การพัฒนาโปรแกรมควบคุมการใช้งานอินเตอร์เน็ตจากระยะไกล แบบใช้ข้อตกลงร่วมกัน

System Development of Internet Roaming Remote Access Server

โดย

นายนฤพนธ์ พนาวงศ์

รหัส 42067113

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
ภาคการเรียนที่ 1 ปีการศึกษา 2544
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	การพัฒนาโปรแกรมควบคุมการใช้งานอินเตอร์เน็ตจากระยะไกลแบบใช้ข้อตกลงร่วมกัน
นักศึกษา	นายนฤพนธ์ พนาวงศ์
อาจารย์ที่ปรึกษา	อาจารย์อัครินทร์ คุณกิตติ
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2544

บทคัดย่อ

พัฒนาโปรแกรมควบคุมการใช้งานอินเตอร์เน็ตจากระยะไกลแบบใช้ข้อตกลงร่วมกัน โดยผู้ใช้ติดต่อเข้ามาใช้งานด้วยการ dial-up ซึ่งใช้ e-mail address เพื่อให้ทราบถึง Server ที่ผู้ใช้ลงทะเบียนไว้ในระบบเครือข่ายในกรณีที่ตรวจสอบไม่พบใน Local Server จะไปตรวจสอบที่เซิร์ฟเวอร์ใดตามที่ได้ทำการตกลงร่วมกันโดยมีตารางเก็บข้อมูลเซิร์ฟเวอร์ที่ทำการตกลงร่วมกันเพื่อให้ใช้ข้ามเครื่องได้ภายใต้ข้อตกลงร่วมกัน ทำให้ทำการ Authentication, Authorization และ Accounting ได้ถูกต้อง โดยทำการพัฒนาระบบบนระบบปฏิบัติการ Linux 6.1 Thai (Mandrake) ใช้ภาษา C ในการพัฒนาระบบในส่วนของ AAA ที่ใช้ TACACS+ Protocol ติดต่อกับ AAA Server ซึ่งใช้วิธีการแบบ Peer-To-Peer และใช้ PHP พัฒนาในส่วน Admin ที่ควบคุมการทำงานผ่าน Web Browser เพื่อกำหนดค่าของระบบและดูรายงานการใช้งานต่าง ๆ โดยมี mySQL เป็น Database Server และใช้ Apache เป็น Web Server

Title	System Development of Internet Roaming Remote Access Server
Student	Mr.Narupon Panawong
Advisor	Mr.Akharin Khunkitti
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	2001

ABSTRACT

System Development of Internet Roaming Remote Access Server. The user connects by dial-up that uses e-mail address to discover the server that is registered in the network when they check is not found in the local serer, to check in the server that is roaming that keep data to roaming table for used machine cross is roaming, the authentication, authorization and accounting is correct. Develop on linux 6.1 thai operating system. C & PHP language, Database is mySQL, Apache is Web Server. Connect AAA server by TACACS+ Protocol, Peer-To-Peer Methodology and Administrator interface with graphic work on web browser.

กิตติกรรมประกาศ

โครงการพัฒนาระบบงานนี้สำเร็จได้เพราะได้รับการส่งเสริม และสนับสนุนจากบุคคลหลายท่าน กระผมจึงใคร่ขอกราบขอบพระคุณ

- บิดาและมารดาที่ได้อบรมสั่งสอนและสนับสนุนส่งเสียให้ได้เล่าเรียนจบประสบความสำเร็จในการศึกษา
- อาจารย์อัครินทร์ คุณกิตติ ที่ได้ให้ความกรุณาให้คำปรึกษาแนะนำสิ่งต่าง ๆ ในโครงการพัฒนาระบบงาน
- คุณสมภพ วชิรลาภไพฑูรย์ รุ่นพี่ IS6 ภาคสมทบ ที่แบ่งปันความรู้และให้คำแนะนำในการพัฒนาระบบเป็นอย่างดี
- อาจารย์ทุก ๆ ท่านที่ได้ประสิทธิ์ประสาทความรู้ หลักวิชาการต่าง ๆ เพื่อเป็นพื้นฐานในการดำเนินชีวิตและการทำงาน
- เจ้าหน้าที่คณะเทคโนโลยีสารสนเทศทุกท่านที่ให้คอยอำนวยความสะดวกอย่างดี
- สำนักคอมพิวเตอร์ฯและโปรแกรมวิชาวิทยาการคอมพิวเตอร์ สถาบันราชภัฏนครสวรรค์ที่ให้ความร่วมมือในการทดสอบระบบและอุปกรณ์ต่าง ๆ ที่ใช้ในการพัฒนาระบบ
- เพื่อน ๆ IS8.1 ทุกท่านที่ได้กำลังใจ และให้คำแนะนำดี ๆ เสมอมา
- น้อง ๆ IS10 โดยเฉพาะ P-MAN เพื่อนร่วมห้องช่วยชี้แนะวิธีการเขียน DFD และ ER

