchar | 255 | | ชื่อผู้ใช้งาน |

ตารางที่ 3.2 แสดง โครงสร้างและรายละเอียดของ Table Register

| Field | Type | Length | Key | Description |
|------------|---------|--------|-----|----------------------------|
| id | varchar | 10 | PRI | Login Name ของผู้ให้บริการ |
| sex | varchar | 10 | | เพศ |
| fnameth | varchar | 50 | | ชื่อผู้ใช้งานภาษาไทย |
| lnameth | varchar | 50 | | นามสกุลผู้ใช้งานภาษาไทย |
| fnameen | varchar | 50 | | ชื่อผู้ใช้งานภาษาอังกฤษ |
| lnameen | varchar | 50 | | นามสกุลผู้ใช้งานภาษาอังกฤษ |
| birthday | date | | | วันเดือนปีเกิด |
| curriculum | varchar | 10 | | ระดับการศึกษา |
| email | varchar | 50 | | อีเมล |

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

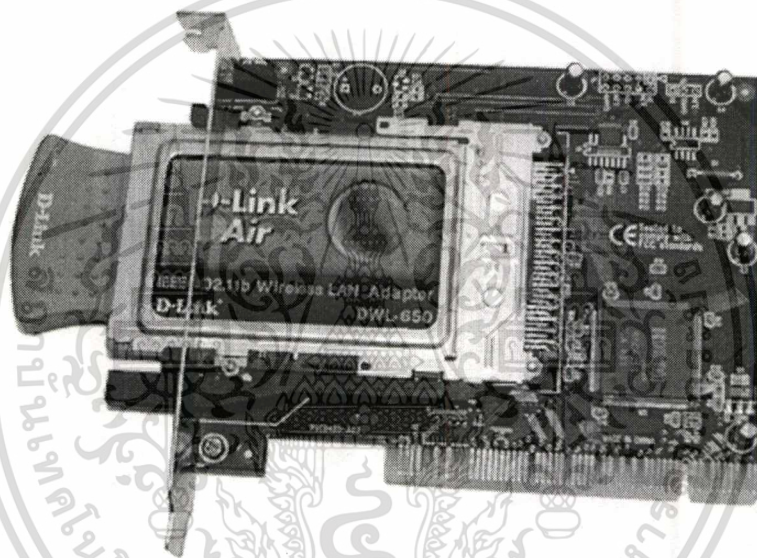
บทที่ 4

การสร้าง ไร้เลสแอกเซสพอยท์

4.1 อุปกรณ์และเครื่องมือที่ต้องใช้

4.1.1 ฮาร์ดแวร์

- การ์ด ไร้เลสแลน D-Link DWL-500 PCMCIA Card PCI ทำ ไร้เลสแอกเซสพอยท์



รูปที่ 4.1 แสดงภาพ D-Link DWL-500

- การ์ดแลน 10/100 1 ใบ
- เครื่องคอมพิวเตอร์ที่ประกอบด้วยฮาร์ดแวร์ CPU Intel Celeron 1.7 GHz หน่วยความจำ 512 MB ฮาร์ดดิสก์ 20 GB

4.1.2 เฟิร์มแวร์

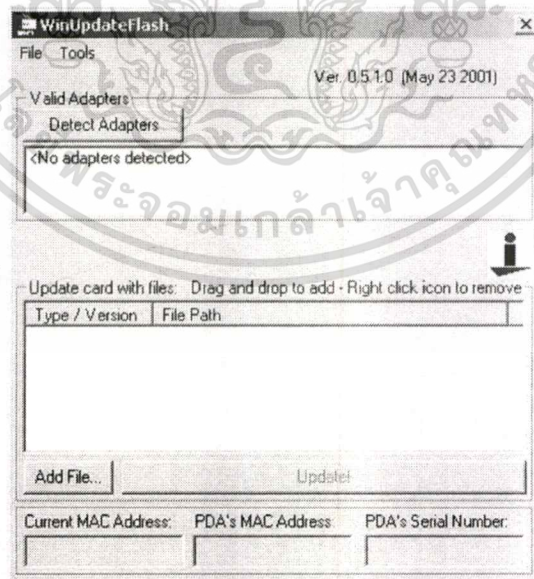
- ซอฟต์แวร์อัปเดตการ์ด ไร้เลสแลน WinUpdate-0-5-1-0.exe
- ไฟล์เฟิร์มแวร์ SF010704.HEX
- ไฟล์เฟิร์มแวร์ PK010101.HEX

4.1.3 ซอฟต์แวร์

- เซิร์ฟเวอร์ ใช้ระบบปฏิบัติการ Linux RedHat 9.0
- ซอฟต์แวร์ไควร์เวอร์ kernel-2.4.20-13.9.HOSTAP.i686.rpm
- เครื่องมือการในการทำบริดจ์ ใช้ bridge-utils-0.9.3-8.rpm
- เครื่องมือการในการทำบริดจ์ ใช้ bridge-utils-devel-0.9.3-8.rpm
- เครื่องมือการในการทำบริดจ์ในแบบ GUI ใช้ gbrctl-0.0-1.i386.rpm

4.2 ขั้นตอนการอัปเดตเฟิร์มแวร์

เฟิร์มแวร์ ที่มากับตัวอุปกรณ์ยังมีปัญหาบางอย่างทำให้เครื่องลูกข่ายไวร์เลสแลนไม่สามารถค้นหา SSID ได้จึงต้องทำการอัปเดตเป็นเวอร์ชัน 1.7.4 ทำการอัปเดตบนวินโดวส์ไฟล์ WinUpdate-0-5-1-0.exe และไฟล์เฟิร์มแวร์ อีกสองไฟล์ ไฟล์ SF010704.HEX กับ PK010101.HEX จากประสบการณ์ในการทำขั้นตอนนี้มีความเสี่ยงมากอาจทำให้อุปกรณ์เสียหายและการอัปเดตเป็นเวอร์ชันที่สูงกว่าเดิมเมื่อมีปัญหาต้องการใช้เวอร์ชันเดิมนั้นทำไม่ได้ จะต้องอัปเดตเป็นเวอร์ชันที่สูงกว่าตลอด และสิ่งที่สำคัญในการทำ จะต้องทำการถอนการติดตั้งไดร์เวอร์การ์ดไวร์เลสแลน อันอื่นออกให้หมด ให้ทำการอัปเดตที่ละใบ



รูปที่ 4.2 แสดงภาพ WinUpdate-0-5-1-0

4.3 การติดตั้งซอฟต์แวร์ HostAP

ซอฟต์แวร์ HostAP เป็น Opensource สามารถนำมาใช้งานได้โดยไม่ต้องเสียค่าใช้จ่าย ลิขสิทธิ์แต่มีข้อจำกัดที่ฮาร์ดแวร์ต้องเป็นชิปเซต Intersil Prism2/2.5/3 เท่านั้น รายละเอียดตรวจสอบได้ที่ภาคผนวก เมื่อทำการติดตั้ง Linux Redhat 9 แล้ว ให้ทำการตรวจสอบ Services ดังต่อไปนี้ที่จำเป็นต้องทำงาน Pcmcia = PCMCIA monitor daemon ติดตั้งซอฟต์แวร์ HostAP

ใช้คำสั่งดังนี้ # rpm -ivh kernel-2.4.20-13.9.HOSTAP.i686.rpm

เมื่อติดตั้งเสร็จแล้วให้ทำการโหลดระบบปฏิบัติการใหม่ เมื่อถึงหน้าจอเมนู GRUB ให้เลือกเมนู RedHat Linux (2.4.20-13.9.HOSTAP) เพื่อเข้าสู่ระบบปฏิบัติการ linux เสร็จแล้วจึงทำการสร้างไฟล์ชื่อ hostap_cs.conf ไปยัง Directory /etc/pcmcia/ จะเป็นไฟล์กำหนดไดรเวอร์ของการ์ดไวร์เลสแลนที่สามารถนำมาใช้งานทำเป็นไวร์เลสแอสเซสซมยท์ได้โดยมีข้อความดังนี้

```
device "hostap_cs"
  class "network" module "hostap_crypt", "hostap", "hostap_cs"

card "Intersil PRISM2 Reference Design 11Mb/s WLAN Card"
  version "INTERSIL", "HFA384x/IEEE"
  bind "hostap_cs"

card "Linksys WPC11 Ver 3 11Mbps WLAN Card"
  manfid 0x0274, 0x1613
  bind "hostap_cs"

card "D-Link DWL-650 11Mbps WLAN Card"
  version "D", "Link DWL-650 11Mbps WLAN Card", "Version 01.02"
  bind "hostap_cs"

# Optional configuration parameters for hostap_cs.o
# module "hostap_cs" opts "channel=3 iw_mode=3 essid=test ignore_cis_vcc=0"
```

ตรวจสอบไวร์เลสแอสเซสซมยท์ HOSTAP ว่าทำงานหรือไม่โดยใช้คำสั่งนี้ # dmesg | more ทำ
เอกสารนี้ค้นหาข้อความ ดังนี้ สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

hostap_crypt: registered algorithm 'NULL'
hostap_cs: 0.0.3 - 2003-05-18 (Jouni Malinen <jkmaline@cc.hut.fi>)
hostap_cs: setting Vcc=33 (constant)
hostap_cs: CS_EVENT_CARD_INSERTION
prism2_config()
hostap_cs: setting Vcc=50 (from config)
Checking CFTABLE_ENTRY 0x01 (default 0x01)
IO window settings: cfg->io.nwin=1 dflt.io.nwin=1
io->flags = 0x0046, io.base=0x0000, len=64
hostap_cs: index 0x01: Vcc 5.0, irq 11, io 0x0100-0x013f
divert: allocating divert_blk for wlan0
hostap_cs: Registered netdevice wlan0
prism2_hw_init()
prism2_hw_init: initialized in 17391 iterations
wlan0: NIC: id=0x801b v1.0.0
wlan0: PRI: id=0x15 v1.1.0
wlan0: STA: id=0x1f v1.4.2
    
```

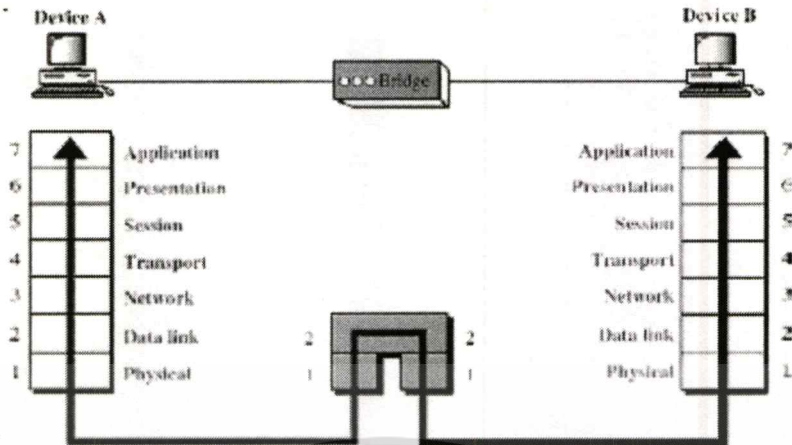
ทำการตรวจสอบโมดูลโดยใช้คำสั่ง # lsmod ดูโมดูลเหล่านี้ทั้ง ห้า โมดูล ปรากฏมาให้เห็นจึงจะสามารถใช้งานได้

| Module | Size | Used by | Not tainted |
|--------------|-------|---------|-----------------------------|
| hostap_cs | 53932 | 1 | |
| hostap | 86148 | 0 | [hostap_cs] |
| hostap_crypt | 2992 | 0 | [hostap] |
| ds | 8680 | 1 | [hostap_cs] |
| pcmcia_core | 57216 | 0 | [hostap_cs ds yenta_socket] |

4.4 การติดตั้งซอฟต์แวร์ บริดจ์

บริดจ์ (bridge) เป็นอุปกรณ์เครือข่ายที่ทำหน้าที่เชื่อมต่อเครือข่ายย่อยสองเครือข่ายเข้าด้วยกัน บริดจ์จะทำงานในระดับชั้นเดทาลิงก์ จึงสามารถเชื่อมต่อเครือข่ายประเภทเดียวกันหรือต่างกันเข้า

ด้วยกันได้ แบบจำลองการทำงานของบริดจ์จะแสดงได้ดังรูปที่ 4.2



รูปที่ 4.3 แสดงภาพ แบบจำลองการทำงานของบริดจ์

ที่ระดับชั้นเดทาลิงก์ การทำงานของชั้นนี้จะรับข้อมูลที่ส่งลงมาจากระดับชั้นเน็ตเวิร์ก แล้วทำการเพิ่ม Header ของตัวเองเข้าไปก่อนที่จะส่งลงไปที่ระดับชั้นฟิสิคัลเพื่อส่งออกไปทางการ์ดเน็ตเวิร์ก เมื่อข้อมูลถูกส่งไปถึงบริดจ์ บริดจ์จะทำงานที่ระดับชั้นเดทาลิงก์ นั่นคือจะส่งผ่านข้อมูลจากชั้นล่างสุดขึ้นไปเรื่อยๆ พร้อมทั้งทำการถอด Header ของแต่ละชั้นไปด้วย (Decapsulate) จนถึงระดับชั้นเดทาลิงก์ แล้วจึงตรวจสอบว่า MAC Address ของเครือข่ายปลายทางที่ระบุมาในเฟรมนั้นใช่เครือข่ายที่อยู่อีกอินเทอร์เฟซหนึ่งหรือไม่ ถ้าใช่ ก็จะมีการ Encapsulate ใหม่อีกครั้งด้วยสภาพแวดล้อมของเครือข่ายปลายทาง แล้วจึงส่งข้อมูลไปยังเครือข่ายปลายทาง

ทำการติดตั้ง บริดจ์ ทั้งหมด สาม ไฟล์ ด้วยคำสั่งดังนี้

```
# rpm -ivh bridge-utils-0.9.3-8.rpm
# rpm -ivh bridge-utils-devel-0.9.3-8.rpm
# rpm -ivh gbrctl-0.0-1.i386.rpm
```

ทำการตรวจสอบ โมดูลทำงานหรือไม่ ด้วยคำสั่ง # lsmod

| Module | Size | Used by | Not tainted |
|--------|-------|---------|-------------|
| bridge | 24764 | 1 | (autoclean) |

ขั้นตอนการสร้างไฟล์ให้โปรแกรมทำงานทุกครั้งเมื่อเปิดระบบ โดยเข้าไปเพิ่มคำสั่งในไฟล์ /etc/rc.local คำสั่งดังนี้

```
#!/bin/sh

# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local

ifconfig eth0 down

ifconfig wlan0 down

ifconfig br0 down

ifconfig eth0 0.0.0.0 up

ifconfig wlan0 0.0.0.0 up

brctl addbr br0

brctl addif br0 eth0

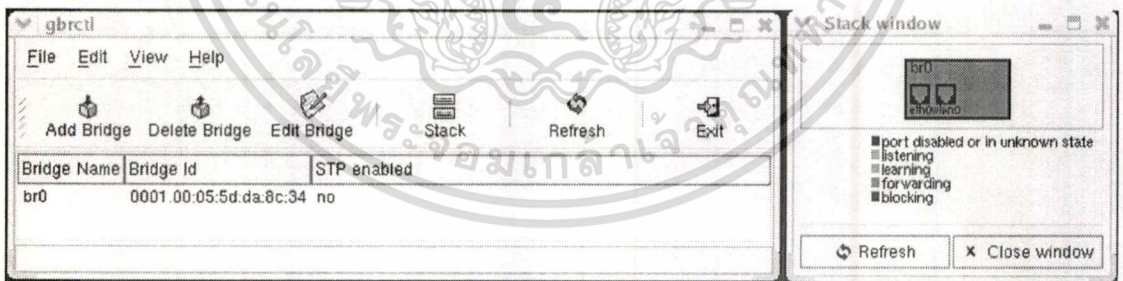
brctl addif br0 wlan0

brctl stp br0 off

ifconfig br0 0.0.0.0 up

iwconfig wlan0 essid hostap channel 3
```

ทำการตรวจสอบโดยให้คำสั่ง #gbrctl



รูปที่ 4.4 แสดงภาพ การทำงานของบริดจ์

คำสั่งตรวจสอบไวร์เลสแอสเซทพอยท์ ดังนี้

