บทที่ 2
เอกสาร และงานวิจัยที่เกี่ยวข้อง

ในการพัฒนาระบบลงทะเบียนและสนับสนุนการเข้าใช้เครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่ ผู้ศึกษาได้ค้นคว้าเอกสาร บทความ และงานวิจัยที่เกี่ยวข้องโดยมีรายละเอียดดังนี้

2.1 ความรู้เบื้องต้นเกี่ยวกับเครือข่ายไร้สาย

ศิวรักษ์ ศิวโมกษธรรม (2547) กล่าวถึงมาตรฐาน IEEE 802.11 ดังนี้

1) ความรู้เบื้องต้นเกี่ยวกับมาตรฐาน IEEE 802.11

มาตรฐาน IEEE 802.11 ซึ่งได้รับการตีพิมพ์ครั้งแรกเมื่อปี พ.ศ. 2540 โดย IEEE (The Institute of Electronic Engineers) และเป็นเทคโนโลยีสำหรับ WLAN ที่นิยมใช้กันอย่างแพร่หลายมากที่สุด คือ ข้อกำหนด (Specification) สำหรับอุปกรณ์ WLAN ในส่วนของ Physical (PHY) Layer และ Media Access Control (MAC) Layer โดยในส่วนของ PHY Layer มาตรฐาน IEEE 802.11 ได้กำหนดให้อุปกรณ์มีความสามารถในการรับส่งข้อมูลด้วยความเร็ว 1, 2, 5.5, 11 และ 54 Mbps. โดยมีสื่อ 3 ประเภทให้เลือกใช้ได้แก่ คลื่นวิทยุที่ความถี่สาธารณะ 2.5 GHz และ 5 GHz และอินฟาเรด (Infrared) (1 Mbps และ 2 Mbps เท่านั้น) สำหรับในส่วนของ MAC Layer มาตรฐาน IEEE 802.11 ได้กำหนดให้มีกลไกการทำงานที่เรียกว่า CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) ซึ่งมีความหมายคล้ายคลึงกับหลักการ CSMA/CD (Collision Detection) ของมาตรฐาน IEEE 802.11 Ethernet ซึ่งเป็นที่นิยมใช้กันทั่วไปในเครือข่าย LAN แบบใช้สายนำสัญญาณ นอกจากนี้ในมาตรฐาน IEEE 802.11 ยังกำหนดให้มีทางเลือกสำหรับสร้างความปลอดภัยให้กับเครือข่าย IEEE 802.11 WLAN โดยกลไกการเข้ารหัสข้อมูล (Encryption) และการตรวจสอบผู้ใช้ (Authentication) ที่มีชื่อเรียกว่า WEP (Wired Equivalent Privacy) ด้วย

2) วิวัฒนาการของมาตรฐาน IEEE 802.11

มาตรฐาน IEEE 802.11 มีความสามารถในการรับส่งข้อมูลด้วยความเร็ว 1 และ 2 Mbps ด้วยสื่อ อินฟราเรด (Infrared) หรือคลื่นวิทยุที่ความถี่ 2.4 GHz และมีกลไก WEP ซึ่งเป็นทางเลือกสำหรับความปลอดภัยให้กับเครือข่าย WLAN ได้ในระดับหนึ่ง เนื่องจากมาตรฐาน IEEE 802.11 เวอร์ชั่นแรกเริ่มนั้นมีประสิทธิภาพค่อนข้างต่ำ และไม่มีการรองรับหลักการ Quality of

Service (QoS) ซึ่งเป็นที่ต้องการของตลาด อีกทั้งกลไกรักษาความปลอดภัยที่ใช้ยังมีช่องโหว่อยู่มาก IEEE จึงได้จัดตั้งคณะทำงาน (Task Group) ขึ้นมาหลายชุดด้วยกันเพื่อทำการปรับปรุงเพิ่มเติมมาตรฐานให้มีศักยภาพสูงขึ้น คณะทำงานกลุ่มที่มีผลงานที่น่าสนใจ และเป็นที่รู้จักกันดีได้แก่ IEEE 802.11a, IEEE 802.11b, และ IEEE 802.11g