นายนฤพนธ์ พนาวงศ์

สารบัญ

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญรูปภาพ

หน้า

ภาพที่

บทที่ 1
บทนำ

1.1 ความเป็นมา

ในปัจจุบันการติดต่อสื่อสาร ได้รับความนิยมอย่างมาก ทำให้ระบบเครื่อข่ายต้องเพิ่มความจุให้มากขึ้น ทำให้จำนวนอุปกรณ์เครือข่าย (Network Access Server) มากขึ้นตามปริมาณผู้ใช้ทำให้ เกิดปัญหาใหม่คือทำอย่างไรจึงจะสามารถควบคุมการเข้าออกของผู้ใช้บริการแต่ละคนได้ตามที่ต้องการ และเมื่อผู้ใช้ (โดยเฉพาะระดับผู้บริหาร) ที่มีการเดินทางไปมาอยู่ตลอดเวลาซึ่งต้องทำการตรวจสอบงานต่าง ๆ หรือสั่งงานทางอินเตอร์เน็ต หรือ ส่งข้อมูลสำคัญ ๆ ทำให้ต้องสมัครสมาชิกใช้งานอินเตอร์เน็ตกับท้องที่นั้น ๆ ซึ่งไม่สะดวกและเป็นการยุ่งยากอีกทั้งยังเสียค่าใช้จ่ายโดยไม่จำเป็น ดังนั้น Internet Roaming ซึ่งเป็นแนวทางใหม่ที่ผู้ใช้จะใช้ e-mail address ในการ dial-up เข้ามาใช้งานอินเตอร์เน็ต แต่ Server เหล่านั้นจะต้องทำการตกลงร่วมกันก่อนเพื่อให้สามารถทำขบวนการ Authentication, Authorization และ Accounting ได้อย่างถูกต้อง

ในระบบเครือข่ายขนาดใหญ่ การเข้มงวดในการรักษาความปลอดภัยมีความสำคัญมาก ผู้ดูแลระบบจะต้องป้องกันระบบเครือข่ายและทรัพยากรของเครือข่ายจากผู้ที่ไม่มีสิทธิ์ใช้ โดยมีหลักการดังนี้ Authentication, Authorization, Accounting หรือ AAA

AAA Protocols ถูกพัฒนาขึ้นมาเพื่อใช้รักษาความปลอดภัยในระบบเครือข่าย โดย AAA Protocols นั้นจะทำหน้าที่ติดต่อกับ AAA Servers เพื่อตรวจสอบสิทธิในการเข้าถึง (Authentication), ตรวจสอบสิทธิในการใช้งาน (Authorization) และบันทึกการใช้งาน (Accounting) เมื่อผู้ใช้มีสิทธิในการใช้งานทรัพยากรบนระบบเครือข่าย

การตรวจสอบสิทธิในการเข้าถึง (Authentication) คือ การพิจารณาว่าผู้ใช้คนนั้นคือใคร อาจจะทำได้หลายแบบ เช่น ใช้ชื่อผู้ใช้และรหัสผ่านคงที่ โดยทั่วไปจะใช้วิธีนี้ ซึ่งนี้มีจุดอ่อนด้านความปลอดภัย วิธีที่ทันสมัยขึ้นอาจจะใช้ รหัสผ่านแบบครั้งเดียว (one-time password) หรือแบบโต้ตอบ (challenge and response query) การตรวจสอบสิทธิในการเข้าถึง จะขึ้นอยู่กับนโยบายของผู้ควบคุม บางที่อาจจะมี บางที่อาจจะไม่มี

การตรวจสอบสิทธิในการใช้งาน (Authorization) คือ การพิจารณาว่าบริการใดบ้างที่อนุญาตให้ผู้ใช้ ใช้ได้ โดยทั่วไปแล้วการตรวจสอบสิทธิในการเข้าถึงจะทำก่อนการตรวจสอบสิทธิในการใช้งาน โดยสามารถกำหนดบริการที่จะให้ผู้ใช้แต่ละคนใช้ได้ไม่เหมือนกัน บริการต่างๆ เช่น

command shell, PPP, etc. TACACS+ Server จะตอบรับการขอใช้บริการ โดยอนุญาตให้ใช้บริการแต่จะไม่จำกัดเวลาในการใช้