```
[root@hostap root]# ifconfig

br0    Link encap:Ethernet HWaddr 00:05:5D:DA:8C:34

        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

        RX packets:65 errors:0 dropped:0 overruns:0 frame:0
```

เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์และเผยแพร่โดยทางทีมงาน ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

TX packets:0 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:8392 (8.1 Kb) TX bytes:0 (0.0 b)

eth0 Link encap:Ethernet HWaddr 00:0C:6E:E8:3A:E2

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:9 errors:0 dropped:0 overruns:0 frame:0

TX packets:261 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:100

RX bytes:1420 (1.3 Kb) TX bytes:20802 (20.3 Kb)

Interrupt:5 Base address:0x8800

wlan0 Link encap:Ethernet HWaddr 00:05:5D:DA:8C:34

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:130 errors:0 dropped:14 overruns:0 frame:0

TX packets:327 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:100

RX bytes:16426 (16.0 Kb) TX bytes:37195 (36.3 Kb)

Interrupt:10 Base address:0x100

[root@hostap root]# iwconfig wlan0

wlan0 IEEE 802.11b ESSID:"hostap"

Mode:Master Frequency:2.422GHz Access Point: 00:05:5D:DA:8C:34

Bit Rate:11Mb/s Tx-Power:-2 dBm Sensitivity=1/3

Retry min limit:8 RTS thr:off Fragment thr:off

Encryption key:off

Power Management:off

Link Quality:0 Signal level:0 Noise level:0

Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0

Tx excessive retries:0 Invalid misc:0 Missed beacon:0

เอกสารนี้เป็นเอกสารของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
[root@hostap root]# iwlist wlan0 freq
```

```
wlan0 14 channels in total; available frequencies :
```

```
Channel 01 : 2.412 GHz
```

```
Channel 02 : 2.417 GHz
```

```
Channel 03 : 2.422 GHz
```

```
Channel 04 : 2.427 GHz
```

```
Channel 05 : 2.432 GHz
```

```
Channel 06 : 2.437 GHz
```

```
Channel 07 : 2.442 GHz
```

```
Channel 08 : 2.447 GHz
```

```
Channel 09 : 2.452 GHz
```

```
Channel 10 : 2.457 GHz
```

```
Channel 11 : 2.462 GHz
```

```
Channel 12 : 2.467 GHz
```

```
Channel 13 : 2.472 GHz
```

```
Current Frequency:2.422GHz (channel 03)
```

```
[root@hostap root]#
```

```
[root@hostap root]# iwspy wlan0
```

```
wlan0 Statistics collected:
```

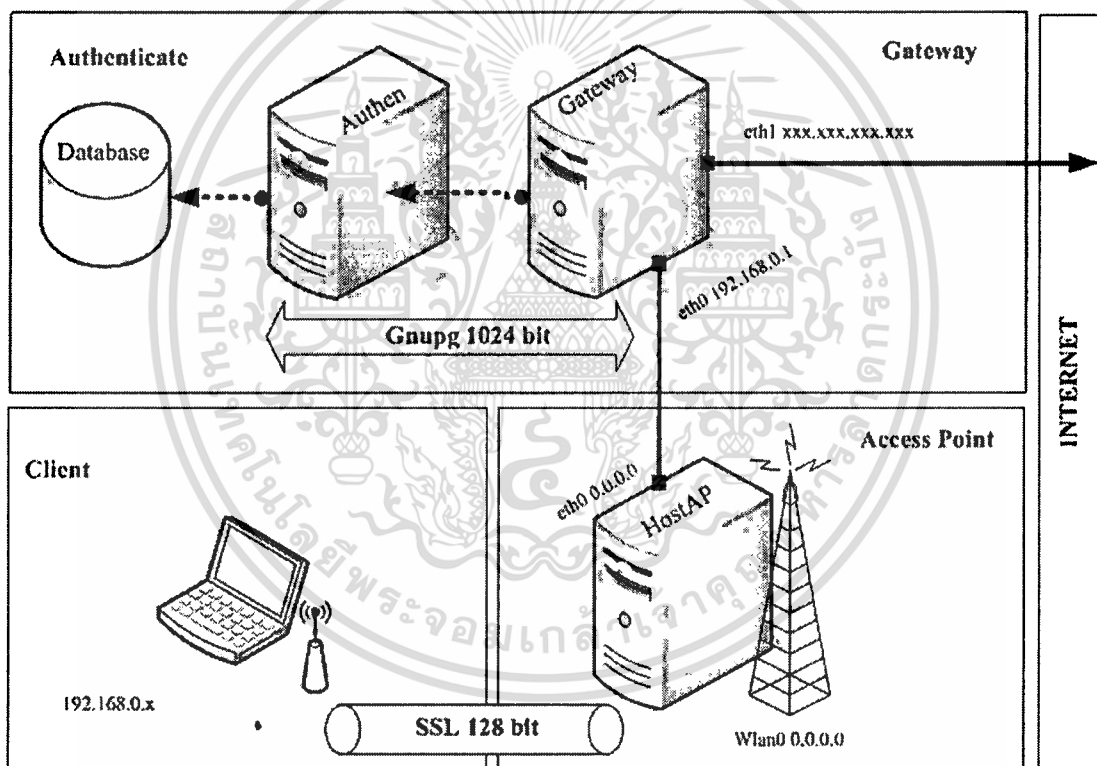
```
00:06:25:18:82:83 : Quality:254/92 Signal level:-85 dBm Noise level:-98 dBm (updated)
```

```
typical/average : Quality:0 Signal level:0 Noise level:0
```

บทที่ 5

การพิสูจน์ตัวตนจริงและเกตเวย์

ใช้ ซอฟต์แวร์ NoCat เป็นเครื่องมือทำหน้าที่หลัก สอง ส่วน คือทำหน้าที่เป็นตัวกลางพิสูจน์ตัวตนจริงและทำหน้าที่เป็น เกตเวย์ แต่การทำงานสามารถแยกออกจากกันเป็น สอง ส่วนได้ ส่วนที่ทำนี้จะทำการร่วมทั้งส่วนไว้ในเครื่องคอมพิวเตอร์เดียวกัน



รูปที่ 5.1 แสดงภาพ ของการทำการระบบการพิสูจน์ตัวตนจริงกับเกตเวย์

5.1 อุปกรณ์และเครื่องมือที่ต้องใช้

5.1.1 ซอฟต์แวร์

- เซิร์ฟเวอร์ ใช้ระบบปฏิบัติการ Linux RedHat 9.0
- เครื่องมือการพิสูจน์ตัวตนจริงและเกตเวย์ ใช้ NoCatAuth-0.82.tar.gz

เอกสารนี้เป็นเอกสารลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ห้ามมิให้คัดลอกหรือเผยแพร่โดยไม่ได้รับอนุญาตให้ไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

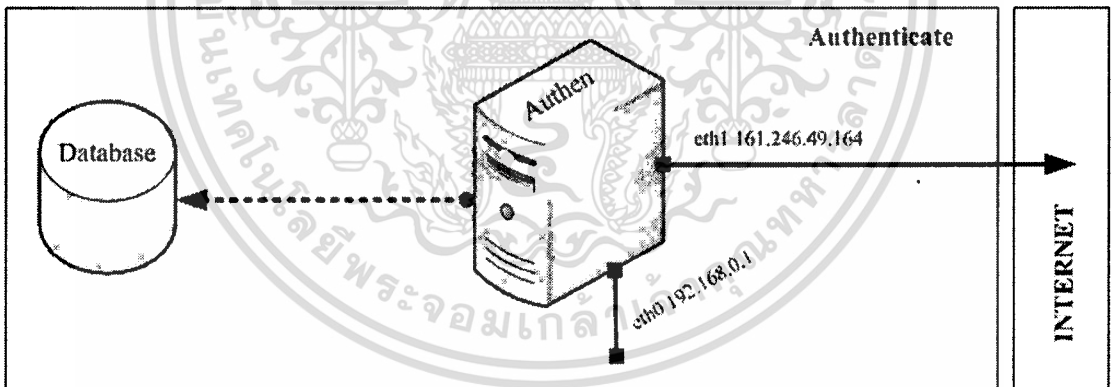
- เครื่องมือการในการทำ NAT ใช้ iptables 1.2.7a-2
- เครื่องมือการในการแจกไอพีอัตโนมัติ ใช้ Dhcp 3.0pl1-23
- เว็บเซิร์ฟเวอร์และการเข้ารหัสความปลอดภัยใช้โปรแกรม Apache-2.0.40-21+mod_ssl-2.0.40-21
- ภาษาที่ใช้ในการพัฒนาแอปพลิเคชัน ใช้ Perl 5.8.0-88
- ดาต้าเบสของระบบ ใช้ MySQL 3.23.54a

5.1.2 ฮาร์ดแวร์

- เครื่องคอมพิวเตอร์ที่ประกอบด้วยฮาร์ดแวร์ CPU Intel Pentium 4 2.4 GHz หน่วยความจำ 512 MB ฮาร์ดดิสก์ 20 GB
- การ์ดแลน 10/100 2 ใบ

5.2 ขั้นตอนการติดตั้ง

เมื่อติดตั้ง linux redhat 9 แล้วให้ทำการตรวจสอบการให้บริการ Service เหล่านี้ httpd dhcpd iptables ipchains และ mysqld แล้วทำการกำหนดค่า IP Address รูปที่ 5.1



รูปที่ 5.2 แสดงภาพ การกำหนด IP Address eth1 และ eth0

| | |
|--|--|
| <pre> DEVICE=eth0 BOOTPROTO=static BROADCAST=192.168.0.255 IPADDR=192.168.0.1 NETMASK=255.255.255.0 NETWORK=192.168.0.0 </pre> | <pre> DEVICE=eth1 BOOTPROTO=dhcp ONBOOT=yes </pre> |
|--|--|

| | |
|------------|--|
| ONBOOT=yes | |
|------------|--|

5.2.1 การกำหนด DHCP ให้กับเครื่องลูกข่าย

เป็นการกำหนด IP Address ให้กับเครื่องลูกข่ายอัตโนมัติ โดยที่เครื่องลูกข่ายจะทำการร้องขอจาก DHCP Server ที่ให้บริการ ในการตั้งค่านั่นทำโดยการสร้างไฟล์ /etc/dhcpd.conf มีค่าดังนี้

```
# /etc/dhcpd.conf
DHCPDARGS=eth0;
ddns-update-style ad-hoc;
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.0.255;
option routers 192.168.0.1;
option domain-name-servers 161.246.38.21;
subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.10 192.168.0.50;
}
```

ทำการเริ่มการทำงานของ DHCP ด้วยคำสั่ง

```
#/etc/rc.d/init.d/dhcp start
```

ตรวจสอบค่าให้ DHCP ทำงานโดยอัตโนมัติโดยพิมพ์คำสั่ง setup แล้วทำเครื่องหมายหน้า dhcpd แล้วทำการ Reboot เครื่องคอมพิวเตอร์ใหม่

5.2.2 ขั้นตอนการติดตั้ง NoCatAuth

ในการติดตั้งซอฟต์แวร์ทั้งหมดให้ทำสำเนาเอาไว้ในห้อย /usr/local/src ในการติดตั้งซอฟต์แวร์ NoCatAuth ในบทยี่ต้องการสร้างการพิสูจน์ตัวตนจริงและเกตเวย์ อยู่ในคอมพิวเตอร์เครื่องเดียวกันจึงมีขั้นตอนการติดตั้งดังนี้

```
# tar xfvz NoCatAuth-0.82.tar.gz
```

```
# cd NoCatAuth-0.82
```

```
# make PREFIX=/usr/local/nocat/gateway gateway
```

```
# make PREFIX=/usr/local/nocat/authserv
```

```
# make PREFIX=/usr/local/nocat pgpkey
# cp /usr/local/nocat/trustedkeys.gpg /usr/local/nocat/gateway/pgp
# chown -R apache:apache /usr/local/nocat/pgp
```

ตรวจสอบการทำงานของ NoCatAuth ใช้คำสั่งดังนี้

```
# cd /usr/local/nocat
# vi nocat.conf
# bin/gateway
```

```
[2004-01-12 17:35:13] Resetting firewall.
```

```
[2004-01-12 17:35:13] Detected InternalDevice 'eth0'
```

```
[2004-01-12 17:35:13] Detected ExternalDevice 'eth1'
```

```
[2004-01-12 17:35:13] Detected LocalNetwork '192.168.0.0/255.255.255.0'
```

```
[2004-01-12 17:35:15] Binding listener socket to 0.0.0.0
```

การตั้งค่าอัตโนมัติเมื่อทำการเปิดระบบปฏิบัติการลินุกซ์ NoCatAuth จะทำงานไปพร้อมกันตอนทำการเปิดระบบ

```
#cp /usr/local/src/ NoCatAuth-0.82/etc/nocat.rc /etc/rc.d/init.d/nocat
```

```
# pico /etc/rc.d/nocat
```

ทำการแก้ไขไฟล์ดังนี้ NC=/usr/local/nocat/gateway แล้วทำการบีนที่ก

```
# ln -s /etc/rc.d/init.d/nocat.rc /etc/rc.d/rc3.d/S99nocat
```

หรือ ใน Mode Graph

```
# ln -s /etc/rc.d/init.d/nocat.rc /etc/rc.d/rc5.d/S99nocat
```

ขั้นต่อไปทำการ แก้ไขไฟล์ /usr/local/nocat/nocat.conf

```
#### authserv.conf -- NoCatAuth Authentication Service Configuration.
```

| | |
|--------------|--------------------------|
| Verbosity | 10 |
| HomePage | http://192.168.0.1/ |
| DocumentRoot | /usr/local/nocat/htdocs |
| DataSource | DBI |
| Database | dbi:mysql:database=nocat |
| DB_User | root |

และ /usr/local/nocat/gateway/nocat.conf

```
##### gateway.conf -- NoCatAuth Gateway Configuration.
```

```

Verboisity    10
GatewayName   Wireless IT.KMITL
GatewayMode   Passive
GatewayLog    /usr/local/nocat/gateway/nocat.log
LoginTimeout  600
HomePage      http://192.168.0.1/
DocumentRoot  /usr/local/nocat/gateway/htdocs
AuthServiceAddr 192.168.0.1
AuthServiceURL https://$AuthServiceAddr/cgi-bin/login
LogoutURL     https://$AuthServiceAddr/logout.html
ExternalDevice eth1
InternalDevice eth0
LocalNetwork  192.168.0.0/24
ExcludePorts  25

```

รายละเอียดมากกว่านี้ตรวจสอบได้ที่ภาคผนวก

5.2.3 ขั้นตอนการติดตั้งฐานข้อมูล MySQL

โดยการจัดเก็บฐานข้อมูลลงบน MySQL ด้วยคำสั่ง `# mysql nocat < /etc/nocat.schema` ในห้องที่ทำการแตกไฟล์ต้นฉบับ NoCatAuth-0.82

5.2.4 ขั้นตอนการติดตั้ง iptables

ใน Linux RedHat 9 นั้นมี Iptables มาให้แล้ว ใช้คำสั่งตรวจสอบ `# iptables -L`

```

Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination

```

โดยไม่ต้องกำหนดค่านี้ `echo "1" > /proc/sys/net/ipv4/ip_forward` เมื่อ NoCatAuth ทำงาน

จะทำการกำหนด Firewall rule และ `echo "1" > /proc/sys/net/ipv4/ip_forward` ให้อัตโนมัติ

เอกสารนี้เป็นลิขสิทธิ์ของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง การนำเอกสารนี้ไปใช้โดยไม่ได้รับอนุญาตถือว่าผิดกฎหมาย การนำเอกสารนี้ไปใช้โดยไม่ได้รับอนุญาตถือว่าผิดกฎหมาย การนำเอกสารนี้ไปใช้โดยไม่ได้รับอนุญาตถือว่าผิดกฎหมาย