คณะทำงานชุด IEEE 802.11a ได้ตีพิมพ์มาตรฐานเพิ่มเติมนี้เมื่อปี พ.ศ. 2542 มาตรฐาน IEEE 802.11a ใช้เทคโนโลยีที่เรียกว่า OFDM (Orthogonal Frequency Division Multiplexing) เพื่อปรับปรุงความสามารถของอุปกรณ์ให้รับส่งข้อมูลได้ด้วยความเร็วสูงสุดที่ 54 Mbps แต่จะใช้คลื่นวิทยุที่ความถี่ 5 GHz ซึ่งเป็นย่านความถี่สาธารณะสำหรับใช้งานในประเทศสหรัฐอเมริกาที่มีสัญญาณรบกวนจากอุปกรณ์อื่นน้อยกว่าในย่านความถี่ 2.4 GHz อย่างไรก็ตาม ข้อเสียหนึ่งของมาตรฐาน IEEE 802.11a ที่ใช้คลื่นวิทยุความถี่ 5 GHz ก็คือ ในบางประเทศย่านความถี่ดังกล่าวไม่สามารถนำไปใช้งานได้อย่างสาธารณะ ตัวอย่างเช่น ประเทศไทยไม่อนุญาตให้มีการใช้งานอุปกรณ์ IEEE 802.11a เนื่องจากความถี่ย่าน 5 GHz ได้ถูกจัดสรรสำหรับกิจการอื่นอยู่ก่อนแล้ว นอกจากนี้ข้อเสียอีกอย่างหนึ่งของอุปกรณ์ IEEE 802.11a WLAN ก็คือ รัศมีของสัญญาณมีขนาดค่อนข้างสั้น (ประมาณ 30 เมตร ซึ่งสั้นกว่ารัศมีสัญญาณของอุปกรณ์ IEEE 802.11b WLAN ที่มีขนาดประมาณ 100 เมตร สำหรับการใช้งานภายในอาคาร) อีกทั้งอุปกรณ์ IEEE 802.11a WLAN ยังมีราคาสูงกว่า IEEE 802.11b WLAN ด้วย ดังนั้นอุปกรณ์ IEEE 802.11a WLAN จึงได้รับความนิยมน้อยกว่า IEEE 802.11b WLAN มาก

คณะทำงานชุด IEEE 802.11b ได้ตีพิมพ์มาตรฐานเพิ่มเติมนี้เมื่อปี พ.ศ. 2542 เช่นเดียวกัน ซึ่งเป็นที่รู้จักกันดี และใช้งานกันอย่างแพร่หลายมากที่สุดมาตรฐาน IEEE 802.11b ใช้เทคโนโลยีที่เรียกว่า CCK (Complimentary Code Keying) ผนวกกับ DSSS (Direct Sequence Spread Spectrum) เพื่อปรับปรุงความสามารถของอุปกรณ์ให้รับส่งข้อมูลได้ด้วยความเร็วสูงสุดที่ 11 Mbps ผ่านคลื่นวิทยุความถี่ 2.4 GHz เป็นย่านความถี่ที่เรียกว่า ISM (Industrial Scientific and Medical) ซึ่งถูกจัดสรรไว้อย่างสากลสำหรับการใช้งานอย่างสาธารณะด้านวิทยาศาสตร์ อุตสาหกรรม และการแพทย์ โดยอุปกรณ์ที่ใช้ความถี่ย่านนี้ก็เช่น IEEE 802.11, Bluetooth, โทรศัพท์ไร้สาย และเตาไมโครเวฟ ส่วนใหญ่แล้วอุปกรณ์ IEEE 802.11 WLAN ที่ใช้กันอยู่ในปัจจุบันจะเป็นอุปกรณ์ตามมาตรฐาน IEEE 802.11b นี้และใช้เครื่องหมายการค้าที่รู้จักกันดีในนาม Wi-Fi ซึ่งเครื่องหมายการค้าดังกล่าวถูกกำหนดขึ้นโดยสมาคม WECA (Wireless Ethernet Computability Alliance) โดยอุปกรณ์ที่ได้รับเครื่องหมายการค้าดังกล่าวได้ผ่านการตรวจสอบแล้วว่าเป็นไปตามมาตรฐาน IEEE 802.11b และสามารถนำไปใช้งานร่วมกับอุปกรณ์ยี่ห้ออื่นๆ ที่ได้รับเครื่องหมาย Wi-Fi ได้

ประมาณช่วงกลางปี พ.ศ. 2546 คณะทำงานชุด IEEE 802.11g ได้ตีพิมพ์มาตรฐานเพิ่มเติมนี้ โดยได้นำเทคโนโลยี OFDM มาประยุกต์ใช้ในช่องสัญญาณวิทยุความถี่ 2.4 GHz ซึ่งอุปกรณ์ IEEE 802.11g WLAN มีความสามารถในการรับส่งข้อมูลด้วยความเร็วสูงสุดที่ 54 Mbps ส่วนรัศมีสัญญาณของอุปกรณ์ IEEE 802.11g WLAN จะอยู่ระหว่ารัศมีสัญญาณของอุปกรณ์ IEEE 802.11a และ IEEE 802.11b เนื่องจากความถี่ 2.4 GHz เป็นย่านความถี่สาธารณะสากล อีกทั้งอุปกรณ์ IEEE 802.11g WLAN สามารถทำงานร่วมกับอุปกรณ์ IEEE 802.11b WLAN ได้ (backward-compatible) อุปกรณ์ IEEE 802.11g WLAN จึงได้รับความนิยมอย่างแพร่หลาย