การบันทึกการใช้งานของผู้ใช้ (Accounting) คือการบันทึกว่าผู้ใช้ทำอะไร มีจุดประสงค์ 2 อย่าง คือ เก็บข้อมูลเพื่อจัดทำระบบ Billing หรือ เพื่อตรวจสอบในระบบรักษาความปลอดภัย ข้อมูลที่บันทึกประกอบด้วย ข้อมูลเกี่ยวกับการตรวจสอบสิทธิในการใช้บริการ และข้อมูลทรัพยากรที่ใช้ไป การบันทึกมี 3 ลักษณะ คือ แจ้งเริ่มใช้ระบบ (start), แจ้งเลิกใช้ระบบ (stop), ปรับปรุงในขณะที่ใช้งานอยู่

1.2 วัตถุประสงค์ในการพัฒนาระบบ

- เพื่อพัฒนาระบบที่ทำหน้าที่เป็นศูนย์กลางในการควบคุมอุปกรณ์เครือข่าย เกี่ยวกับการตรวจสอบสิทธิการใช้บริการเครือข่ายของผู้ใช้บริการ
- เพิ่มประสิทธิภาพในการจัดการทรัพยากร ทั้งบุคลากร และอุปกรณ์เครือข่ายให้มากขึ้น
- เพิ่มความสะดวกในการใช้งาน โดยผู้ใช้ไม่ต้องลงทะเบียนกับทุก ๆ Server ที่เข้าไปใช้งาน และทำให้จดจำได้ง่ายเพราะใช้เพียงรหัสเดียว (E-mail Address)
- เพื่อให้สามารถใช้งานใช้ข้ามเครื่องได้ภายใต้ข้อตกลงร่วมกัน

1.3 ขอบเขตของการพัฒนาระบบงาน

ระบบนี้ทำการพัฒนาโดยมีพื้นฐานจากโปรแกรมควบคุม TACACS+ Server ผ่าน web ที่ถูกพัฒนาขึ้นมาแล้วในรุ่นก่อน โดยมีรายละเอียดของพัฒนาที่จะพัฒนาขึ้นมาใหม่ดังต่อไปนี้

- ข้อมูลยังคงเก็บอยู่ในฐานข้อมูล MySQL เช่นเดิม โดยเพิ่มตาราง Roaming เพื่อเก็บ domain name ที่ใช้ในการทำข้อตกลงร่วมกัน
- เพิ่มข้อมูลสถานะของการ Roaming, จำนวนครั้งในการเข้ามาใช้งานต่อวันและจำนวนนาทีที่จะใช้งานได้ต่อเดือนในตารางของผู้ใช้
- ปรับปรุงระบบการตรวจสอบสิทธิในการเข้าถึง, ตรวจสอบสิทธิในการใช้งานและบันทึกเวลาการใช้งานของผู้ใช้ลงในฐานข้อมูล โดยมีรูปแบบ Roaming ที่ผู้ใช้ติดต่อเข้ามาในระบบโดยใช้ e-mail address เพื่อบ่งบอกข้อมูลของ domain name ที่ใช้สำหรับเงื่อนไข Roaming
- ปรับปรุงส่วนการติดต่อผู้บริหารระบบเครือข่ายผ่านทาง Web Browser โดยผู้ใช้จะต้องลงทะเบียนในฐานข้อมูลผู้ใช้ด้วยและสามารถตรวจสอบเวลาการใช้งาน (Audit) ได้เพื่อให้ผู้ใช้

สามารถทราบจำนวนเวลา (นาที) ที่ใช้ไปแล้วในแต่ละเดือน, จำนวนครั้งที่เคยเข้าใช้งานในกรณีที่ผู้ใช้ไม่ได้เป็นผู้บริหารเครือข่าย

- ปรับปรุงรายงาน (ทาง Web Browser) โดยเพิ่มรายละเอียดเกี่ยวกับ Roaming เช่น ผู้ใช้ที่เข้ามาใช้งานเป็นแบบ Roaming หรือไม่เป็น Roaming
- ใช้ TACACS+ Protocol เพื่อติดต่อกับ AAA Server โดยทำการพัฒนาด้วยภาษาซีในส่วนของ Protocol ต่อจากรุ่นก่อน
- ใช้วิธี Roaming แบบ Peer-To-Peer