เมื่อได้ติดตั้งเสร็จเรียบร้อยแล้ว ทำการตรวจสอบ # iptables -L จะได้ค่าดังนี้

```
[root@authen root]# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination
NoCat all -- anywhere anywhere

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

Chain NoCat (1 references)
target prot opt source destination
NoCat_Ports all -- anywhere anywhere
NoCat_Inbound all -- anywhere anywhere
ACCEPT all -- 192.168.0.0/24 anywhere MARK match 0x1
ACCEPT all -- 192.168.0.0/24 anywhere MARK match 0x2
ACCEPT all -- 192.168.0.0/24 anywhere MARK match 0x3
ACCEPT tcp -- 192.168.0.0/24 192.168.0.1 tcp dpt:http
ACCEPT tcp -- 192.168.0.1 192.168.0.0/24 tcp spt:http
ACCEPT tcp -- 192.168.0.0/24 192.168.0.1 tcp dpt:https
ACCEPT tcp -- 192.168.0.1 192.168.0.0/24 tcp spt:https
ACCEPT all -- platinum.it.kmitl.ac.th 192.168.0.0/24
ACCEPT tcp -- 192.168.0.0/24 platinum.it.kmitl.ac.th tcp dpt:domain
ACCEPT udp -- 192.168.0.0/24 platinum.it.kmitl.ac.th udp dpt:domain
DROP tcp -- !192.168.0.1 anywhere tcp dpt:5280
DROP all -- anywhere anywhere
```

Chain NoCat_Inbound (1 references)

เอกสารนี้เป็นเอกสารลิขสิทธิ์ของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านอื่น

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

| target | prot opt source | destination | |
|----------------------------------|-----------------|-------------|-----------------------------|
| Chain NoCat_Ports (1 references) | | | |
| target | prot opt source | destination | |
| DROP | tcp -- anywhere | anywhere | tcp dpt:smtp MARK match 0x3 |
| DROP | udp -- anywhere | anywhere | udp dpt:smtp MARK match 0x3 |

5.2.5 ขั้นตอนการติดตั้ง Apache กับ mod_ssl

apache ทำหน้าที่ให้บริการเว็บเซิร์ฟเวอร์ ส่วน mod_ssl เป็นเครื่องมือรักษาความปลอดภัยระหว่างเบราว์เซอร์กับเครื่องแม่ข่ายเว็บ ทำการเข้ารหัสรักษาความปลอดภัย 128 บิต ส่วนใน ลินุกซ์ RedHat 9 นั้นมี Apache กับ mod_ssl อยู่แล้ว ให้ทำการเปิดไฟล์ /etc/httpd/conf/httpd.conf ทำการเพิ่มคำสั่งนี้ Include /usr/local/nocat/httpd.conf แล้วทำการบันทึก Restart httpd ใหม่เพื่อให้ระบบทำงานด้วยคำสั่ง # /etc/rc.d/init.d/httpd restart

บทที่ 6

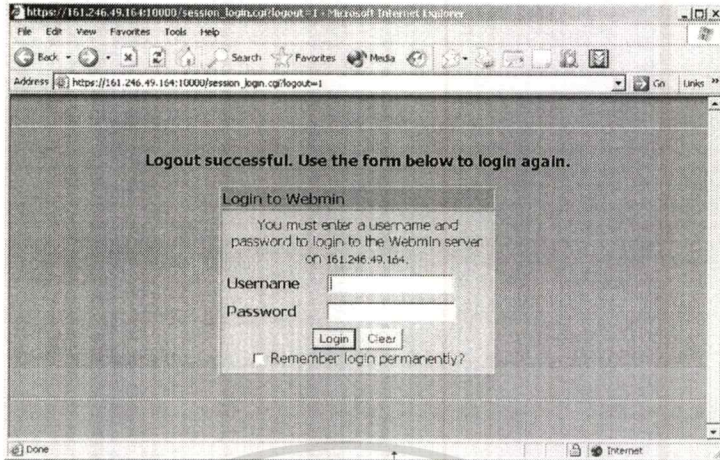
การพัฒนาระบบ

6.1 ซอฟต์แวร์ที่ใช้ในส่วนของการพัฒนาระบบ มีดังนี้

- ภาษาที่ใช้ในการพัฒนาแอปพลิเคชัน ใช้ Php 4..2.2-17
- ภาษาที่ใช้ในการพัฒนาแอปพลิเคชัน ใช้ Perl 5.8.0-88
- เครื่องมือการส่งเมลระบบปฏิบัติการลินุกซ์ Sendmail 8.12.8-4
- ดาต้าเบสของระบบ ใช้ MySQL 3.23.54a
- เครื่องมือในการจัดการระบบผ่านเว็บเบราว์เซอร์และการเข้ารหัสความปลอดภัย webmin-1.121-1.noarch.rpm + Net_SSLeay.pm-1.23.tar.gz
- โมดูล nocat-0.50.wbm+nocat-0.51.wbm
- เครื่องมือจัดการดาต้าของระบบแบบ GUI MySQL-Front-3 Beta
- Editor Coding Program ใช้ Edits Plus 2.1 Allaire HomeSite 4.5
- เครื่องมือการรับส่งข้อมูลยังเซิร์ฟเวอร์ SSHSecureShellClient-3.2.3.exe
- โปรแกรมเบราว์เซอร์ ใช้ Internet Explorer 6.0

6.2 การติดตั้งซอฟต์แวร์ Webmin

ทำการติดตั้ง webmin-1.121-1.noarch.rpm ด้วยคำสั่ง # rpm -ivh webmin-1.121-1.noarch.rpm ทำการลอกอินเข้า webmin ที่ <http://19.168.0.1:10000> หรือ <http://161.246.49.164:10000> รูปที่ 6.1

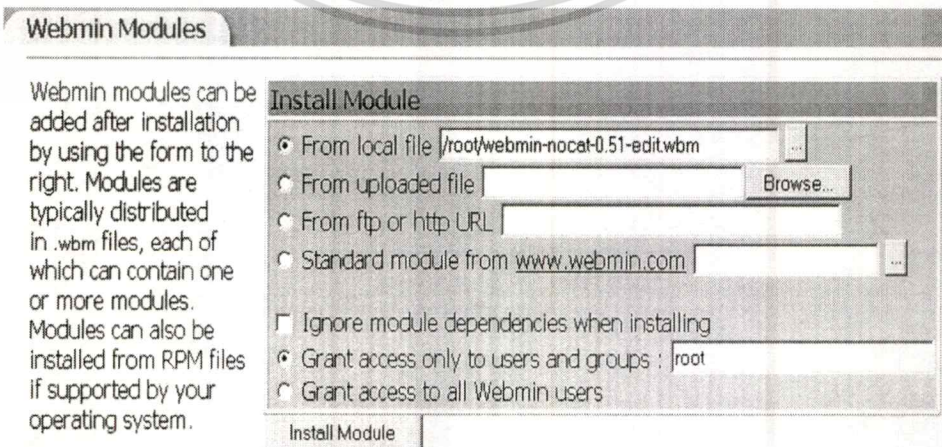


รูปที่ 6.1 แสดงหน้าจอล็อกอิน Webmin

ทำการติดตั้ง Net_SSLeay.pm-1.23.tar.gz เพื่อเป็นการเข้ารหัสความปลอดภัย SSL 128 บิต ด้วยคำสั่งดังนี้

```
# tar xvfz Net_SSLeay.pm-1.23.tar.gz
# cd Net_SSLeay.pm-1.23
# perl Makefile.PL /usr
# make install
```

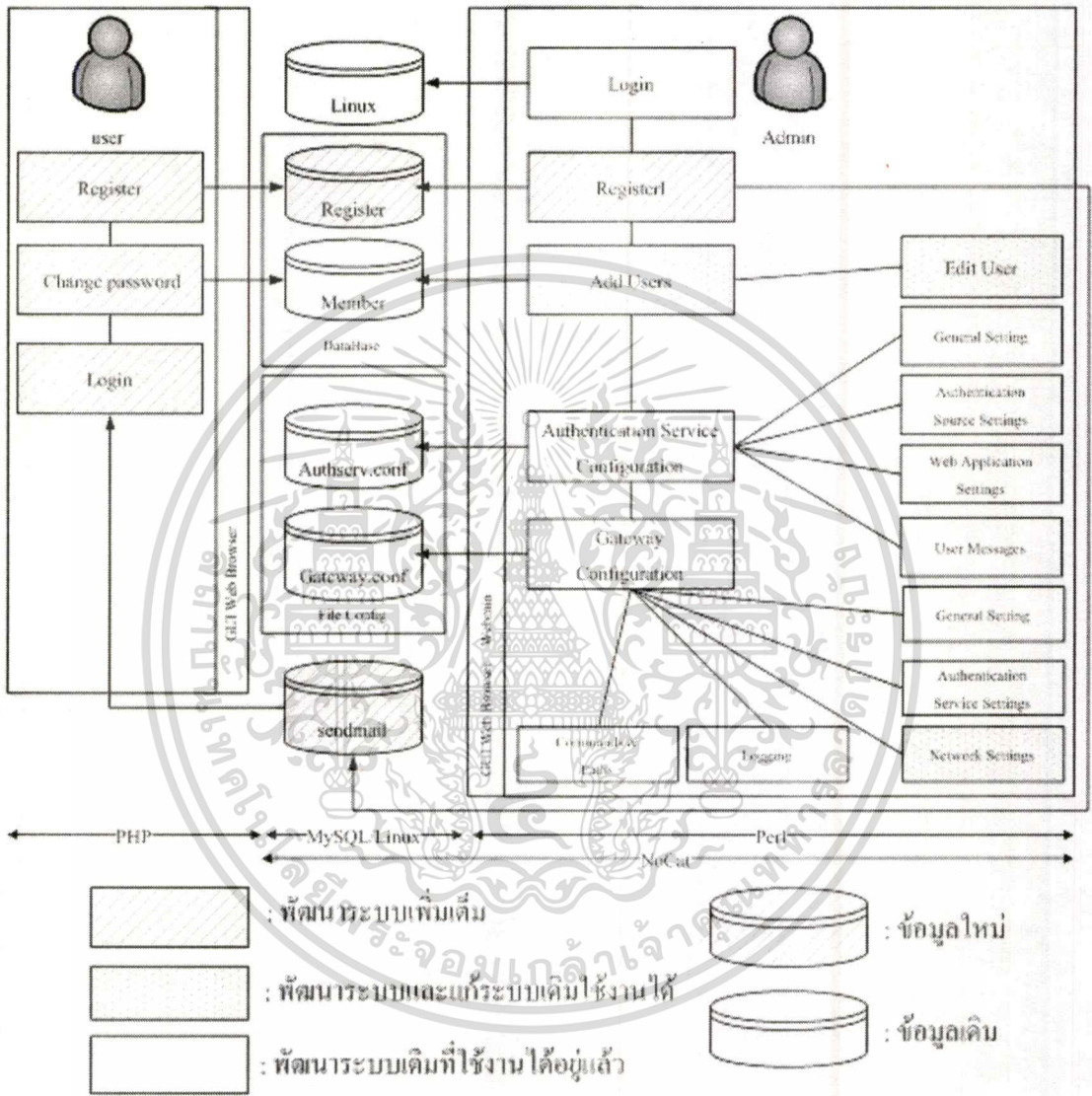
ทำการตรวจสอบด้วยคำสั่งนี้ #perl -e 'use Net::SSLeay' ถ้าใช้งานได้จะต้องไม่อะไรขึ้นมา แสดง ต่อไปให้เข้ายังหน้าจอ Webmin Configuration ทำการเปิดใช้งาน SSL เสร็จเข้าหน้าจอ Webmin Modules เพื่อทำการติดตั้ง nocat-0.50.wbm และ nocat-0.51.wbm ดังรูปที่ 6.2



เอกสารนี้เป็นเอกสารรูปที่ 6.2 แสดงการติดตั้งโมดูล nocat-0.50.wbm และ nocat-0.51.wbm ระโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.3 โครงสร้างและการพัฒนาระบบ

การพัฒนาแบ่งเป็นสองส่วน คือ ส่วนของผู้ดูแลระบบกับส่วนของผู้ใช้ ดังรูปที่ 6.3



รูปที่ 6.3 แสดงการทำงานและการพัฒนาระบบงาน

ในส่วนของการพัฒนาระบบเพิ่มเติมนั้นใช้ภาษา PHP ในการทำหน้าที่ให้ผู้ใช้ทำการลงทะเบียน เปลี่ยนรหัสผ่าน และหน้าจอลงทะเบียนผ่านเว็บเบราว์เซอร์ และทำการสร้างฐานข้อมูลเพิ่มเติมอีก หนึ่งตารางทำหน้าที่เก็บข้อมูลการลงทะเบียนสมัครขอใช้งานระบบ ทำการส่งรหัสผ่านให้แก่ผู้ใช้ทางเมล์ สำหรับผู้ดูแลระบบพัฒนาโดยนำเครื่องมือการจัดการลินุกซ์ผ่านเว็บเบราว์เซอร์ที่ชื่อว่าโปรแกรมเวบบิน โดยการใช้ภาษา Perl ทำการเขียนเป็นโมดูลสำหรับผู้ดูแลระบบใช้

ตรวจสอบการลงทะเบียนของผู้ใช้งานเมื่อผู้ดูแลระบบอนุญาตจะทำการส่งคำรหัสผ่านไปทางเมลที่ผู้ใช้ทำการป้อนข้อมูลลงทะเบียนครั้งแรก

ในส่วนของการแก้ไขให้ใช้งานได้นั้น ได้ทำการนำโมดูลของ Nocat เวอร์ชัน 0.50 กับ 0.51 ในส่วนที่ใช้งานได้ไม่มีปัญหาสร้างเป็นเวอร์ชันใหม่ ผสมกับการเพิ่มเติมข้างต้นที่ได้กล่าวมานั้น มาทำเป็น โมดูล เพื่อความสะดวกในการติดตั้งในครั้งต่อไป

6.3.1 ส่วนของผู้ดูแลระบบ Admin

จากขั้นตอนการตั้งโมดูล nocat-0.50.wbm และ nocat-0.51.wbm นั้นยังไม่สามารถใช้งานได้ ต้องทำการแก้ไขและเพิ่มเติมส่วนยังไม่มี โดยการทำข้อคิดและข้อเสียที่สองโมดูลมารวมกันทำให้ดีขึ้นแล้วทำการเพิ่มส่วนของการ register เพื่อให้ผู้ดูแลระบบทำการตรวจสอบการลงทะเบียนของผู้ใช้แล้วทำการส่งรหัสผู้ใช้งานกับรหัสผ่านไปยังผู้ใช้ทางเมล ตอนนี้จะมีสถานะสามสถานะคือ อนุญาต ลบทิ้งและเก็บไว้ ในส่วนนี้ใช้ภาษา Perl เป็นภาษาในการพัฒนา ใช้ฐานข้อมูล MySQL