อนันต์ ผลเพิ่ม (2547) กล่าวถึงการตั้งค่าการรักษาความปลอดภัยเครือข่ายไร้สายว่า เทคโนโลยี Wireless local area network (WLAN) ได้กลายเป็นทางเลือกเครือข่ายที่นิยมใช้ในการเชื่อมต่อเครื่องคอมพิวเตอร์หลายเครื่องในบ้านหรือธุรกิจขนาดเล็ก แม้ว่าเครือข่ายไร้สายจะให้ความยืดหยุ่นในเรื่องสถานที่ แต่ก็เพิ่มความเสี่ยงให้กับคอมพิวเตอร์และสภาพแวดล้อมการทำงานในเครือข่าย อีกทั้งยังเพิ่มประเด็นด้านการรักษาความปลอดภัยที่ไม่มีในเทคโนโลยีเครือข่ายแบบมีสายทั่วไป เช่น การเชื่อมต่อแบบอีเทอร์เน็ต ประเด็นเรื่องความปลอดภัยที่กล่าวถึงมีดังต่อไปนี้

1) ข้อกำหนดการตรวจสอบเพื่อระบุว่าคอมพิวเตอร์ใดบ้างที่ได้รับอนุญาตให้เข้าร่วมในเครือข่ายไร้สาย

2) การตั้งค่าการเข้ารหัสที่อธิบายถึงวิธีการเข้ารหัสข้อมูลที่ส่งแบบไร้สาย เพื่อไม่ให้ผู้ลักลอบสามารถแปลข้อมูลที่ส่ง หรือเข้าใช้ทรัพยากรในเครือข่าย เช่น โฟลเดอร์ที่ใช้งานร่วมกันได้

Microsoft Support (2006) กล่าวถึงการรักษาความปลอดภัยด้วย WPA ว่า มาตรฐานการรักษาความปลอดภัยด้วย WPA ประกอบด้วย

1) การพิสูจน์ตัวตนผู้ใช้ด้วยมาตรฐาน IEEE 802.1x เป็นส่วนประกอบจำเป็นในการรักษาความปลอดภัยด้วย WPA เมื่อใช้งาน WPA ร่วมกับ RADIUS Server สามารถใช้งาน Extensible Authentication Protocol (EAP) เป็นโปรโตคอลในการพิสูจน์ตัวตนของผู้ใช้ โดยทำการตั้งค่าให้ RADIUS Server รองรับการใช้ EAP และตั้งค่าที่เครื่องลูกข่ายให้เลือกใช้โปรโตคอลดังกล่าวในการติดต่อกับเครื่องแม่ข่ายให้ตรงกัน

2) การจัดการรหัสที่ใช้ในการเข้ารหัสสำหรับการใช้ระบบรักษาความปลอดภัยด้วย WPA จำเป็นจะต้องมีการเลือกใช้รหัสในการเข้ารหัส ซึ่งวิธีการจัดการรหัสแบบ Temporal Key Integrity Protocol (TKIP) วิธีการนี้จะทำการเปลี่ยนแปลงรหัสไปเรื่อยๆในทุกๆเฟรมของสัญญาณที่ส่งระหว่างอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายกับเครื่องคอมพิวเตอร์ โดยจะเปลี่ยนแปลงตรงกันทั้งสองฝ่าย หากผู้ไม่ประสงค์ดีสามารถจับรหัสได้ ก็ไม่สามารถจะใช้รหัสนั้น

กับเฟรมต่อมา เนื่องจากมีค่าเริ่มต้นที่ไม่ได้ตรงกันทั้งสองด้าน เป็นการป้องกันไม่ให้ถูกขโมยข้อมูลในการสื่อสารระหว่างอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายกับเครื่องคอมพิวเตอร์