1.4 องค์ประกอบและเครื่องมือในการพัฒนาระบบงาน

1.4.1 องค์ประกอบด้านฮาร์ดแวร์

- เครื่องคอมพิวเตอร์สำหรับให้บริการ AAA (AAA Server)
- เครื่องคอมพิวเตอร์สำหรับให้บริการฐานข้อมูล (Database Server)
- เครื่องคอมพิวเตอร์สำหรับผู้ใช้ในการขอใช้บริการเครือข่าย
- เครื่องคอมพิวเตอร์สำหรับผู้บริหารระบบเครือข่าย
- อุปกรณ์เครือข่าย (Network Access Server)

1.4.2 องค์ประกอบด้านซอฟท์แวร์

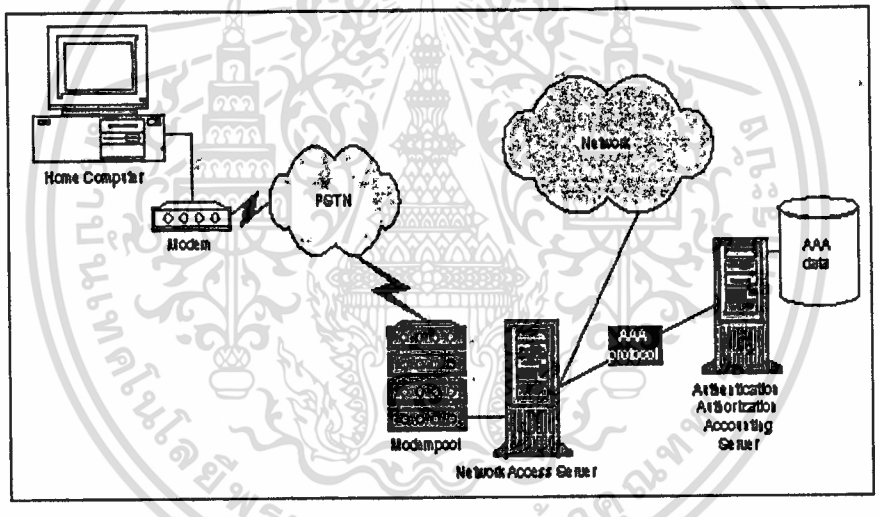
- Operating System : Linux 6.1 Thai (Mandrake)
- Web Server : Apache 1.3.14
- DBMS : MySQL 3.22.32-pc-Linux-gnu-i686
- Web Browser : Internet Explorer 5.00 or More
- Tool : PHP 4.0.4pl1 with MySQL Client API ใช้ในการพัฒนาส่วนการติดต่อผ่าน Web Browser, C API for MySQL ใช้พัฒนา TACACS+ Protocol ที่มีส่วนการติดต่อกับ AAA Server

บทที่ 2

AAA Protocol and Internet Roaming

2.1 AAA Protocol

AAA Protocol ถูกพัฒนาขึ้นมาเพื่อใช้รักษาความปลอดภัยในระบบเครือข่ายโดย AAA Protocol นั้นจะทำหน้าที่ติดต่อกับ AAA Server เพื่อตรวจสอบสิทธิในการเข้าถึง (Authentication), ตรวจสอบสิทธิในการใช้งาน (Authorization) และบันทึกการใช้งาน (Accounting) เมื่อผู้ใช้มีสิทธิในการใช้งานทรัพยากรบนระบบเครือข่าย



รูปที่ 2.1 แสดง AAA Architecture

จากรูปที่ 2.1 แสดงการทำงานเมื่อผู้ใช้ Dial-up เข้ามายัง NAS (Network Access Servers) AAA Protocols จะทำหน้าที่ติดต่อไปยัง AAA Servers เพื่อตรวจสอบสิทธิในการเข้าถึง (Authentication), ตรวจสอบสิทธิในการใช้งาน (Authorization) และบันทึกการใช้งาน (Accounting) เมื่อผู้ใช้เข้ามาใช้งานในระบบเครือข่าย

AAA Protocols ได้ถูกพัฒนาออกไปในหลายรูปแบบ โดยที่นิยมใช้คือ RADIUS Protocol และ TACACS+ Protocol