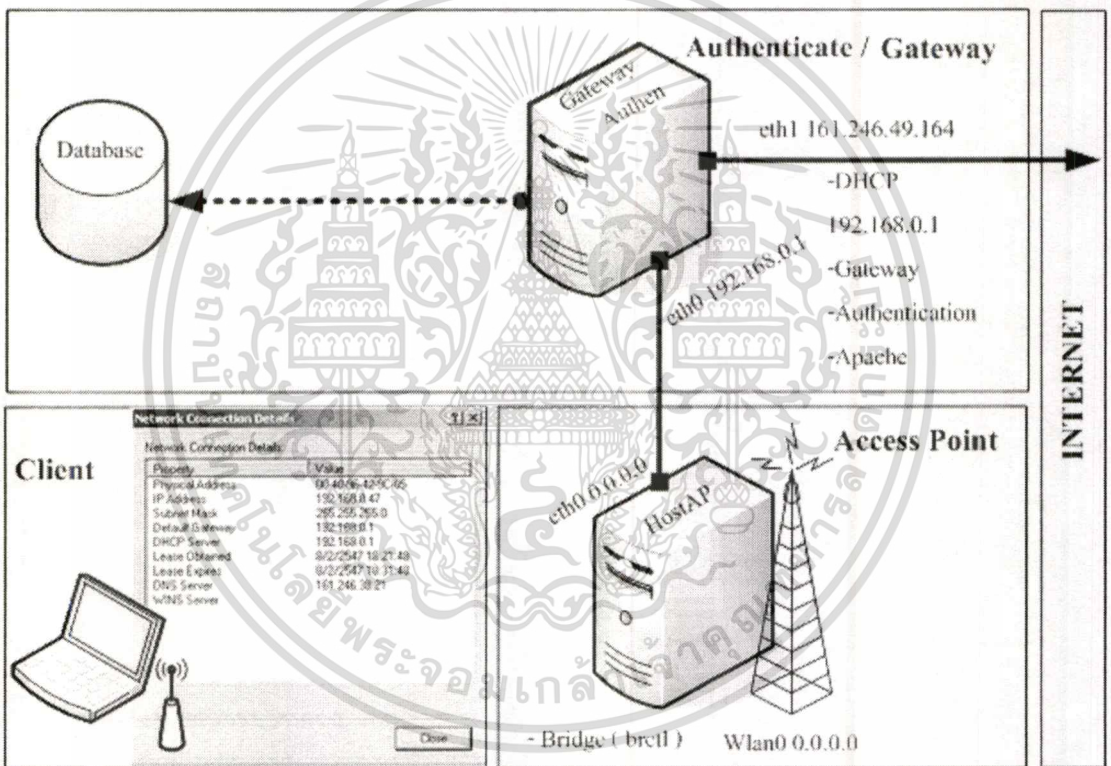
6.3.1 ส่วนของผู้ใช้ User

ส่วนนี้ได้ทำการพัฒนาด้วยภาษา Php ทำการพัฒนาเพิ่มสำหรับให้ผู้ใช้ ทำการลงทะเบียนขอใช้งานอินเทอร์เน็ต การเปลี่ยนแปลงรหัสผ่าน และการล็อกอินเข้าใช้ระบบ

บทที่ 7

ผลการทดลอง

เนื้อหาในบทนี้จะกล่าวถึง การทดสอบใช้งานระบบไวร์เลสแอสเซสพอยท์ รายละเอียดการทดสอบใช้งานนำเสนอ ดังนี้

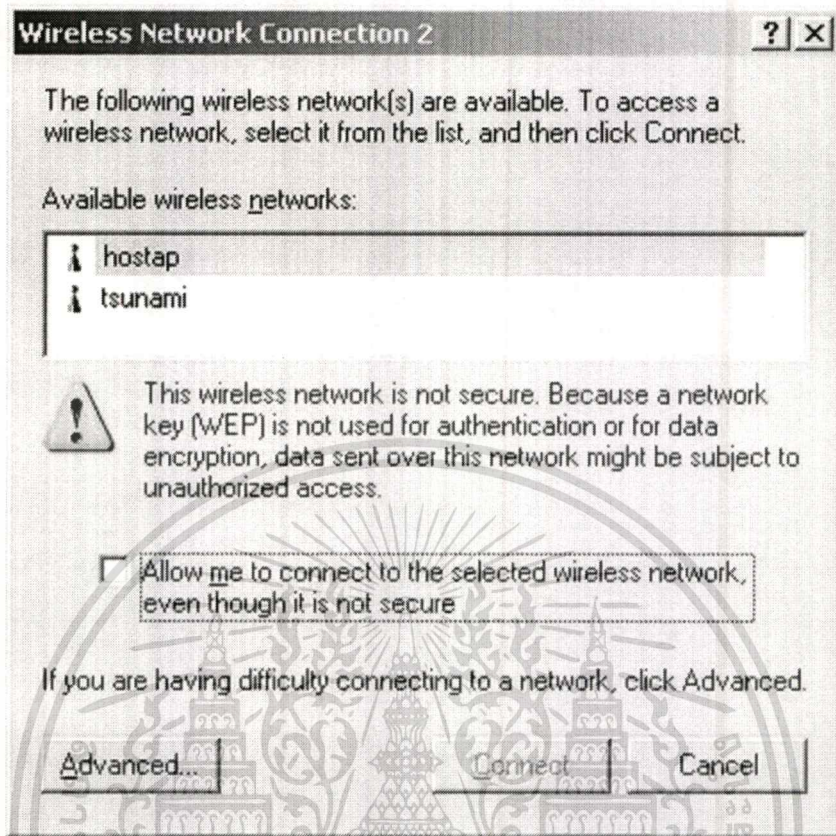


รูปที่ 7.1 แสดงภาพการทดสอบระบบไวร์เลสแอสเซสพอยท์

7.1 เริ่มต้นการใช้งานระบบ

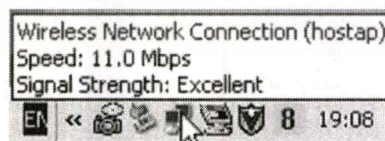
เมื่อติดตั้งการ์ดไวร์เลสใช้งานได้แล้วเครื่องลูกข่ายจะต้องเลือกตัวไวร์เลสแอสเซสพอยท์ให้เลือกชื่อ `hostap` และทำเครื่องหมายหน้า `Allow me to connect to the selected wireless network, even though it is secure` จึงกดปุ่ม `Connect`

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



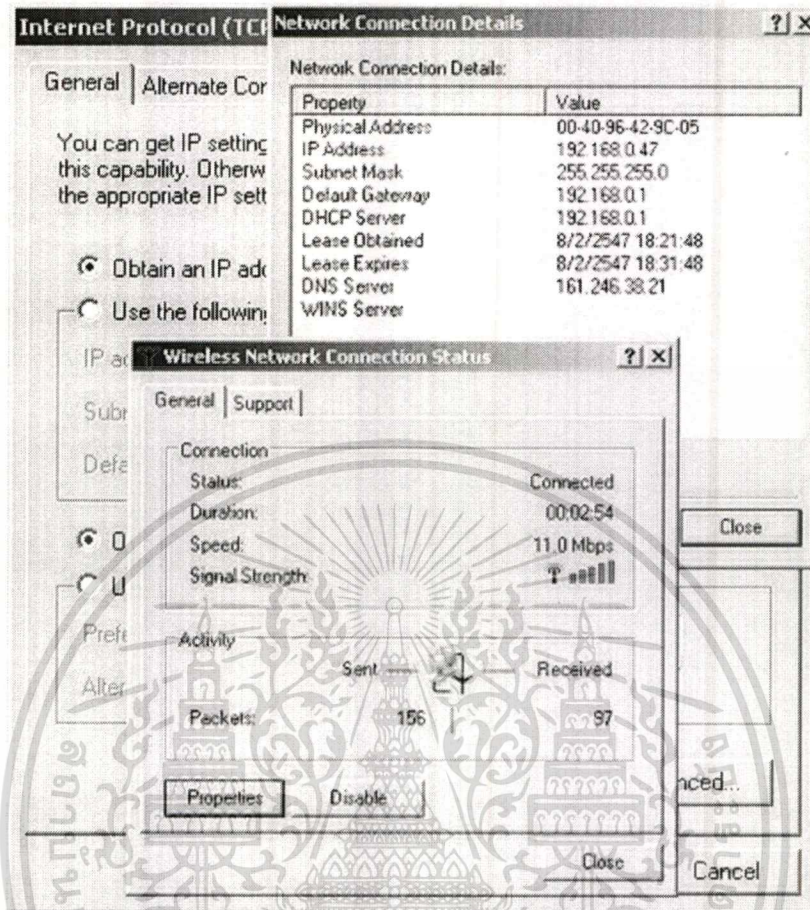
รูปที่ 7.2 แสดงหน้าจอเลือกตัวไวร์เลสแอกเซสพอยท์

จะเห็นรูปเครื่องคอมพิวเตอร์สองเครื่องระบบเครือข่ายเมื่อนำเมาส์ไปใกล้ๆจะมีข้อความดังนี้ ซึ่งจะบอกชื่อไวร์เลสแอกเซสพอยท์ ชื่อ hostap บอกความเร็วที่ 11 Mbps และบอกความแข็งแรงของสัญญาณ ดังรูปที่ 7.3



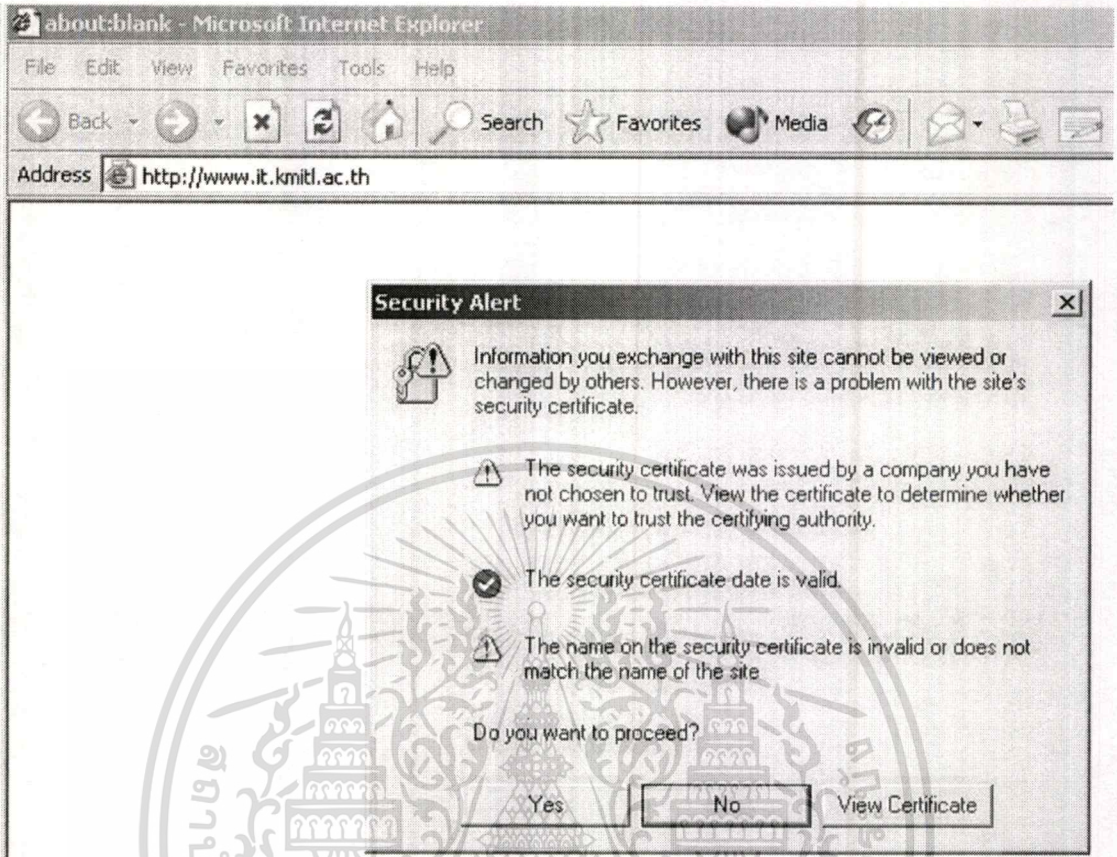
รูปที่ 7.3 แสดงหน้าจอข้อความรายละเอียดโดยย่อในการเลือกตัวไวร์เลสแอกเซสพอยท์

เมื่อเลือกตัวไวร์เลสแอกเซสพอยท์ที่ต้องการแล้ว เครื่องลูกข่ายจะทำการร้องขอไอพีจากเครื่องที่ให้บริการ DHCP เครื่องให้บริการจะทำการส่งไอพีมาให้เป็นไอพี 192.168.0.10-50 เกตเวย์ 192.168.0.1 เครื่องให้บริการ DHCP 192.168.0.1 เครื่องให้บริการ DNS 161.246.38.21 ดังรูปที่ 7.4 เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



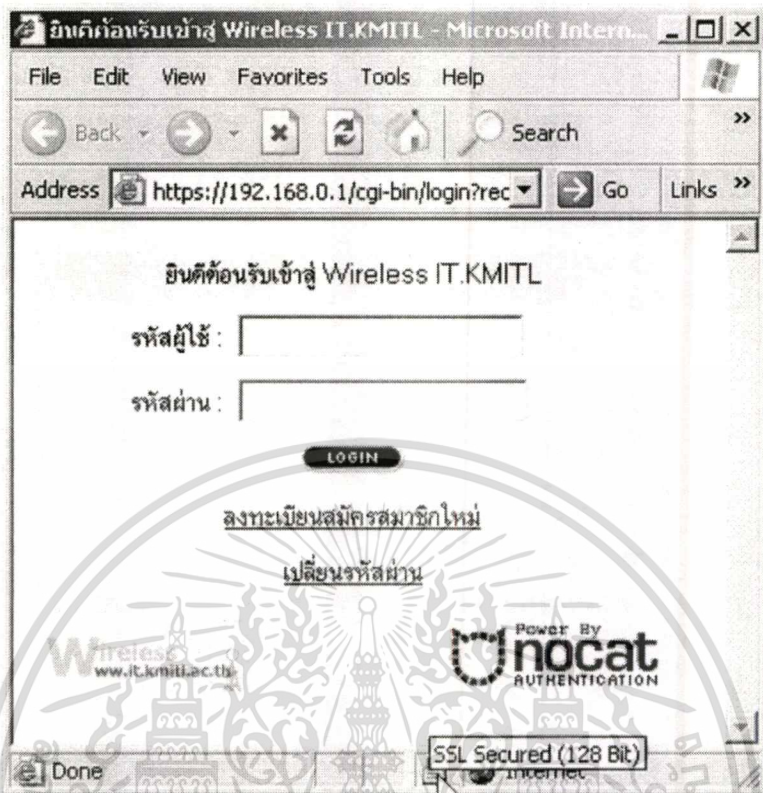
รูปที่ 7.4 แสดงหน้าจอเครื่องลูกข่ายไร้สายแลนได้รับไอพี

เมื่อทำการตั้งค่าพื้นฐานข้างต้นเสร็จเรียบร้อยแล้ว จะเข้าสู่ระบบงานได้ต้องทำการพิสูจน์ตัวตนจริงผ่าน SSL โดยใช้เว็บเบราว์เซอร์ พิมพ์ยูอาร์แอลเว็บไซต์ที่ต้องการ ดังรูปที่ 7.5



รูปที่ 7.5 แสดงหน้าจอยืนยันการเข้ารหัส SSL เครื่องลูกข่ายไวร์เลสแลน

เมื่อทำการตอบยืนยันกดปุ่ม Yes แล้วระบบจะทำการขึ้นหน้าจอให้ล็อกอินขึ้นมาโดยอัตโนมัติ



รูปที่ 7.6 แสดงหน้าจอล็อกอินเข้าสู่ระบบ

จากขั้นตอนที่ผ่านมาผู้ใช้ ยังไม่สามารถเข้าสู่ระบบได้ ถ้าไม่ทำการลงทะเบียนก่อน ดังนั้นจะต้องการลงทะเบียนเองหรือผู้ดูแลระบบลงทะเบียนให้เอง แต่ในส่วนนี้ให้ผู้ใช้ทำการลงทะเบียน โดยทำการป้อนข้อมูลให้ครบทุกช่อง และข้อมูลที่เป็นความจริง เพื่อเป็นประโยชน์ต่อการตัดสินใจของผู้ดูแลระบบเอง

ลงทะเบียน Wireless IT.KMITL

รหัสผู้ใช้: it 44067405 (รหัสนักศึกษา เช่น : 44067439)

เพศ: ชาย หญิง

ชื่อ (Th): สมเจ็ด

นามสกุล (Th): โพธิ์ทอง

ชื่อ (En): somjerd

นามสกุล (En): pothong

วันเดือนปีเกิด: 3/2/2516 (dd/mm/yyyy)