2.2 ความรู้เกี่ยวกับ RADIUS Server

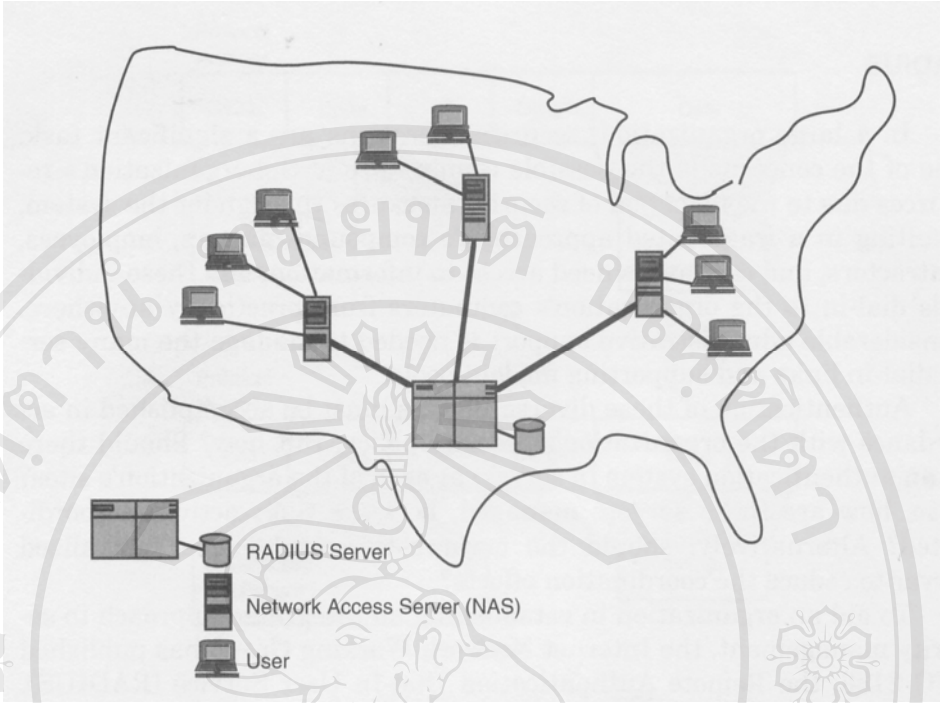
Uyless Black(2000) กล่าวว่าในองค์กรขนาดใหญ่การจัดการเกี่ยวกับระบบรักษาความปลอดภัยระบบเครือข่ายถือเป็นเรื่องที่สำคัญมาก ประเด็นที่จะต้องเป็นห่วงคือ เรื่องของการจัดการทรัพยากรของระบบซึ่งเป็นตัวชี้วัดที่เกี่ยวเนื่องกับการรักษาความปลอดภัย ในหลาย ๆ หน่วยงานอาจจะมีการเข้าถึงทรัพยากรขององค์กรผ่านระบบโทรเข้า ไม่ว่าจะเป็นลูกค้าหรือพนักงานขององค์กรซึ่งผู้ดูแลระบบจะต้องมีการจัดการการเชื่อมต่อระบบโทรเข้า และการจัดการอุปกรณ์ที่รองรับการเชื่อมต่อระบบโทรเข้าหรือระบบโมเด็มพูล (Modem Pool)

ด้วยเหตุนี้องค์กรจะต้องมีการวางแผนนโยบาย เพื่อจัดการในเรื่องของการตรวจสอบสิทธิ (Authentication System) ในการใช้งานทรัพยากรระบบด้วยซึ่งในการที่จะจัดการนั้นองค์กรที่ทำงานเกี่ยวข้องกับระบบเครือข่ายสากลหรือ Internet Network Working Group ได้จัดสร้างมาตรฐาน RFC2138 ขึ้นมาซึ่งโดยทั่วไปแล้วจะเรียกว่า Remote Authentication Dial-In User Service หรือเรียกย่อ ๆ ว่า RADIUS โดยที่มาตรฐานดังกล่าวได้กล่าวถึงขั้นตอนในการทำงานของเครื่องให้บริการตรวจสอบสิทธิ์ในการเข้าใช้งานระบบ (Authentication Server) โดยที่จะมีการจัดการเกี่ยวกับฐานข้อมูลกลางที่จะทำการแยกแยะผู้ใช้งานระบบโทรเข้าและข้อมูลต่าง ๆ ของผู้ใช้งานที่มีสิทธิเข้าใช้งานระบบ

การทำงานของ RADIUS นั้นสามารถทำงานร่วมกันระหว่างเครื่องแม่ข่ายทั้งที่เป็นระบบ RADIUS เหมือนกัน และแม้กระทั่งกับเครื่องแม่ข่ายที่ไม่ได้ทำงานแบบ RADIUS ด้วยการทำงานเช่นนี้ ทำให้ RADIUS Server นั้นสามารถทำงานเป็นตัวแทน (Proxy) สำหรับเครื่องแม่ข่ายอื่น ๆ ได้ด้วยยกตัวอย่างเช่น ระบบ PPP, rlogin และ telnet เป็นต้น