2.2 RADIUS Protocol

RADIUS (Remote Authentication Dial-In User Service) เป็น AAA protocol ซึ่งถูกพัฒนาโดย Livingston Enterprise Incorporation RADIUS Draft 5 ถูกยอมรับจาก IETF ให้เป็น draft standard ในเดือนมิถุนายน ปี 1996 RADIUS เป็น fully open protocol ซึ่งเผยแพร่ในรูปของ source code ซึ่งสามารถทำการแก้ไขเพื่อใช้งานกับระบบรักษาความปลอดภัยในปัจจุบันที่มีอยู่ในตลาดได้ RADIUS Protocol ประกอบด้วย 3 ส่วนดังนี้

1. Protocol ในรูปแบบ Frame ซึ่งใช้ UDP/IP
2. Server หรือผู้ให้บริการ AAA
3. Client หรือผู้ขอใช้บริการ AAA

2.2.1 ลักษณะเด่น

- Client/Server Model

  NAS ทำงานเป็น client ของ RADIUS โดย Client จะทำหน้าที่ส่งข้อมูลของผู้ใช้ให้กับ RADIUS server ที่กำหนดไว้แล้ว จากนั้นก็ปฏิบัติตามข้อมูลที่ได้รับกลับ RADIUS server ทำหน้าที่รับข้อมูลของผู้ใช้ และส่งข้อกำหนดของผู้ใช้กลับไปให้ client เพื่อให้บริการต่อผู้ใช้ต่อไป RADIUS Server สามารถทำตัวเป็น proxy client สำหรับ RADIUS Server ตัวอื่นได้หรือเป็น Authentication เพื่อจุดประสงค์อื่น ๆ

- Network Security

  ข้อมูลที่รับส่งกันระหว่าง RADIUS Server และ NAS ใช้วิธี share secret และในส่วนของ user password จะถูก encrypt เพื่อป้องกันไม่ให้ผู้ใดที่ดักจับข้อมูลอยู่ไม่สามารถอ่าน user password ออก

- วิธี Authentication ที่ยืดหยุ่น

  RADIUS Server สนับสนุนวิธี Authentication นอกเหนือจากวิธีพื้นฐานได้แก่ PPP, PAP หรือ CHAP , UNIX login และอื่น ๆ

- สามารถเพิ่มขยายได้

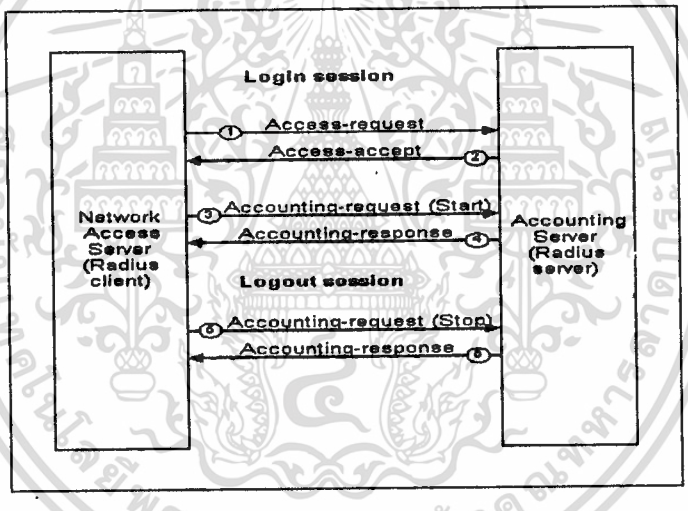
  ข้อมูลที่รับส่งนั้น ประกอบไปด้วยตัวแปรต่าง ๆ ซึ่งสามารถเพิ่มเติมได้ โดยไม่รบกวนการพัฒนา Protocol

2.2.2 นิยาม

Session แต่ละบริการจาก NAS คือ session ซึ่งการเริ่ม session นั้นเริ่มพร้อมกับบริการที่เริ่มขึ้น และการสิ้นสุดของ session พร้อมกับบริการที่สิ้นสุด ผู้ใช้สามารถมี session ได้หลาย session ขึ้นอยู่กับการสนับสนุนของ NAS

NAS (Network Access Server) คืออุปกรณ์ใด ๆ ที่ให้บริการติดต่อกับผู้ใช้ (Access Service) ปัจจุบัน NAS ทำหน้าที่มากกว่าเพียงแค่ Terminal Server ซึ่งให้บริการ charecter mode front end โดยจะอนุญาตให้ผู้ใช้ telnet หรือ rlogin ไปยัง host อื่น ๆ NAS อาจจะสนับสนุน protocol หลายตัวเช่น PPP, ARAP, LAT, XREMOTE และอื่น ๆ