หลักสูตร: ปรียญตรี ปรียญโท ปรียญเอก

อีเมล: somjerd@hotmail.com

OK Cancel

Power By nocat AUTHENTICATION

รูปที่ 7.7 แสดงหน้าจอลงทะเบียน

เมื่อป้อนข้อมูลการลงทะเบียนครบแล้ว จะมีข้อความการลงทะเบียนเรียบร้อยแล้ว

Register Wireless IT.KMITL

ลงทะเบียนเรียบร้อยแล้ว

Automatic refresh page 5 sec

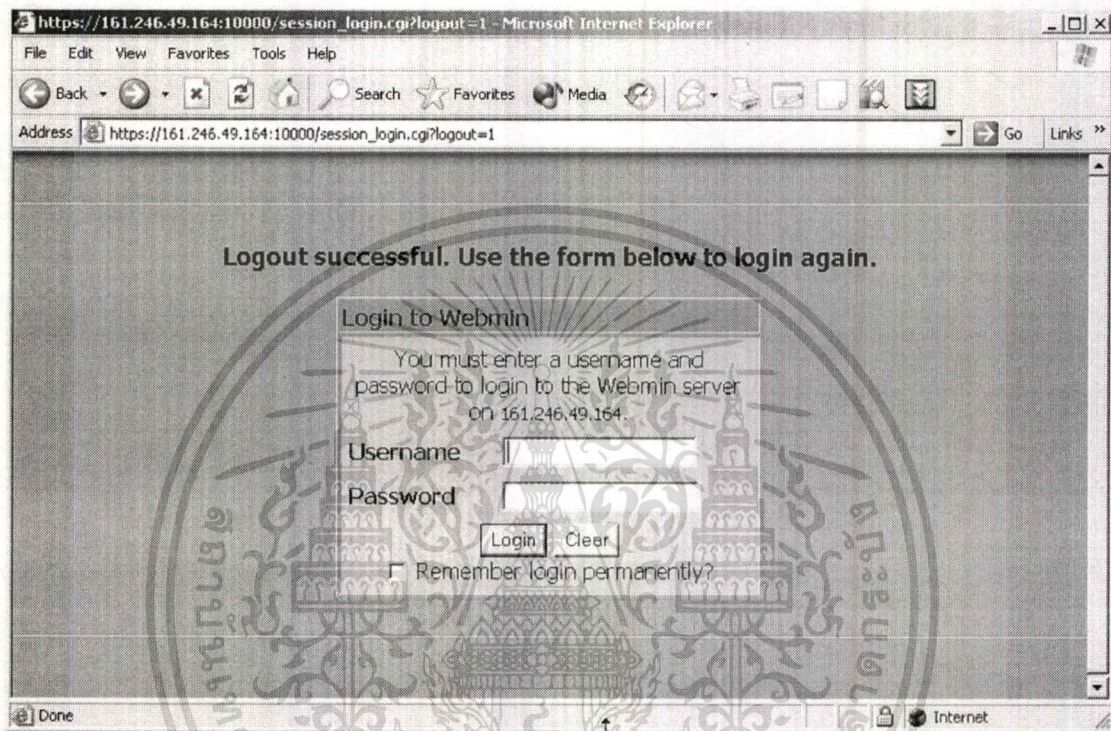
OK

Power By nocat AUTHENTICATION

รูปที่ 7.8 แสดงหน้าจอลงทะเบียนเรียบร้อยแล้ว

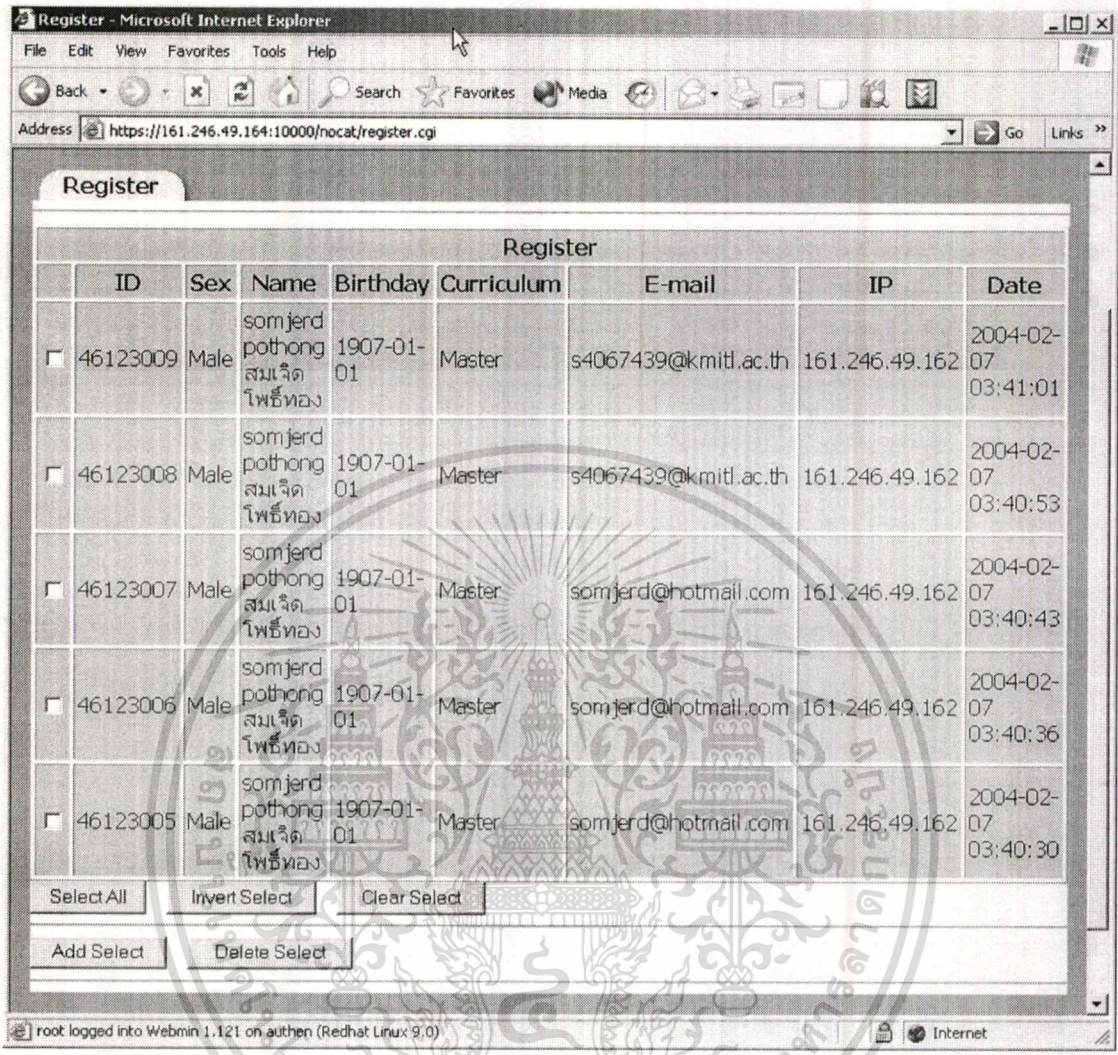
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อผู้ใช้ทำการลงทะเบียนเรียนเรียบร้อยแล้ว ผู้ดูแลระบบจะทำการตรวจสอบจากข้อมูลของผู้ใช้ที่ได้ทำการลงทะเบียน ทางเว็บมิน Webmin โดยผู้ดูแลระบบทำการล็อกอินโดย root



รูปที่ 7.9 แสดงหน้าจอการล็อกอินของผู้ดูแลระบบ

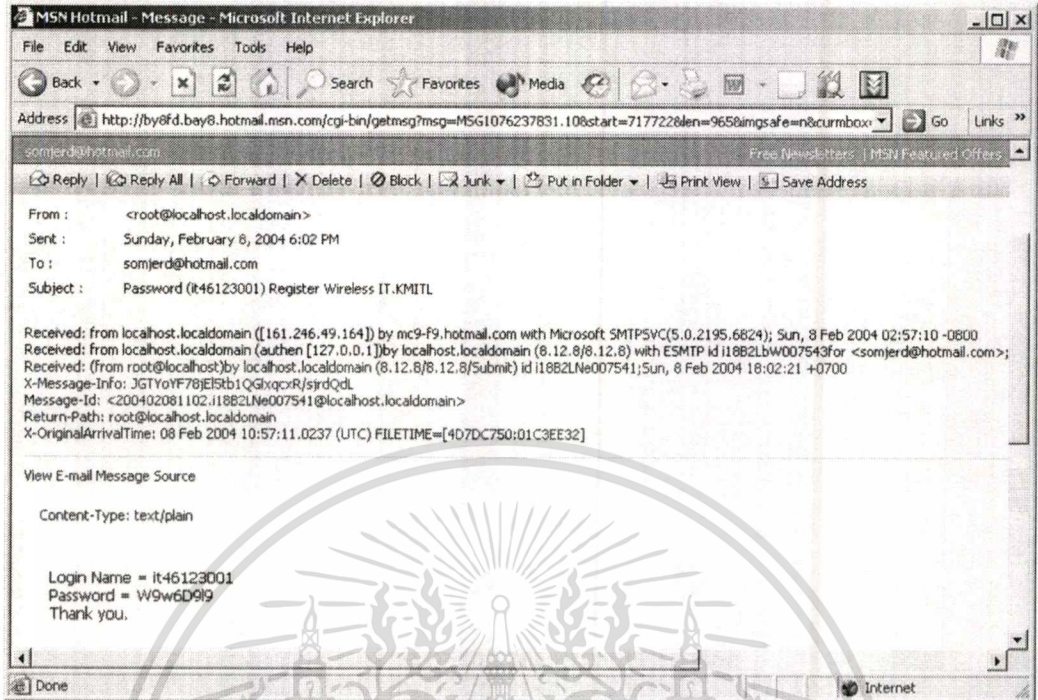
ผู้ดูแลระบบทำการตรวจสอบ เมื่ออนุญาตให้งาน ได้แล้วระบบจะทำการส่งรหัสผู้ใช้พร้อมกับรหัสผ่านไปทางอีเมล รูปที่ 7.10



รูปที่ 7.10 แสดงหน้าจอข้อมูลการลงทะเบียนของผู้ใช้เพื่อผู้ดูแลระบบทำการตรวจสอบ

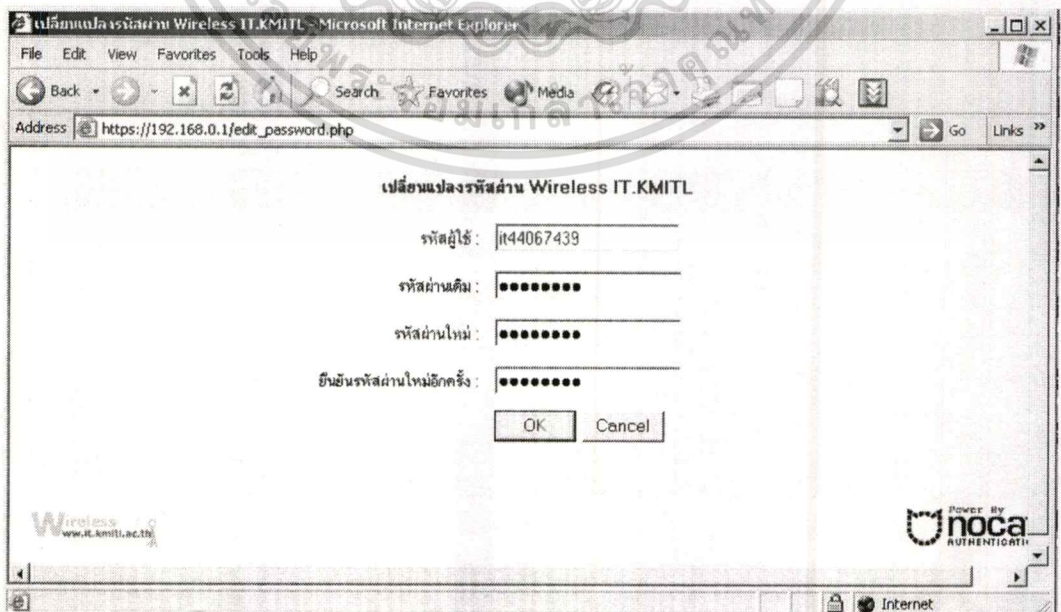
เมื่อผ่านขั้นตอนดังกล่าวอีเมลจะถูกส่งมาพร้อมกับัตรรหัสผู้ใช้กับรหัสผ่าน ดังรูปที่ 7.11

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

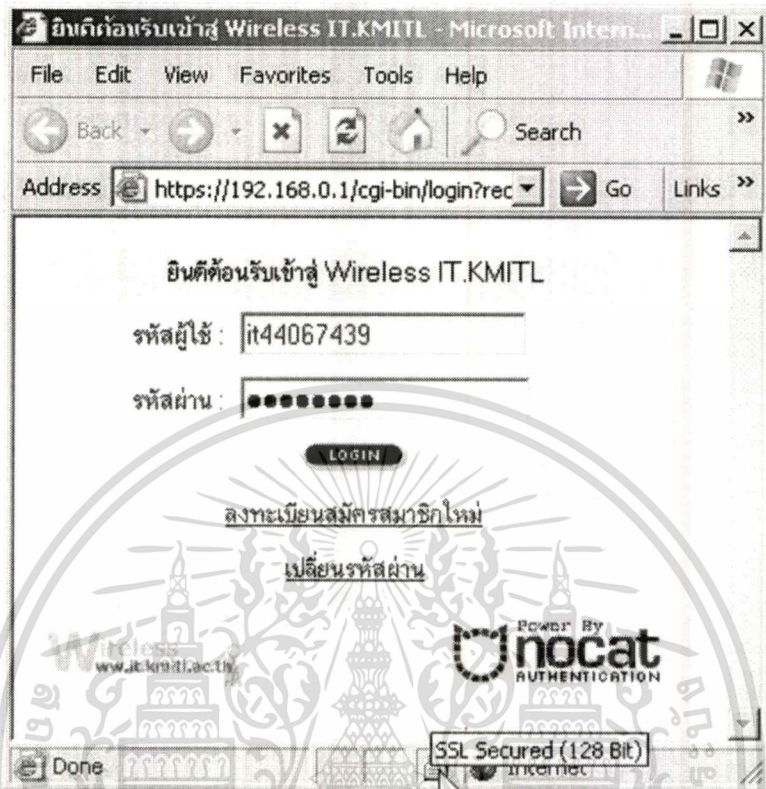


รูปที่ 7.11 แสดงหน้าจอรหัสผู้ใช้กับรหัสผ่านที่ส่งมาจากผู้ดูแลระบบ

เมื่อผู้ใช้ได้รับรหัสผู้ใช้กับรหัสผ่านแล้ว ผู้ใช้สามารถทำการเปลี่ยนรหัสผ่านหรือทำการล็อกอินเข้าสู่ระบบได้ ดังรูปที่ 7.13 และ 7.14



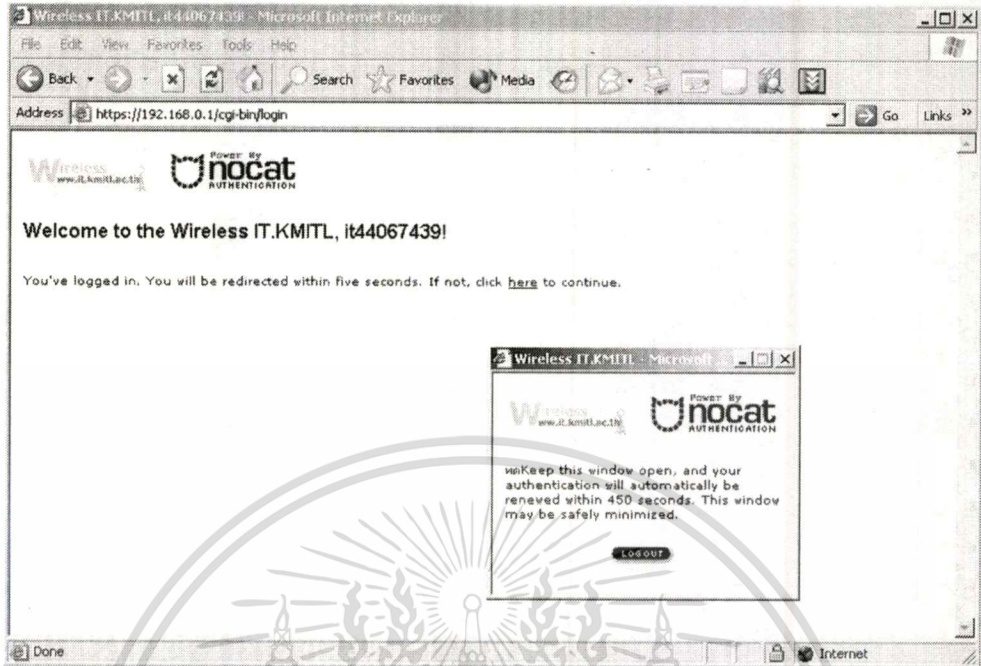
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับใช้ในการปฏิบัติงานของเจ้าหน้าที่ระบบคอมพิวเตอร์เท่านั้น ไม่ควรนำเอกสารนี้ไปใช้ประโยชน์ด้านการค้า
รูปที่ 7.12 แสดงหน้าจอการเปลี่ยนรหัสผ่าน
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 7.13 แสดงหน้าจอการล็อกอินเข้าใช้งานระบบ