2.2.1 โครงสร้างระบบ RADIUS

ในรูป 2.1 แสดงโครงสร้างระบบ RADIUS เป็นการทำงานในรูปแบบของ Client-Server ผู้ใช้งานจะทำการติดต่อไปยัง Network Access Server (NAS) ผ่านระบบโทรเข้า ในทำนองเดียวกัน NAS ก็จะเปรียบเสมือนเป็น Client ของ RADIUS Server ซึ่งอาจจะเชื่อมต่อผ่านระบบเครือข่าย (Network) หรือแบบจุดต่อจุด (Point-to-Point Link) ก็ได้ และดังที่กล่าวมาข้างต้น RADIUS Server ก็อาจจะมีการติดต่อกับเครื่องแม่ข่ายที่เป็น RADIUS เหมือนกันหรือต่างระบบกันก็ได้ โดยที่ระบบทั้งหมดจะมีการใช้ฐานข้อมูลกลางร่วมกัน



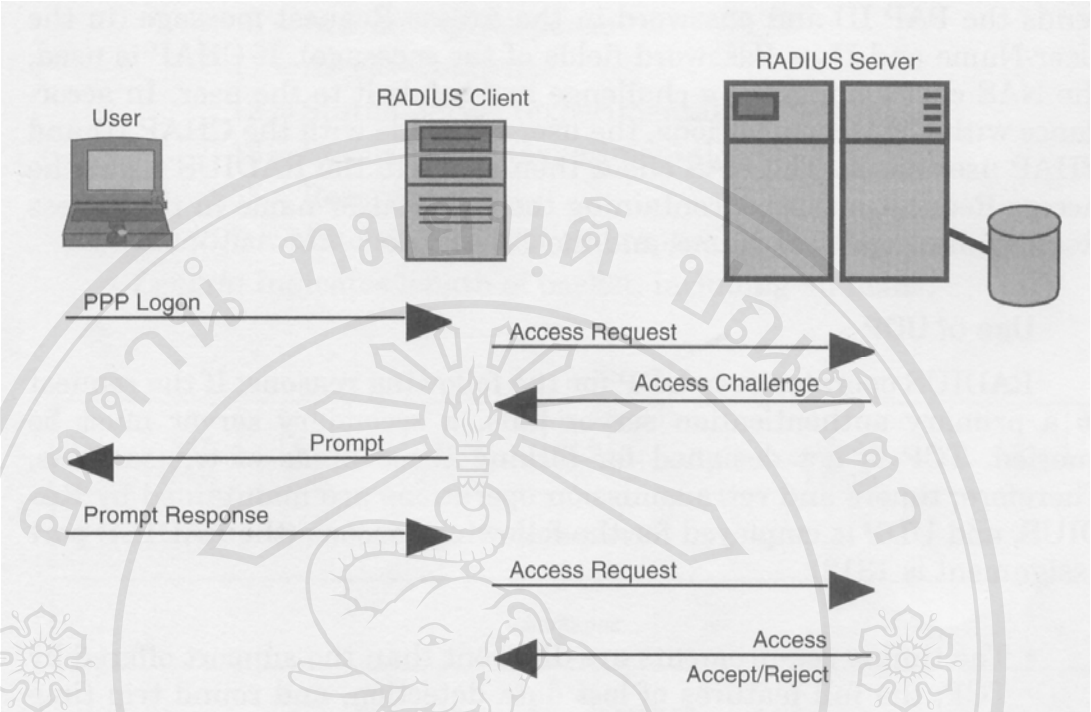
รูป 2.1 RADIUS Setup

ผู้ใช้งานจะต้องมีการส่งข้อมูลเกี่ยวกับการตรวจสอบสิทธิ์ให้แก่ NAS ได้แก่ รหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) หรือไม่ก็ PP Authentication Packet และหลังจากนี้ Client จะทำการติดต่อกับระบบ RADIUS โดยที่จะทำการสร้าง Access Request Message เพื่อติดต่อกับ RADIUS Node ซึ่งใน message จะประกอบไปด้วยข้อมูลต่าง ๆ ที่เกี่ยวข้องซึ่งจะเรียกว่า Attribute ซึ่งจะถูกกำหนดโดยระบบ RADIUS ยกตัวอย่างเช่น รหัสผ่าน, พอร์ตปลายทาง (Destination Port), Client ID เป็นต้น

สำหรับข้อมูลที่มีความสำคัญ เช่น รหัสผ่าน (Password) นั้นจะต้องมีการเข้ารหัสแบบ MD5 โดยจะมีการใช้ Key ในการเข้ารหัสข้อมูลร่วมกัน (Share Key)

1) ตัวอย่างการแลกเปลี่ยนข้อมูลของ RADIUS

ข้อมูล (Message) ที่ร้องขอ (Request) จากเครื่องลูกข่าย (Client) จะต้องมีการใช้กุญแจในการเข้ารหัสร่วมกัน (Share Secret Key) ดังรูป 2.2 ในกรณีที่ Secret Key ของ Client ไม่ตรงกับเครื่องแม่ข่าย (server) แล้วจะทำให้ Request Message ถูกปฏิเสธ และจะไม่มีการประมวลผลในขั้นตอนต่อไป แต่ถ้า Key ตรงกันแล้ว server จะทำการตรวจสอบข้อมูลกับฐานข้อมูลกลางเพื่อทำการตรวจสอบข้อมูลของผู้ใช้ (user) ต่อไป