2.2.3 RADIUS Message Flow



รูปที่ 2.2 แสดงการทำงานของ RADIUS

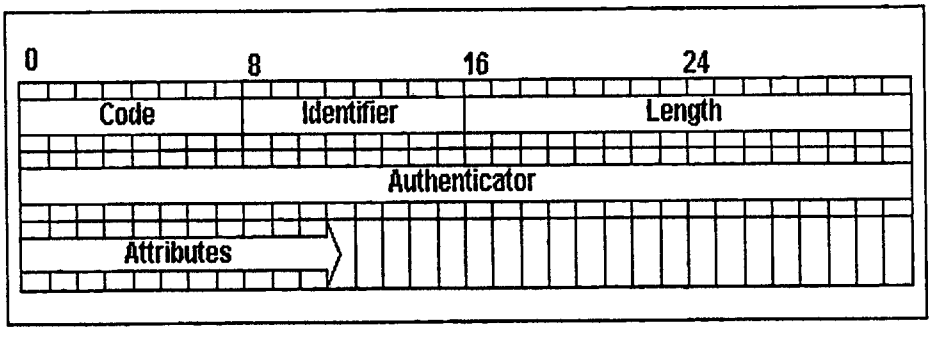
จากรูปที่ 2.2 อธิบายการทำงานได้ดังนี้

1. เมื่อผู้ใช้ต้องการเข้าสู่ระบบเครือข่ายจะต้องมีการป้อนชื่อและรหัสผ่านจากนั้น NAS จะส่งข้อมูลเหล่านี้พร้อมค่า Attribute ต่าง ๆ เช่น IP Address ของ NAS, ID ของ NAS, พอร์ตของ NAS ที่ผู้ใช้เชื่อมต่อ โดยค่าเหล่านี้จะถูกส่งไปในเฟรม Access-Request เพื่อให้ Server ทำการตรวจสอบ หลังจากที่ NAS ส่งเฟรม Access-Request จะถูกส่งไปยัง Server แล้วจะรอ Response จาก Server ถ้าไม่ได้รับ Response ภายในช่วงเวลาที่กำหนด NAS จะพยายามส่งเฟรม Request ไปใหม่ จนกระทั่งถ้าครบจำนวนครั้งตามที่กำหนดไว้แล้ว NAS ก็จะทำการส่งเฟรม Request ต่อไปให้ Backup Server เมื่อเซิร์ฟเวอร์ได้รับ

เฟรม Request ก็จะทำการตรวจสอบ Share Secret Key ก่อนเพื่อใช้ตรวจสอบว่าเป็น Client ของตัวเองหรือไม่ ถ้าไม่เหมือนกัน Server จะทิ้งเฟรมนั้น แต่ถ้าเป็น Key เดียวกัน Server จะทำการตรวจสอบชื่อผู้ใช้, รหัสผ่าน และค่า Attribute อื่น ๆ

2. เมื่อป้อนชื่อผู้ใช้ถูกต้อง Server จะส่งเฟรม Access-Accept กลับไปให้ NAS พร้อมทั้งส่งค่า Attribute ต่าง ๆ เพื่อใช้กำหนดสิทธิการใช้งานของ User เช่น กำหนดระยะเวลาการใช้งานของ User, Framed Protocol, การกำหนดขนาดของ Framed-MTU เป็นต้น และถ้าชื่อผู้ใช้ไม่ถูกต้อง Server จะส่งเฟรม Access-Reject กลับไปให้ NAS จากนั้น NAS จะทำการยกเลิกการติดต่อของผู้ใช้รายนั้น
3. NAS จะส่งเฟรม Accounting-Request (Start)เพื่อเข้าสู่ระบบ (Accounting phase)
4. RADIUS Server จะส่งเฟรม Accounting-response กลับไปยัง NAS เมื่อ Accounting ได้บันทึกข้อมูลเรียบร้อยแล้ว
5. เมื่อผู้ใช้เลิกใช้งาน NAS จะส่งเฟรม Accounting-request (Stop) พร้อมกับข้อมูลดังต่อไปนี้ให้กับ RADIUS Server
   - เวลาที่พยายามส่งข้อมูล (Delay)
   - ระยะเวลาในการใช้งาน
   - จำนวน Packet ที่ใช้รับและส่ง
   - สาเหตุที่ผู้ใช้เลิกติดต่อหรือเลิกใช้งาน
6. RADIUS Server จะส่งเฟรม Accounting-response กลับไปยัง NAS เมื่อ Accounting ได้บันทึกข้อมูลเรียบร้อยแล้ว โดยข้อมูลที่ Accounting Server เก็บจะถูกจัดเก็บเป็น Log File ใน Server