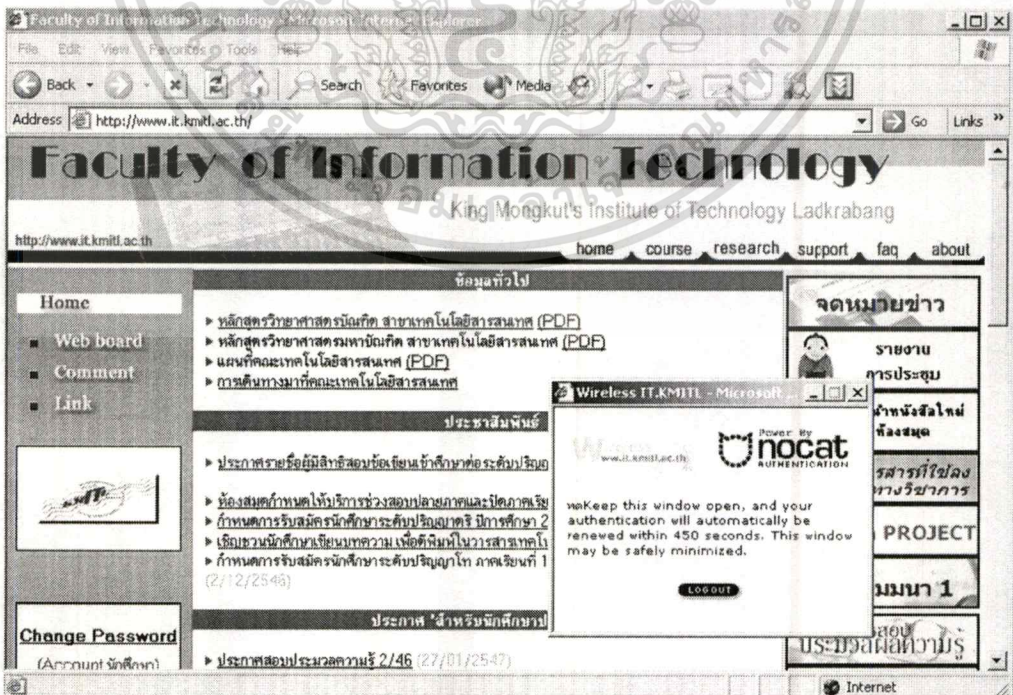
เมื่อทำการล็อกอินผ่านแล้ว ระบบจะมีหน้าวินโดว์เล็กขึ้นมา โดยมีความหมายว่า ถ้าผู้ใช้ทำการปิดหน้าจอนี้โดยไม่ทำการ logout ตามวิธีที่ถูกต้องจะทำให้การใช้งานอินเทอร์เน็ตไม่ต่อเนื่องตรงกันข้ามถ้าเปิดไว้ระบบจะทำการต่ออายุการใช้งานอินเทอร์เน็ตทุก 450 วินาทีโดยอัตโนมัติ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 7.14 แสดงหน้าจอการล็อกอินเข้าใช้งานระบบผ่านแล้ว

เมื่อทำการล็อกอินผ่านแล้ว ระบบจะทำการส่งค่าที่ผู้ใช้เคยทำการพิมพ์ยูอาร์แอลไว้แต่ต้นให้อัตโนมัติ ดังรูปที่ 7.15



เอกสารนี้เป็นเอกสารที่สงวนรูปที่ 7.15 แสดงหน้าจอการใช้งานอินเทอร์เน็ตได้แล้วไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 7.16 แสดงหน้าจอการออกจากระบบ

7.2 สรุปผลการทดลองการใช้งานระบบ

ผลการทดลองใช้งานระบบ ตามเมนูต่างๆ ทั้งในส่วนของผู้ใช้บริการและในส่วนของผู้ดูแลระบบหรือเจ้าหน้าที่ พบว่าบางส่วนของการทำงานได้ผลดีเช่น ส่วนของการจัดการข้อมูลผู้ใช้งานทั้งที่เป็นเจ้าหน้าที่และผู้ใช้บริการ การเพิ่ม ลบ แก้ไขรายละเอียด มีการตรวจสอบข้อมูลที่บันทึกว่ามีการซ้ำกันของข้อมูลที่อยู่ภายในระบบหรือไม่ เช่น รหัสผู้ใช้งานที่เป็นรหัสนักศึกษาเพื่อป้องกันความผิดพลาดในการบันทึกและแก้ไขข้อมูล สำหรับการลบ มีการยืนยันถามก่อนลบเพื่อป้องกันความผิดพลาด

ส่วนของการลงทะเบียนเพื่อขอใช้งานระบบ ระบบได้ทำการตรวจสอบการป้อนข้อมูลให้ครบและถูกต้องตามประเภทของข้อมูล เช่น รหัสผู้ใช้ที่เป็นรหัสนักศึกษาควรเป็นตัวเลขจำนวนแปดตัว ไม่สามารถป้อนเป็นตัวอักษรได้ การป้อนอีเมล ต้องทำการป้อนให้ถูกรูปแบบอีเมล และที่สำคัญระบบจะทำการตรวจสอบรหัสผู้ใช้นั้นทำการลงทะเบียนแล้ว

ส่วนของผู้ดูแลระบบหรือเจ้าหน้าที่ สามารถตรวจสอบการลงทะเบียนแล้วการอนุญาตการใช้ของผู้ใช้ โดยทำการส่งรหัสผู้ใช้กับรหัสผ่านส่งไปทางอีเมล และที่สำคัญรหัสผ่านนั้นทำการสุ่มค่าจำนวนแปดตัวโดยมีทั้งตัวเลขและตัวอักษรผสมกัน แล้วยังมีการเข้ารหัสเพื่อความปลอดภัย ในส่วนของการคอนฟิกค่าต่างๆ สามารถทำได้ง่าย

โดยสรุปแล้ว ภาพรวมการทำงานของระบบสามารถทำงานได้ ตามที่ผู้ศึกษาออกแบบพัฒนาระบบไว้ และคาดหวังว่าจะสามารถนำไปใช้งานได้จริง

บทที่ 8

สรุปผลการพัฒนาระบบงาน และข้อเสนอแนะ

เนื้อหาในบทนี้จะสรุปผล พร้อมทั้งข้อเสนอแนะสำหรับผู้ที่เกี่ยวข้องกับระบบงานไปทำการพัฒนาต่อไป

8.1 สรุปผลการพัฒนาระบบงาน

ผลที่ได้จากการพัฒนาระบบงานพบว่า สามารถทำการพิสูจน์ตัวตนจริงของผู้ใช้งาน ด้วยรหัสผู้ใช้และรหัสผ่าน ทำให้สะดวกต่อการควบคุมการใช้งานระบบอินเทอร์เน็ต จากบุคคลภายนอกได้ และมีความปลอดภัยสูง และอุปกรณ์ที่นำมาพัฒนามีราคาไม่แพง สามารถใช้ระบบปฏิบัติการไม่เสียค่าลิขสิทธิ์ เป็นซอฟต์แวร์ทำให้ยืดหยุ่นต่อการพัฒนาต่อเนื่อง หรือสามารถนำไปดัดแปลงให้สอดคล้องกับระบบที่ใช้งานอยู่ปัจจุบันได้ดี ซึ่งจะช่วยให้การทำงานของหน่วยงานที่ให้บริการคอมพิวเตอร์สารสนเทศมีระบบทำงานที่ดีขึ้น

8.2 ข้อเสนอแนะ

ข้อเสนอแนะสำหรับผู้ที่จะนำระบบงานไปพัฒนาต่อไป ส่วนของการตรวจสอบการบันทึกเวลาการใช้งานระบบ โดยการกำหนดเวลาการใช้งาน การตรวจสอบสถานะของผู้ใช้งาน สามารถทำการเชื่อมฐานข้อมูลในหน่วยงานใหม่หรือระบบ ได้หลากหลายขึ้น จะทำให้การทำงานของระบบมีประสิทธิภาพดีขึ้น

บรรณานุกรม

ก่อกิจ วีระอาชากุล.2546.ติดตั้งและปรับแต่งเซิร์ฟเวอร์ Linux สำหรับ Admin Linux โดยเฉพาะ.

กรุงเทพฯ : อินโฟเพรส.

กิตติศักดิ์ เจริญโภคานนท์. 2540. สร้างเว็บได้ดั่งใจนี้ได้ด้วย PHP. กรุงเทพฯ : ชัคเซสมิเดีย.

ทรงเกียรติ ภาวดี.2543.ครบเครื่องCGIเพื่อจัดระบบเก็บข้อมูล3แบบ3สไตล์.กรุงเทพฯ :วิตตี้ กรุ๊ป.

ทรงเกียรติ ภาวดี.2542.เริ่มเขียนสคริปต์ด้วยภาษา PERL.กรุงเทพฯ :วิตตี้ กรุ๊ป.

ทรงเกียรติ ภาวดี.2542.พื้นฐาน CGI ผนึกกำลัง SSI เพื่อการประยุกต์.กรุงเทพฯ :วิตตี้ กรุ๊ป.

ทรงเกียรติ ภาวดี.2547. **Web Programming CGI/Perl PHP.** [Online]. Available:

<http://www.cgitop.com/phpBB2/index.php>

บัณฑิต จามรภูมิ.2546.คัมภีร์ Linux Red Hat เล่ม 1.กรุงเทพฯ :บัณฑิต จามรภูมิ.

ไพศาล โมลิสกุลมงคล. 2542. พัฒนา Web Database ด้วย PHP. กรุงเทพฯ : ดวงกมล กรุ๊ป.

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่. **Introduction to MySQL Database Server.** เชียงใหม่ : คณะวิศวกรรมศาสตร์มหาวิทยาลัยเชียงใหม่.

สงกรานต์ ทองสว่าง.2544. **My SQL ระบบฐานข้อมูลสำหรับอินเทอร์เน็ต.**กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

Aaron Baer. 2003. **Offical RedHat Kernel with HostAP.** [Online]. Available:

http://www.cat.pdx.edu/~baera/redhat_hostap/

AbsoluteValue Systems. 2003. **Complete listing of WLAN adapters with chipset information.**

[Online]. Available: http://www.linux-wlan.org/docs/wlan_adapters.html.gz

Amsternet. 2003. **NoCatAuthOnFreeBsd.**[Online]. Available:

<http://wiki.savage.net/amsternet/NoCatAuthOnFreeBsd>

Bebas. 2003. **NoCat Authentication System.**[Online]. Available:

<http://bebas.ylsm.org/v14/onno/the-guide/wifi/ch-15-nocat.doc>

Bruce Baikie, Dave Clements, Steve Gaede, Bob Gray . 2002. **Install Instructions for NoCat**

0.81 Software using the Cobalt 2.2 Kernel and the DWL-500 Wireless Card.

[Online]. Available: <http://www.aerocube.com/howto-2.html>

Ellie Quigley.2001.Perl By Example.US :Prentice Hall.

Gdead, Heidi . 2004. **HostAP Project.** [Online]. Available:

<http://lists.shmoo.com/mailman/listinfo/hostap>

- Jason Boxman. 2002. **Installing and Setting up basic HostAP box**. [Online]. Available:
http://trekweb.com/~jasonb/articles/hostap_20021012.shtml
- Jason. 2003. **Installing and Configuring HostAP**. [Online]. Available:
http://www.trekweb.com/~jasonb/articles/hostap_20030727.shtml
- Jean Tourrilhes. 2003. **Wireless LAN resources for Linux**. [Online]. Available:
http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/
- JerrittCollord. 2003. **HostApMode**. [Online]. Available:
<http://www.personaltelco.net/index.cgi/HostApMode>
- Jouni Malinen. 2004.. **Host AP driver for Intersil Prism2/2.5/3**. [Online]. Available:
<http://hostap.epitest.fi/>
- Matt Gunter. 2003. **NoCatAuth Authentication Server Configuration**. [Online]. Available:
<http://www.wi-fiplanet.com/tutorials/article.php/3286631>
- Mike Glover,Aidan Humphreys,Ed Weiss.1996 .Perl 5 How-To. CA: Waite Group.
- Nathan Zorn. 2002. **Authentication Gateway HOWTO**. [Online]. Available:
<http://www.traduc.org/docs/HOWTO/lecture/Authentication-Gateway-HOWTO.html>
- Olivier. 2003. **Doc d'installation de Nocat** . [Online]. Available:
http://www.wifi-vitry.net/imprimersans.php3?id_article=14
- Peter Seebach . 2003. **Building a wireless access point on Linux**. [Online]. Available:
<http://www-106.ibm.com/developerworks/linux/library/l-wap.html>
- Petrus. 2003. **Installation de Nocat sur une Debian**. [Online]. Available:
http://www.campus.ecp.fr/~petrus/linux_nocat.php
- Rob Flickenger.2002.**Building Wireless Community Networks**. [Online]. Available:
http://www.hipatia.info/red_libre/download/oreilly.pdf
- Robert Rose. 2002. **Prism II Access Point Mini-Howto**. [Online]. Available:
<http://www.cafwap.net/prism2ap/>
- Sameer Verma. 2002. **Implementing Secure Services over a Wireless Network**.
 [Online]. Available: http://verma.sfsu.edu/users/wireless/nocatauth_report.pdf
- Schuyler Erle , Robert Flickenger. 2003. **NoCatNet**. [Online]. Available:
<http://nocat.net/>

Simon Anderson. 2003. **A Linux Wireless Access Point HOWTO**. [Online]. Available:

<http://oob.freeshell.org/nzwireless/LWAP-HOWTO.html>

Sown. 2003. **HostAPWalkthru**. [Online]. Available:

<http://www.sown.org.uk/index.php/HostAPWalkthru>

Tanabutr. 2003. **Basic Linux Firewall By IPTABLES**. [Online]. Available:

<http://www24.brinkster.com/shadowpd/db/ossys/article/firewall.html>

Toni dIF Diaz. 2003. **NoCatBOX HOWTO v1.4**. [Online]. Available:

<http://blyx.com/public/wireless/nocatbox/nocatbox-howto-en.pdf>

UnixQi. 2003. **nocat hotspot howto**. [Online]. Available:

http://www.unixqi.com/learn/nocat_hotspot_howto.pdf





เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ไฟล์คอนฟิก NoCat nocat.conf (gateway.conf)

อยู่ห้อง /usr/local/nocat/gateway

```
##### gateway.conf -- NoCatAuth Gateway Configuration.
```

```

Verboesity                10
GatewayName               Wireless IT.KMITL
GatewayMode               Passive
GatewayLog                /usr/local/nocat/gateway/nocat.log
LoginTimeout              600
HomePage                  http://192.168.0.1/
DocumentRoot              /usr/local/nocat/gateway/htdocs
SplashForm                splash.html
StatusForm                status.html
TrustedGroups              Any
AuthServiceAddr            192.168.0.1
AuthServiceURL             https://$AuthServiceAddr/cgi-bin/login
LogoutURL                  https://$AuthServiceAddr/logout.html
ExternalDevice             eth1
InternalDevice             eth0
LocalNetwork              192.168.0.0/24
DNSAddr                   161.246.38.21
RouteOnly                  1
ExcludePorts              25
IdleTimeout                100

```

ไฟล์คอนฟิก NoCat nocat.conf (authserv.conf)