รูป 2.2 ตัวอย่างการแลกเปลี่ยน Message ของ RADIUS

เมื่อขั้นตอนการตรวจสอบสิทธิเบื้องต้นโดย share secret key เป็นที่เรียบร้อยแล้ว RADIUS Server จะทำการสร้าง Access Challenge message ให้แก่ RADIUS Client และ Client ก็จะทำการส่งผ่านต่อไปให้กับ user ในรูปแบบของ Prompt เพื่อรับข้อมูล สำหรับ message ที่ทำการส่งผ่านให้แก่ user นั้น อาจจะมีการเพิ่มเติมในบางส่วน เช่น ข้อมูลเกี่ยวกับการเข้ารหัสข้อมูลกลับไปให้ RADIUS Client เพื่อทำการส่งให้ RADIUS Server ต่อไป

เมื่อ Server ได้รับ message จาก user และผ่านการตรวจสอบตามเงื่อนไขผ่านแล้ว Server จะทำการส่งกลับ Access Accept จะประกอบไปด้วยข้อมูลต่าง ๆ ได้แก่ PPP, Login user เป็นต้น เพื่อที่จะให้ RADIUS Client ทำการกำหนดค่าต่าง ๆ ให้แก่ user ต่อไป ยกตัวอย่างเช่น IP Address, compression services, Maximum Transmission Unit (MTU) เป็นต้น

2) RADIUS กับการใช้ UDP

เหตุผลที่ RADIUS เลือกใช้งาน UDP Protocol ที่หมายเลข Port มาตรฐาน คือ 1812 นั้น มีเหตุผลที่เลือกใช้ UDP Protocol ดังนี้

- หาก request ที่ไปยัง RADIUS Server หลักทำงานผิดพลาด ก็จะมีการทำงานของ RADIUS Server ตัวที่สองแทน ซึ่ง TCP Protocol นั้นไม่สามารถทำได้
- เวลาที่ต้องการใช้งาน RADIUS นั้นไม่เหมาะสมกับการใช้ TCP Protocol เนื่องจากไม่มีความจำเป็นที่จะต้องทำการตรวจสอบการสูญหายของข้อมูล (lost data detection) และค่า Round

Trip Time (RTT) ที่จะต้องใช้ในการส่งข้อมูลซ้ำนั้นไม่มีความจำเป็นต้องใช้ เนื่องจาก user จะได้ไม่ต้องรอการตรวจสอบในระยะเวลานาน ๆ เมื่อเกิดความผิดพลาดในการส่งข้อมูล เนื่องจากสามารถเลือกใช้ server อื่นแทนได้

- ในกรณีที่เกิดการปิดหรือเปิดระบบใหม่ของทั้ง Client และ Server นั้นถ้ามีการใช้ TCP Protocol นั้นจะทำให้ยากต่อการจัดการการเชื่อมต่อ
- การใช้ UDP Protocol นั้นง่านต่อการทำ multi-threading โดยที่ user อาจทำการสร้าง Process ในการทำ Authentication หลาย ๆ Process พร้อมกันได้

0	2-7	8	9	10-14	15	16	18-30	31
Code			Identifier			Length		
Authenticator								
Attributes…								

รูป 2.3 The RADIUS Packet

3) รูปแบบข้อมูล RADIUS

รูป 2.3 แสดงถึงรูปแบบ Packet ข้อมูลของ RADIUS โดยที่แต่ละ Packet ของ RADIUS นั้นจะใช้การส่งข้อมูลแบบ UDP Packet โดยจะมี field ต่างๆ ดังนี้

- **Code** : บ่องบอกถึงชนิดของ RADIUS Packet ต่าง ๆ ดังนี้

1 = Access-Request
2 = Access-Accept
3 = Access-Reject
4 = Accounting-Request
5 = Accounting-Response
11 = Access-Challenge
12 = Status-Server (experimental)
13 = Status-Client (experimental)
255 = Reserved