2.2.4 RADIUS Packet Format



รูปที่ 2.3 แสดง RADIUS Packet Format

จากรูปที่ 2.3 แสดงรูปแบบของ RADIUS Packet โดย RADIUS ส่ง packet แบบ UDP port 1812 มีรูปแบบดังนี้

Code - กำหนดชนิดของ RADIUS packet มีขนาด 8 bits ดังแสดงตามตารางที่ 2.1

Code	Description
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

ตารางที่ 2.1 แสดง RADIUS Code Packet

Identifier - กำหนดว่าเป็น Request และ Reply packet เดียวกัน

Length - กำหนดความยาวของ packet รวมทั้ง Code, Identifier, Length และ Attribute field ถ้า packet ที่มีความยาวสั้นกว่าที่ค่า Length field ให้เพิกเฉย packet นั้น ความยามที่น้อยที่สุด คือ 20 ความยาวมากที่สุด คือ 4096

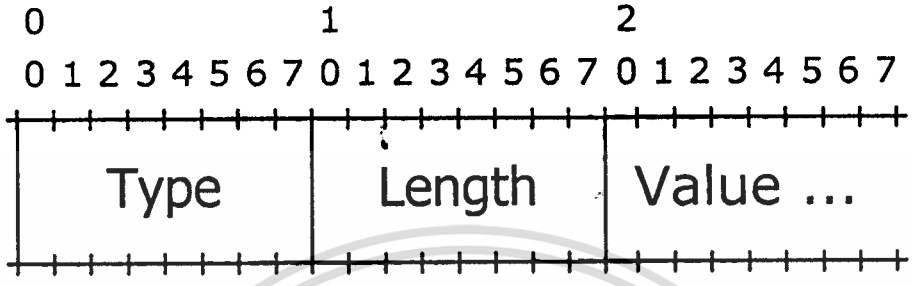
Authenticator - มีขนาด 16 bytes เป็นข้อมูลที่ถูกใช้ในรวจสอบเวลา reply จาก server และใช้เป็นส่วนหนึ่งของ password hiding algorithm โดยแบ่งออกเป็น

- Request Authenticator ใช้ใน Access-Request Packets และจะเป็นค่าสุ่มไปเรื่อย ๆ
- Response Authenticator คือ ค่าของ Authenticator field ใน Access-Accept, Access-Reject และ Access-Challenge Packet เป็นค่าที่ได้จากการเข้ารหัสด้วยวิธี MD5 ซึ่งจะนำค่าของ Code, Id, Length, Request Authenticator, Attribute และ secret มาทำการเข้ารหัส

Attribute - กำหนดค่าของ Attribute ต่าง ๆ

2.2.5 Attributes

RADIUS Attribute แสดงถึงข้อมูลที่ใช้ในการ Authentication, Authorization และ Accounting มีรูปแบบดังนี้



รูปที่ 2.4 แสดงรูปแบบของ Attributes

RADIUS Client / Server จะเพิกเฉยต่อ Attribute ที่มี type ไม่มีในตารางต่อไปนี้

Attribute Type	Description
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
9	Framed-IP-Netmask
10	Framed-Routing
11	Filter-Id
12	Framed-MTU
13	Framed-Compression
14	Login-IP-Host
15	Login-Service

Attribute Type	Description
16	Login-TCP-Port
17	(unassigned)
18	Reply-Message
19	Callback-Number
20	Callback-id
21	(unassigned)
22	Framed-Route
23	Framed-IPX-Network
24	State
25	Class
26	Vender-Specific
27	Session-Timeout
28	Idle-Timeout
29	Termination-Action
30	Called-Station-id
31	Calling-Station-id
32	NAS-Identifier
33	Proxy-State
34	Login-LAT-Service
35	Login-LAT-Node
36	Login-LAT-Group
37	Framed-AppleTalk-Link
38	Framed-AppleTalk-Network
39	Framed-AppleTalk-Zone
40-59	(Accounting Reserve)
60	CHAP-Challenge
61	NAS-Port-Type
62	Port-Limit

Attribute Type	Description
63	Login-LAT-Port
192-223	(Experimental Reserve)
224-240	(Implementation Reserve)
241-255	(Unused Reserve)

ตารางที่ 2.2 แสดงAttribute Type

2.2.6 สรุปการทำงาน

เมื่อ client ถูกกำหนดให้ใช้ RADIUS เมื่อมีผู้ใช้มาขอใช้บริการ ผู้ใช้อาจจะคาดหวังว่าจะต้อง input username และ password ที่ login prompt อย่างไรก็ตามผู้ใช้อาจจะใช้ link framing protocol เช่น Point-to-Point (PPP) ซึ่งมี Authentication packet ในการส่งข้อมูล