อยู่ห้อง /usr/local/nocat

```
##### authserv.conf -- NoCatAuth Authentication Service Configuration.
```

```

Verboisity          10
HomePage            http://192.168.0.1/
DocumentRoot       /usr/local/nocat/htdocs
DataSource          DBI
Database            dbi:mysql:database=nocat
DB_User            root
DB_Passwd          root
UserTable           member
UserIDField        login
UserPasswdField    pass
UserAuthField      status
UserStampField     created
GroupTable         network
GroupIDField       network
GroupAdminField    admin
MinPasswdLength    6
LocalGateway       192.168.0.1
LoginForm          login.html
LoginOKForm        login_ok.html
FatalForm          fatal.html
ExpiredForm        expired.html
RenewForm          renew.html
PassiveRenewForm   renew_pasv.html
RegisterForm       register.html
RegisterOKForm     register_ok.html

```

| | |
|---------------------|--|
| RegisterFields | name url description |
| UpdateForm | update.html |
| UpdateFields | url description |
| LoginGreeting | ยินดีต้อนรับเข้าสู่ Wireless IT.KMITL |
| LoginMissing | กรุณาป้อนข้อมูลให้ครบ ! |
| LoginBadUser | รหัสผู้ใช้ผิด. กรุณาป้อนข้อมูลใหม่. |
| LoginBadPass | รหัสผ่านไม่ถูกต้อง. กรุณาป้อนข้อมูลใหม่. |
| LoginBadStatus | Sorry, you are not a registered co-op member. |
| RegisterGreeting | Welcome! Please enter the following information to register. |
| RegisterMissing | Name, E-mail, and password fields must be filled in. |
| RegisterUserExists | Sorry, that e-mail address is already taken. Are you already registered? |
| RegisterBadUser | The e-mail address provided appears to be invalid. Did you spell it correctly? |
| RegisterInvalidPass | All passwords must be at least six characters long. |
| RegisterPassNoMatch | The passwords you provided do not match. Please try again. |
| RegisterSuccess | Congratulations, you have successfully registered. |
| UpdateGreeting | Enter your E-mail and password to update your info. |
| UpdateBadUser | That e-mail address is unknown. Please try again. |
| UpdateBadPass | That e-mail and password do not match. Please try again. |
| UpdateInvalidPass | New passwords must be at least six characters long. |
| UpdatePassNoMatch | The new passwords you provided do not match. Please try again. |
| UpdateSuccess | Congratulations, you have successfully updated your account. |

ไฟล์คอนฟิก NoCat httpd.conf

อยู่ห้อง /usr/local/nocat

```
ScriptAlias /cgi-bin/ /usr/local/nocat/cgi-bin/
```

```
<Directory /usr/local/nocat/cgi-bin>
```

```
SetEnv PERL5LIB /usr/local/nocat/lib
```

```
SetEnv NOCAT /usr/local/nocat/nocat.conf
```

```
</Directory>
SetEnvIf User-Agent ".*MSIE.*" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
```

ไฟล์คอนฟิก Apache httpd.conf

อยู่ห้อง /etc/httpd/conf/

```
Include /usr/local/nocat/httpd.conf
```

ไฟล์คอนฟิก Apache ssl.conf

อยู่ห้อง /etc/httpd/conf.d/

```
<VirtualHost _default_:443>
DocumentRoot /usr/local/nocat/htdocs
ServerName 192168.0.1:443
SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
SetEnvIf User-Agent ".*MSIE.*" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
CustomLog logs/ssl_request_log \
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

การแก้ไขปัญหา Perl ให้แสดงภาษาไทย

การแก้ไขปัญหา Perl แสดงภาษาไทยไม่อัตโนมัติ เข้าไปแก้ที่ /usr/lib/perl5/5.8.0/CGI.pm

```
ทำการแก้เป็น $self->charset('tis-620');
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

อุปกรณ์การ์ดไวร์เลสที่สนับสนุนการทำไวร์เลสแอสซอสพอยท์

WLAN Adapter Chipset Directory compiled by AbsoluteValue Systems, Inc.

Updated 02-February-2004 ADAPTERS SUPPORTED BY LINUX-WLAN-NG

http://www.linux-wlan.org/docs/wlan_adapters.html.gz

| VENDOR | WLAN TYPE | PRODUCT ID | HOST I/F | CHIPSET |
|------------|-----------|------------|----------|--------------|
| Abocom | 802.11b | CWB 1000 | CF | Prism2/2.5/3 |
| Abocom | 802.11b | WB1500 | PCMCIA | Prism2/2.5/3 |
| Abocom | 802.11b | WB 1500H | PCMCIA | Prism2/2.5/3 |
| Abocom | 802.11b | WB 1500S | PCMCIA | Prism2/2.5/3 |
| Abocom | 802.11b | WB 1500SH | PCMCIA | Prism2/2.5/3 |
| Abocom | 802.11g | WG 2000 | Cardbus | Prism GT ? |
| Abocom | 802.11g | WPG 2000 | PCI | Prism GT |
| AboveCable | 802.11b | ACPC2000 | PCMCIA | Prism2/2.5/3 |
| AboveCable | 802.11b | ACPC2000 | USB | Prism2/2.5/3 |
| AboveCable | 802.11b | ACPC2000 | CF | Prism2/2.5/3 |
| Accton | 802.11b | WN 3101J | PCMCIA | Prism2/2.5/3 |
| Accton | 802.11b | WN 3501B | USB | Prism2/2.5/3 |
| Accton | 802.11g | WN 4201 | PCI | Prism GT |
| Accton | 802.11g | WN 4301 | Cardbus | Prism GT |
| Accton | 802.11g | WN 4401 | mini-PCI | Prism GT |
| Accton | 802.11g | WN 4501 | USB | Prism GT |
| Acer | 802.11b | 2411 | PCMCIA | Prism2/2.5/3 |
| Acer | 802.11b | ? | mini-USB | Prism2/2.5/3 |
| Acrowave | 802.11b | AWL-1100P | PCI | Prism2/2.5/3 |
| Acrowave | 802.11b | AWL-1100C | PCMCIA | Prism2/2.5/3 |
| Actiontec | 802.11b | 802PI25 | PCI | Prism2/2.5/3 |
| Actiontec | 802.11b | 802CI2 | PCMCIA | Prism2/2.5/3 |
| Actiontec | 802.11b | 802UI3 | USB | Prism2/2.5/3 |

เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์สำหรับการใช้งานเพื่อการศึกษาค้นคว้าเท่านั้น ไม่อนุญาตให้นำไปเผยแพร่โดยไม่ได้รับอนุญาต

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

| | | | | |
|----------------|---------|--------------|------------|---------------|
| Actiontec | 802.11b | HWP01170-01 | PCI | Prism2/2.5/3 |
| Actiontec | 802.11b | HWU01170-01 | USB | Prism2/2.5/3 |
| Actiontec | 802.11b | HWC01170-01 | PCMCIA | Prism2/2.5/3 |
| Actiontec | 802.11g | tbd | Cardbus | Prism GT |
| Adaptec | 802.11b | AWN8020 | USB | Prism2/2.5/3 |
| Adaptec | 802.11b | AWN 8030 | PCMCIA | Prism2/2.5/3 |
| Addtron | 802.11b | AWP-100 | PCMCIA | Prism2/2.5/3 |
| Addtron | 802.11b | AWP-101 | PCMCIA | Prism2/2.5/3 |
| Adtec | 802.11b | ADLINK 345CF | CF | Prism2/2.5/3 |
| Airvast | 802.11b | WN-100 | PCMCIA | Prism2/2.5/3 |
| Airvast | 802.11b | WN-100S | PCMCIA | Prism2/2.5/3 |
| Airvast | 802.11b | WN-110 | PCMCIA | Prism2/2.5/3 |
| Airvast | 802.11b | WN-220 | USB stick | Prism2/2.5/3 |
| Airvast | 802.11b | WN168b | USB module | Prism2/2.5/3 |
| Airvast | 802.11g | WN-150g | Cardbus | PrismGT |
| Airvast | 802.11g | WN-360g | mini-PCI | PrismGT |
| Alfa | 802.11b | GWPC001E | PCMCIA | Prism2/2.5/3 |
| Alfa | 802.11b | GWPCI01 | PCI | Prism2/2.5/3 |
| Alfa | 802.11b | AWUS001B | USB | Prism2/2.5/3 |
| Alfa | 802.11b | GWUS001D | USB | Prism2/2.5/3 |
| Alfa | 802.11b | AWCF001 | CF | Prism2/2.5/3 |
| Alfa | 802.11b | AWCF001A | CF | Prism2/2.5/3 |
| Alfa | 802.11g | GWPC006 | Cardbus | Prism GT |
| Alfa | 802.11g | GWPCI06 | mini-PCI | Prism GT |
| Alfa | 802.11g | GWPCI16 | PCI | Prism GT |
| Allied Telesyn | 802.11b | AT-WCL452 | PCMCIA | Prism 2/2.5/3 |
| Allied Telesyn | 802.11b | AT-WCL007 | PCI | Priism2/2.5/3 |
| Allied Telesyn | 802.11b | AT-WCL460 | mini-USB | Priism2/2.5/3 |
| Allied Telesyn | 802.11b | AT-WR2411 | PCMCIA | Prism2/2.5/3 |

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้เผยแพร่ไปยังบริษัทภายนอก

ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้คัดลอกเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

| | | | | |
|------------------------|---------|----------------|----------|----------------|
| Allnet | 802.11b | ALL0191 | PCI | Prism2/2.5/3 |
| Allnet | 802.11b | ALL0192 | PCMCIA | Prism2/2.5/3 |
| Allnet | 802.11g | ALL0271 | PCI | PrismGT |
| Allnet | 802.11g | ALL0273 | USB | PrismGT |
| Ambicom | 802.11b | WL1100 | PCMCIA | Prism2/2.5/3 |
| Ambicom | 802.11b | WL1100B | PCMCIA | Prism2/2.5/3 |
| Ambicom | 802.11b | WL1100C | CF | Prism2/2.5/3 |
| Artem | 802.11b | CC-STD-PC-b | PCMCIA | Prism2/2.5/3 |
| Artem | 802.11b | CC-EMB-PC-b | mini-PCI | Prism2/2.5/3 |
| Artem | 802.11g | CC-STD-PC-g | Cardbus | Prism GT |
| Asante | 802.11b | AL-1011-DP | PCMCIA | Prism2/2.5/3 |
| Asante | 802.11b | AL 1011-PC | PCMCIA | Prism2/2.5/3 |
| Asante | 802.11b | AL 1011-Rev. B | PCMCIA | Prism2/2.5/3 |
| Asante | 802.11b | AL 1211-DP | PCMCIA | Prism2/2.5/3 ? |
| Asante | 802.11b | AL 3011-DP | PCI | Prism2/2.5/3 |
| Asante | 802.11b | AL 3011-PC | PCI | Prism2/2.5/3 |
| Ashton Digital | 802.11b | WRUB-2011i | USB | Prism2/2.5/3 |
| Askey | 802.11b | WLC010 | PCMCIA | Prism2/2.5/3 |
| Askey | 802.11b | WLC020 | PCMCIA | Prism2/2.5/3 |
| Askey | 802.11b | WLL030m | mini-PCI | Prism2/2.5/3 |
| Asus | 802.11b | WL-100 | PCMCIA | Prism2/2.5/3 |
| Asus | 802.11b | WL-110 | CF | Prism2/2.5/3 |
| Asus | 802.11b | WL-140 | USB | Prism2/2.5/3 |
| Aus.Linx Technology | 802.11b | AL-95002A | PCMCIA | Prism2/2.5/3 |
| Aus.Linx Technology | 802.11b | AL-95002CF | CF | Prism2/2.5/3 |
| Belkin | 802.11b | F5D6020 | PCMCIA | Prism2/2.5/3 |
| Belkin | 802.11b | F5D6001 | PCI | Prism2/2.5/3 |

เอกสารนี้เป็นเอกสารที่กรมส่งเสริมการค้าระหว่างประเทศ กระทรวงพาณิชย์ ไม่สามารถทำซ้ำโดยไม่ได้รับอนุญาตจากกรมการค้า

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

| | | | | |
|-----------|---------|------------|----------|--------------|
| Macromate | 802.11b | MWN-511 | USB | Prism2/2.5/3 |
| Macromate | 802.11b | MWN-611+ | PCI | Prism2/2.5/3 |
| Macromate | 802.11b | MWN-711+ | PCMCIA | Prism2/2.5/3 |
| Macsense | 802.11b | WUA-400 | USB | Prism2/2.5/3 |
| Macsense | 802.11b | WPE-600 | PCMCIA | Prism2/2.5/3 |
| Macsense | 802.11b | WUA-700 | USB | Prism2/2.5/3 |
| Macsense | 802.11b | WPE-700 | PCMCIA | Prism2/2.5/3 |
| Meritline | 802.11b | MWL-311FA | PCMCIA | Prism2/2.5/3 |
| Micronet | 802.11b | SP 903 | CF | Prism2/2.5/3 |
| Micronet | 802.11b | SP 903B | CF | Prism2/2.5/3 |
| Micronet | 802.11b | SP 905V2 | PCMCIA | Prism2/2.5/3 |
| Micronet | 802.11b | SP 905B | PCMCIA | Prism2/2.5/3 |
| Micronet | 802.11b | SP 905BD | PCMCIA | Prism2/2.5/3 |
| Micronet | 802.11b | SP 905BDV2 | PCMCIA | Prism2/2.5/3 |
| Micronet | 802.11b | SP 906A | PCI | Prism2/2.5/3 |
| Micronet | 802.11b | SP 906BA | PCI | Prism2/2.5/3 |
| Microsoft | 802.11b | MN-510 | USB | Prism2/2.5/3 |
| Microsoft | 802.11b | MN-520 | PCMCIA | Prism2/2.5/3 |
| Microtik | 802.11b | 2G/P20 | PCMCIA | Prism2/2.5/3 |
| Microtik | 802.11b | 2G/PMC | mini-PCI | Prism2/2.5/3 |
| MiLAN | 802.11b | W1897 | PCMCIA | Prism2/2.5/3 |
| MiLAN | 802.11b | W1897B | PCMCIA | Prism2/2.5/3 |
| Nalcom | 802.11b | PW-11P | PCMCIA | Prism2/2.5/3 |
| Nanospeed | 802.11b | NS-1100M | PCMCIA | Prism2/2.5/3 |
| NDC | 802.11b | NWH4020 | USB | Prism2/2.5/3 |
| NDC | 802.11b | NWH1010 | PCMCIA | Prism2/2.5/3 |
| NDC | 802.11b | NWH630 | PCI | Prism2/2.5/3 |
| NEC | 802.11b | CMZ-RT-WP | PCMCIA | Prism2/2.5/3 |
| Netgear | 802.11b | MA 111 | USB | Prism2/2.5/3 |
| Netgear | 802.11b | MA 311 | PCI | Prism2/2.5/3 |