- **Identifier** : บ่งบอกถึง requests และ replies ที่ตรงกัน
- **Length** : บ่งบอกถึงความยาวของ packet โดยรวมทุก ๆ field
- **Authenticator** : ใช้ในการทำการตรวจสอบสิทธิ์ (Authenticate) โดยจะตอบกลับจาก RADIUS server โดยใน Access Request Packet ของ Client นั้นจะประกอบไปด้วยเลขฐาน 8 จำนวน 16 หลัก ที่ทำการสุ่มขึ้นมา เรียกกว่า Request Authenticator ซึ่งค่านี้จะใช้ secret key ร่วมกับการเข้ารหัสแบบ MD5 สร้างขึ้นมาโดยจะทำการ Logical Operator แบบ XOR กับรหัสผ่านของ User อีกทีส่วนใน Access Accept, Accepts Reject หรือ Access Challenge Packet นั้นจะเรียกว่า Respond Authenticator โดยการเข้ารหัสแบบ MD5 จาก field Request Authenticator ใน Access-Request Packet ซึ่งประกอบไปด้วย field ต่าง ๆ ดังนี้คือ code, identifier, length และ Authenticator
- **Attributes** : เป็นส่วนที่บ่งบอกข้อมูลต่าง ๆ ซึ่งมีความจำเป็นในการติดต่อกันระหว่าง RADIUS node ในระบบเพื่อจะทำการ authentication, authorization และ configuration ในมาตรฐาน RFC 2138 ได้กำหนดมาตรฐานของ RADIUS Attributes นี้ ซึ่ง Attributes ที่สำคัญต่าง ๆ จะได้อธิบายต่อไป แต่ในบางส่วนเช่น address, name, port number ซึ่งสามารถเข้าใจความหมายได้ไม่ยากนั้นจะไม่ได้กล่าว

■ *Service-type Attribute* เป็น Attribute ที่บ่งบอกถึงประเภทของ Service ที่ผู้ใช้งานร้องขอ ซึ่งมี Service ต่าง ๆ ดังนี้

- Login : คือ ชื่อผู้ใช้งานที่จะติดต่อ
- Framed : คือ โปรโตคอลที่ผู้ใช้งานใช้ เช่น PPP เป็นต้น
- Callback Login : จะทำให้ผู้ใช้งานยกเลิกการเชื่อมต่อและเชื่อมต่อไปอีกครั้ง
- Callback framed : จะทำให้ผู้ใช้งานยกเลิกการเชื่อมต่อและเชื่อมต่อใหม่อีกครั้งด้วยโปรโตคอลที่ต้องการ
- Outbound : เป็นการอนุญาตให้ผู้ใช้งานสามารถใช้ส่งข้อมูลออกผ่านอุปกรณ์ที่ใช้ในการเชื่อมต่อ
- Administrative : เป็นการอนุญาตให้ผู้ใช้งานสามารถเข้าใช้ส่วนติดต่อผู้ใช้งานผ่าน NAS ได้
- NAS prompt : ผู้ใช้งานจะได้รับหน้าจอรับคำสั่ง (command prompt) ในการเข้าใช้งาน NAS

- Authenticate only : จะทำการร้องขอสิทธิการใช้งานได้เท่านั้น โดยที่จะไม่ต้องการข้อมูลเกี่ยวกับสิทธิ์จาก Access-Accept (โดยทั่วไปจะถูกใช้โดย proxy servers มากกว่าตัว NAS เอง)
- Callback NAS prompt : ผู้ใช้งานจะถูกยกเลิกการเชื่อมต่อและเชื่อมต่อกลับอีกครั้ง โดยได้รับหน้าจอรับคำสั่ง (command prompt) ในการเข้าใช้งาน NAS

- *Framed-MTU* เป็นการกำหนดค่าหน่วยในการส่งข้อมูลสูงสุดหรือMTU (Maximum
Transmission unit) สำหรับผู้ใช้งาน
- *Login-IP-Host* ใช้บอกเครื่องแม่ข่ายของระบบที่ผู้ใช้งานทำการเชื่อมต่อ
- *Login-Service* บ่งบอกถึงบริการที่จะให้ผู้ใช้งาน Login เข้าใช้งาน ยกตัวอย่างเช่น telnet, rlogin และ LAT เป็นต้น
- *Callback-Number* ใช้บอกค่า dialing string ในการใช้เรียกกลับ
- *Framed-Route* ใช้บอกข้อมูลการหาเส้นทางการเชื่อมต่อ (Routing Information) ให้แก่ผู้ใช้งาน
- *Session-Timeout* เป็นการตั้งค่าสูงสุดในหน่วยวินาทีก่อนจะที่ทำการยกเลิกการเชื่อมต่อเมื่อไม่มีการส่งผ่านข้อมูล
- *Idle-Timeout* เป็นการตั้งค่าสูงสุดในหน่วยวินาทีที่จะอนุญาตให้ไม่มีการส่งผ่านข้อมูล ก่อนจะทำการยกเลิกการเชื่อมต่อ
- *Termination-Action* เป็นการบ่งชี้ว่าเมื่อสิ้นสุดการให้บริการแล้ว NAS จะทำงานอย่างไรต่อ
- *Calling-Station-ID* บ่งบอกถึง calling party number
- *Proxy-State* ถูกส่งโดย proxy server ไปยัง server อื่นเมื่อ proxy server ทำการส่งผ่าน Access-Request message
- *NAS-Port-Type* เป็นการบ่งชี้ถึง physical port ของ NAS ซึ่งใช้ในการทำการตรวจสอบผู้ใช้งาน ยกตัวอย่างเช่น asynchronous, synchronous, ISDN asynchronous V.120, และ ISDN asynchronous V.110 เป็นต้น