| | | | | |
|----------------------|--------------------|-----------------|----------|--------------|
| Netgear | 802.11b | MA 401 | PCMCIA | Prism2/2.5/3 |
| Netgear | 802.11b | MA 401RA | PCMCIA | Prism2/2.5/3 |
| Netgear | 802.11b | MA 701 | CF | Prism2/2.5/3 |
| Netgear | 802.11g | WG 121 | USB | Prism GT |
| Netgear | 802.11g | WG 511 | Cardbus | Prism GT |
| Netlux | 802.11g | NX-NWL/G650 | Cardbus | Prism GT |
| Netlux | 802.11g | NX-NWL-G520 | PCI | Prism GT |
| NextLink | 802.11b | NLW-2400PA | PCMCIA | Prism2/2.5/3 |
| Nokia | 802.11b | C110 | PCMCIA | Prism2/2.5/3 |
| Nokia | 802.11b | C111 | PCMCIA | Prism2/2.5/3 |
| Nokia | 802.11 DS 2Mbps | C020/021 | PCMCIA | Prism 1 |
| OTC Wireless | 802.11b | AirEZY 2411-PCC | PCMCIA | Prism2/2.5/3 |
| OTC Wireless | 802.11b | APCC-202 | PCMCIA | Prism2/2.5/3 |
| Ovislink | 802.11b | WL-1100USB | USB | Prism2/2.5/3 |
| Ovislink | 802.11b | WL-1120PCM-SH | PCMCIA | Prism2/2.5/3 |
| Ovislink | 802.11g | WL-5400PCM | Cardbus | Prism GT |
| Ovislink | 802.11g | WL-5400PCI | PCI | Prism GT |
| PheeNet | 802.11b | WL-0011P | PCMCIA | Prism2/2.5/3 |
| PheeNet | 802.11b | WL-5031 | USB | Prism2/2.5/3 |
| PheeNet | 802.11g | WL-0054 | Cardbus | Prism GT |
| Philips | 802.11b | PH 10773 | PCMCIA | Prism2/2.5/3 |
| Philips | 802.11b | PH 10878 | CF | Prism2/2.5/3 |
| Philips | 802.11b | PH 10766 | mini-PCI | Prism2/2.5/3 |
| Philips | 802.11b | PH 10897 | USB | Prism2/2.5/3 |
| Phoebe | 802.11b | PHWL-11 | PCMCIA | Prism2/2.5/3 |
| Planet Technology | 802.11b | WL-3550 | PCMCIA | Prism2/2.5/3 |

| | | | | |
|----------------------|--------------------|--------------|---------|--------------|
| Planet Technology | 802.11b | WL-3600 | CF | Prism2/2.5/3 |
| Planex | 802.11b | GW-NS110 | PCMCIA | Prism2/2.5/3 |
| Planex | 802.11b | GW-NS110PX | PCMCIA | Prism2/2.5/3 |
| Planex | 802.11b | GW-NS11R | PCMCIA | Prism2/2.5/3 |
| Planex | 802.11b | GW-NS11H | PCMCIA | Prism2/2.5/3 |
| Planex | 802.11b | GW-US11H | USB | Prism2/2.5/3 |
| Planex | 802.11b | GW-CF11H | CF | Prism2/2.5/3 |
| Planex | 802.11b | GW-CF110 | CF | Prism2/2.5/3 |
| Planex | 802.11g | GW-DS54G | PCI | Prism GT |
| Proxim | 802.11b | 8430 | PCMCIA | Prism2/2.5/3 |
| Proxim | 802.11b | 8433-05 | PCMCIA | Prism2/2.5/3 |
| Proxim | 802.11b | 8434-05 | PCMCIA | Prism2/2.5/3 |
| RECAM | 802.11b | WL-211F | PCMCIA | Prism2/2.5/3 |
| Repotec | 802.11b | RP-XI305B | PCMCIA | Prism2/2.5/3 |
| Repotec | 802.11b | RP-WE300 | PCMCIA | Prism2/2.5/3 |
| RF TNC | 802.11b | 1100N | PCMCIA | Prism2/2.5/3 |
| Roper | 802.11g | RO80211G-USB | USB | Prism GT |
| Roper | 802.11g | RO80211G-PCI | PCI | Prism GT |
| Roper | 802.11g | RO80211G-CB | Cardbus | Prism GT |
| Samsung | 802.11 DS 2Mbps | SWL-1000 | PCMCIA | Prism 1 |
| Samsung | 802.11b | SWL-2000N | PCMCIA | Prism2/2.5/3 |
| Samsung | 802.11b | SWL-2000P | PCI | Prism2/2.5/3 |
| Samsung | 802.11b | SWL-2100E | PCMCIA | Prism2/2.5/3 |
| Samsung | 802.11b | SWL-2100N | PCMCIA | Prism2/2.5/3 |
| Samsung | 802.11b | SWL-2100P | PCI | Prism2/2.5/3 |
| Samsung | 802.11b | SWL-2200U | USB | Prism2/2.5/3 |
| Samsung | 802.11b | SWL-2200P | PCMCIA | Prism2/2.5/3 |

| | | | | |
|------------------------|---------|----------------|-------------|--------------|
| Samsung | 802.11b | SWL-2210P | PCI | Prism2/2.5/3 |
| Samsung | 802.11b | SWL-2210M | mini-PCI | Prism2/2.5/3 |
| Sandisk | 802.11b | SDWCFB-768 | CF | Prism2/2.5/3 |
| Senao/Engenius | 802.11b | SL-2511CD | PCMCIA | Prism2/2.5/3 |
| Senao/Engenius | 802.11b | SL-2511CD Plus | PCMCIA | Prism2/2.5/3 |
| Senao/Engenius | 802.11b | SL-2511CD Plus | PCMCIA | Prism2/2.5/3 |
| Senao/Engenius | 802.11b | SI-2511MP Plus | mini-PCI | Prism2/2.5/3 |
| Senao/Engenius | 802.11b | SL-2511CF | CF | Prism2/2.5/3 |
| Senao/Engenius | 802.11b | SL-2511UB | USB | Prism2/2.5/3 |
| Sitecom | 802.11b | WL-002 | PCMCIA | Prism2/2.5/3 |
| Sitecom | 802.11b | WL-010 | PCI adapter | Prism2/2.5/3 |
| Sitecom | 802.11b | WL-012 | USB | Prism2/2.5/3 |
| Sitecom | 802.11g | WL-100i | Cardbus | Prism GT |
| SmallBig | 802.11b | SBT-2100M | PCMCIA | Prism2/2.5/3 |
| SmallBig | 802.11b | SBT-2100U | USB | Prism2/2.5/3 |
| SOHOWare | 802.11b | NCP 130 | PCI | Prism2/2.5/3 |
| Siemens Speedstream | 802.11b | 1021 | PCMCIA | Prism2/2.5/3 |
| Siemens Speedstream | 802.11b | 1022 | USB | Prism2/2.5/3 |
| Siemens Speedstream | 802.11b | 1024 | PCI | Prism2/2.5/3 |
| SMC | 802.11b | 2532W-B | PCMCIA | Prism2/2.5/3 |
| SMC | 802.11b | 2632W | PCMCIA | Prism2/2.5/3 |
| SMC | 802.11b | 2602W | PCI | Prism2/2.5/3 |
| SMC | 802.11b | 2642W | CF | Prism2/2.5/3 |
| SMC | 802.11g | 2802W | PCI | Prism GT |
| SMC | 802.11g | 2835W | Cardbus | Prism GT |
| Sparklan | 802.11b | WL-311F | PCMCIA | Prism2/2.5/3 |
| Sparklan | 802.11b | WL-316C | PCMCIA | Prism2/2.5/3 |

เอกสารนี้เป็นเอกสารลิขสิทธิ์สงวนไว้สำหรับใช้ภายในเท่านั้น ไม่อนุญาตให้เผยแพร่ไปภายนอก

ไม่ว่ากรณีใดทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

| | | | | |
|---------------|--------------------|-------------|----------|--------------|
| Sparklan | 802.11b | WL-350F | mini-PCI | Prism2/2.5/3 |
| Sparklan | 802.11b | WL-360F | PCI | Prism2/2.5/3 |
| Sparklan | 802.11b | WL-672 | CF | Prism2/2.5/3 |
| Sparklan | 802.11g | WL-850F | mini-PCI | Prism GT |
| Sumtel | 802.11b | st-PC2111 | PCMCIA | Prism2/2.5/3 |
| 3Com | 802.11b | 3CRDW696 | PCI | Prism2/2.5/3 |
| 3Com | 802.11b | 3CRWE777A | PLX/PCI | Prism2/2.5/3 |
| 3Com | 802.11g | 3CRWE154G72 | Cardbus | Prism GT |
| TDK | 802.11b | LAK-CD011WL | PCMCIA | Prism2/2.5/3 |
| Tekram | 802.11b | PC400 | PCMCIA | Prism2/2.5/3 |
| Tekram | 802.11b | PCF200 | PCMCIA | Prism2/2.5/3 |
| Teletronics | 802.11 DS 2Mbps | WL-2000D | PCMCIA | PRISM 1 |
| Teletronics | 802.11b | WL-11000 | PCMCIA | Prism2/2.5/3 |
| Teletronics | 802.11b | WL-2400 | PCMCIA | Prism2/2.5/3 |
| Teletronics | 802.11b | WL-2400HP | PCMCIA | Prism2/2.5/3 |
| Teletronics | 802.11b | XI-626 | PCI | Prism2/2.5/3 |
| Tellus | 802.11b | C100 | PCMCIA | Prism2/2.5/3 |
| Tellus | 802.11b | C100A | PCMCIA | Prism2/2.5/3 |
| Tellus | 802.11b | C125 | PCMCIA | Prism2/2.5/3 |
| Tellus | 802.11b | C126S | PCMCIA | Prism2/2.5/3 |
| Tellus | 802.11b | P125 | PCI | Prism2/2.5/3 |
| Tellus | 802.11b | M125 | mini-PCI | Prism2/2.5/3 |
| Toko | 802.11b | TMW 1008 | PCMCIA | Prism2/2.5/3 |
| TRENDware | 802.11b | TEW-201PC | PCMCIA | Prism2/2.5/3 |
| TRENDware | 802.11b | TEW-203PI | PCI | Prism2/2.5/3 |
| TRENDware | 802.11b | TEW-PC16 | PCMCIA | Prism2/2.5/3 |
| TRENDware | 802.11b | TEW-PCI | PCI | Prism2/2.5/3 |
| Troy Wireless | 802.11b | ETHSC 001 | PCMCIA | Prism2/2.5/3 |

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปเผยแพร่โดยไม่ได้รับอนุญาต

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดลอกเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

| | | | | |
|---------------|---------|----------------|----------|--------------|
| Troy Wireless | 802.11b | ETHSC 002 | PCMCIA | Prism2/2.5/3 |
| Troy Wireless | 802.11b | ETHSC 006 | PCMCIA | Prism2/2.5/3 |
| Troy Wireless | 802.11b | ETHSC 007 | PCMCIA | Prism2/2.5/3 |
| Troy Wireless | 802.11b | ETHSU 001 | USB | Prism2/2.5/3 |
| Troy Wireless | 802.11b | ETHSU 003 | USB | Prism2/2.5/3 |
| Troy Wireless | 802.11b | ETHSU 006 | USB | Prism2/2.5/3 |
| Troy Wireless | 802.11b | ETHSU 007 | USB | Prism2/2.5/3 |
| Unex | 802.11b | MR011 | PCMCIA | Prism2/2.5/3 |
| Unex | 802.11b | UR012i | USB | Prism2/2.5/3 |
| Uniden | 802.11b | PCW 200 | PCI | Prism2/2.5/3 |
| US Robotics | 802.11b | USR2410 | PCMCIA | Prism2/2.5/3 |
| US Robotics | 802.11b | USR 2445 | PCMCIA | Prism2/2.5/3 |
| US Robotics | 802.11b | USR1120 | USB | Prism2/2.5/3 |
| USI | 802.11g | CB-G-IN-01 | Cardbus | Prism GT |
| USI | 802.11g | MP-G-IN-01(3A) | mini-PCI | Prism GT |
| Wisecom | 802.11b | GL 2411MU-A | USB | Prism2/2.5/3 |
| Wistron | 802.11b | PC-200 | PCMCIA | Prism2/2.5/3 |
| Wistron | 802.11b | PC-250 | PCMCIA | Prism2/2.5/3 |
| Wistron | 802.11b | USB-300 | USB | Prism2/2.5/3 |
| Wistron | 802.11b | USB-400 | USB | Prism2/2.5/3 |
| W-Link | 802.11b | WEN-2050 | CF | Prism2/2.5/3 |
| W-Link | 802.11b | WEN-2015 | PCMCIA | Prism2/2.5/3 |
| W-Link | 802.11b | WEN-2013 | PCMCIA | Prism2/2.5/3 |
| W-Link | 802.11b | WEN-2012 | PCMCIA | Prism2/2.5/3 |
| W-Link | 802.11b | WEN-2011 | PCMCIA | Prism2/2.5/3 |
| W-Link | 802.11b | WEN-2010 | PCMCIA | Prism2/2.5/3 |
| Wlinx | 802.11b | WB 1500 | PCMCIA | Prism2/2.5/3 |
| Xterasys | 802.11g | XN-2422G | Cardbus | PrismGT |
| Xterasys | 802.11g | XN-2522G | PCI | PrismGT |

เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ทางการค้า

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

| | | | | |
|---------------------|--------------------|--------------|----------|--------------|
| Xterasys | 802.11g | XG-600 | mini-PCI | PrismGT |
| Yamaha | 802.11b | YWL-11B5 | PCMCIA | Prism2/2.5/3 |
| YDI | 802.11 DS 2Mbps | WL 2400 PCM | PCMCIA | Prism 1 |
| YDI | 802.11b | Unknown | PCMCIA | Prism2/2.5/3 |
| Z-Com | 802.11b | XI300 | PCMCIA | Prism2/2.5/3 |
| Z-Com | 802.11b | XI300B | PCMCIA | Prism2/2.5/3 |
| Z-Com | 802.11b | XI325 | PCMCIA | Prism2/2.5/3 |
| Z-Com | 802.11b | XI325HP | PCMCIA | Prism2/2.5/3 |
| Z-Com | 802.11b | XI330B | PCMCIA | Prism2/2.5/3 |
| Z-Com | 802.11b | XI625 | mini-PCI | Prism2/2.5/3 |
| Z-Com | 802.11b | XI626 | PCI | Prism2/2.5/3 |
| Z-Com | 802.11b | XI725/726 | USB | Prism2/2.5/3 |
| Z-Com | 802.11b | XI735 | USB | Prism2/2.5/3 |
| Z-Com | 802.11b | XI750 | USB | Prism2/2.5/3 |
| Z-Com | 802.11b | XI815 | CF | Prism2/2.5/3 |
| Z-Com | 802.11b | XI825 | CF | Prism2/2.5/3 |
| Z-Com | 802.11g | XG300 | Cardbus | Prism GT |
| Z-Com | 802.11g | XG600 | mini-PCI | Prism GT |
| Z-Com | 802.11g | XG900 | PCI | Prism GT |
| Zoom Telephonics | 802.11 DS 2Mbps | ZoomAir 4000 | PCMCIA | Prism 1 |
| Zoom Telephonics | 802.11b | ZoomAir 4100 | PCMCIA | Prism2/2.5/3 |
| Zoom Telephonics | 802.11b | ZoomAir 4105 | PCI | Prism2/2.5/3 |
| Zoom Telephonics | 802.11b | 4103 | PCMCIA | Prism2/2.5/3 |
| Zonet | 802.11b | ZEW1000P | PCMCIA | Prism2/2.5/3 |
| Zyxel-Zyair | 802.11b | B-100 | PCMCIA | Prism2/2.5/3 |

| | | | | |
|-------------|---------|-------|----------|--------------|
| Zyxel-Zyair | 802.11b | B-200 | USB | Prism2/2.5/3 |
| Zyxel-Zyair | 802.11b | B-300 | PCI | Prism2/2.5/3 |
| Zyxel-Zyair | 802.11b | B-400 | Ethernet | Prism2/2.5/3 |
| Zyxel-Zyair | 802.11g | G-100 | Cardbus | Prism GT |

FILE CONTENTS COPYRIGHT ABSOLUTEVALUE SYSTEMS, INC. ** ALL RIGHTS
RESERVED ** FOR INFORMATION EMAIL BRUCE@LINUX-WLAN.COM



ประวัติผู้เขียนโครงการ

ชื่อผู้จัดทำโครงการ

นายสมเจ็ด โพธิ์ทอง

วันเดือนปีเกิด

25 กรกฎาคม 2520

สถานที่เกิด

จ.สุพรรณบุรี

ประวัติการศึกษา

ประถมศึกษา

โรงเรียนวัดโบสถ์คอนลำแพน จ.สุพรรณบุรี

มัธยมศึกษาตอนต้น

โรงเรียนสองพี่น้องวิทยา จ.สุพรรณบุรี

มัธยมศึกษาตอนปลาย

โรงเรียนสองพี่น้องวิทยา จ.สุพรรณบุรี

ปริญญาตรี

สถาบันราชภัฏหมู่บ้านจอมบึง จ.ราชบุรี



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้