2.3 บทความและงานวิจัยที่เกี่ยวกับเครือข่ายไร้สาย

อนันต์ ผลเพิ่ม (2547) ได้อธิบายไว้ในวารสารสำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์ว่า แนวทางในการพัฒนาเครือข่ายไร้สาย ในเบื้องต้น เพื่อให้ผู้ใช้สามารถเริ่มต้นใช้งานได้ จึงควรมีระบบสำหรับให้ผู้ใช้สามารถลงทะเบียนเข้าใช้งานด้วยตนเองได้สะดวก แต่ในระยะต่อมาของการพัฒนาเครือข่าย ควรต้องมีการจัดระบบบริหารจัดการเครือข่าย เพื่อให้สามารถตรวจสอบติดตามข้อมูลผู้ใช้ สถานภาพการใช้งาน และสภาพของทรัพยากรเครือข่ายไร้สายที่ใช้ เพื่อจะเป็นประโยชน์แก่การบริหารและจัดการ รวมไปถึงการวางแผนงานในการขยายเครือข่ายได้เหมาะสม

ศิวรักษ์ ศิวโมกษธรรม (2547) ให้รายละเอียดในบทความเรื่องมาตรฐาน IEEE 802.11WLAN:ความรู้เบื้องต้นและการรักษาความปลอดภัยว่า การใช้งานเครือข่ายไร้สายนั้น แม้ว่าจะมีวิธีการรักษาความปลอดภัยในเบื้องต้น แต่ในการใช้งานจริงนั้น ลักษณะของเทคโนโลยีเครือข่ายไร้สาย สามารถทำการดักฟังได้โดยง่าย จึงควรใช้มาตรการความปลอดภัยในระดับที่สูงเพียงพอและมีระบบตรวจสอบควบคุมผู้ใช้อย่างเหมาะสม ในกรณีที่เป็นองค์กรควรเลือกติดตั้งอุปกรณ์ที่รองรับมาตรฐาน IEEE 802.1x และสนับสนุนการทำงานร่วมกับ RADIUS (Remote Authentication Dial-In User Service) เพื่อเสริมในการตรวจสอบผู้ใช้ ในเครือข่ายไร้สาย ให้มีความปลอดภัยสูงขึ้น

ทศพล เหลืองวัฒนะพงศ์ (2547) ได้ศึกษาในงานวิจัยเรื่องระบบตรวจสอบไวร์เลสแอคเซสพอยน์ด้วยการตรวจจับสัญญาณในระยะไกล ซึ่งเป็นงานวิจัยในโครงการกลุ่มงานวิจัยเครือข่ายไร้สาย มหาวิทยาลัยเกษตรศาสตร์ โดยกล่าวถึงการใช้งานเครือข่ายไร้สายที่เข้ามามีบทบาทต่อการเพิ่มขึ้นของการใช้งานระบบเครือข่าย เนื่องจากความสะดวกในการติดตั้งและการใช้งาน แต่สิ่งที่น่าสนใจคือ ความปลอดภัยของการใช้งานเครือข่ายไร้สาย จุดอ่อนของเครือข่ายไร้สายมาจากลักษณะสมบัติ “ไร้สาย” ที่เป็นช่องทางให้ดักจับข้อมูลได้ง่ายกว่าเครือข่ายที่ใช้สาย การดูแลและป้องกันจึงเข้ามามีบทบาท โครงงานที่จัดทำขึ้นอยู่ในส่วนของการดูแลความปลอดภัยเกี่ยวกับไวร์เลสแอคเซสพอยน์เนื่องจากในองค์กร ขนาดใหญ่ เช่น มหาวิทยาลัย ถ้านำระบบไร้สายมาใช้จะต้องติดตั้งไวร์เลสแอคเซสพอยน์กระจายตามพื้นที่ต่างๆ เป็นบริเวณกว้าง และทำให้ต้องใช้ไวร์เลสแอคเซสพอยน์เป็นจำนวนมาก ทำให้การดูแลตรวจสอบเป็นไปอย่างไม่ทั่วถึง ปัญหาหนึ่งที่อาจก่อให้เกิดอันตรายกับการใช้งานเครือข่ายไร้สายก่อคือ อาจจะมีผู้ไม่ประสงค์ดีตรวจจับสัญญาณโดยไม่ได้รับอนุญาต ทำให้สามารถเข้าถึงข้อมูลภายในองค์กรได้