เมื่อ client ได้รับข้อมูลแล้วจะทำการสร้าง Access Request ซึ่งมีข้อมูล username, password, ID ของ client, เลขที่ port ที่ผู้ใช้บริการใช้ โดย password จะถูกซ้อนด้วยเทคนิค RSA Message Digest Algorithm MD5

เมื่อ client ส่ง Access Request ออกไปแล้วและ server ไม่ตอบกลับภายในระยะเวลาที่กำหนดค่าหนึ่ง client จะทำการส่งออกไปอีกครั้ง หรือส่งออกไป server อีกตัวในกรณี server ตัวหลักไม่สามารถให้บริการได้

เมื่อ RADIUS server ได้รับ Access Request จากนั้น server จะทำการตรวจสอบ กรณีที่ Access Request มาจาก client ที่ RADIUS server ไม่มี shared secret อยู่ Request นั้นจะถูกเพิกเฉย ส่วนกรณีที่ RADIUS server มี shared secret ของ client นั้น ๆ อยู่ RADIUS จะทำการตรวจสอบกับฐานข้อมูลว่ามี username ตรงกับใน Access Request หรือไม่ ข้อมูลของผู้ใช้ในฐานข้อมูลประกอบด้วย บริการที่อนุญาตให้ใช้ รวมถึง password และอาจจะกำหนดถึง client และ port ที่อนุญาตให้ใช้งานด้วย

RADIUS server อาจจะส่ง Request ไปยัง server ตัวอื่นได้ในกรณีที่ทำหน้าที่เป็น client ด้วย ถ้าเงื่อนไขไม่ตรงกัน RADIUS server จะส่ง Access-Reject ไปยัง client เพื่อบอกว่า Request ที่ส่งมานั้นเป็นโมฆะ และ server อาจจะส่งข้อความมากับ Access-Reject เพื่อบอกผู้ใช้ด้วย ไม่มี attribute ที่ถูกอนุญาตใน Access-Reject

ถ้าเงื่อนไขทั้งหมดตรงกัน RADIUS จะส่ง Access-Challenge ไปยัง client โดยใน Access-Challenge อาจจะมีข้อความเพื่อบอกให้ผู้ใช้ตอบกลับ client จะส่ง Access-Request มี request ID

ใหม่ พร้อมส่งข้อมูลจากผู้ใช้และสถานะของ attribute จาก Access-Challenge ซึ่งจะมีค่า 0 หรือ 1 เท่านั้น จากนั้น server สามารถตอบรับ Access-Request ใหม่นี้ โดยการส่ง Access-Accept, Access-Reject หรือ Access-Challenge อื่น ๆ

ถ้าเงื่อนไขทั้งหมดตรงกัน ค่าของข้อกำหนดของผู้ใช้ จะถูกส่งไปใน Access-Accept ค่าเหล่านั้นรวมถึงประเภทของบริการเช่น SLIP, PPP หรือ Login User และค่าอื่นๆ ที่มีความจำเป็นสำหรับ SLIP และ PPP จะมีค่าของ IP Address, sub netmask, MTU, compression และ packet filter identifiers สำหรับบริการ Character Mode อาจจะรวมค่า protocol และ host

2.3 TACACS+ protocol

TACACS+ คือ TACACS (Terminal Access Controller Access Control System) ที่ถูกพัฒนาต่อมาล่าสุด TACACS คือ protocol ที่ใช้ควบคุมการเข้าถึงทรัพยากร ที่ใช้ UDP อย่างง่าย ๆ เริ่มแรกถูกพัฒนาโดย BBN (MILNET) Cisco System Incorporation ได้ทำการพัฒนาต่อโดยเรียกว่า XTACACS และต่อมาพัฒนามาเป็น TACACS+ ปรับปรุงมาจาก TACACS และ XTACACS โดยจะแยกหน้าที่ทั้ง 3 อย่างชัดเจน ได้แก่ Authentication, Authorization และ Accounting และยังทำการ encrypt packet ทุก packet ที่ส่งระหว่าง client (Network Access Server) และ Server (daemon)

TACACS+ protocol specification version 1.76 ถูกยอมรับจาก IETF ในเดือนตุลาคม ปี 1996 เป็น Information Internet draft

2.3.1 ลักษณะเด่น

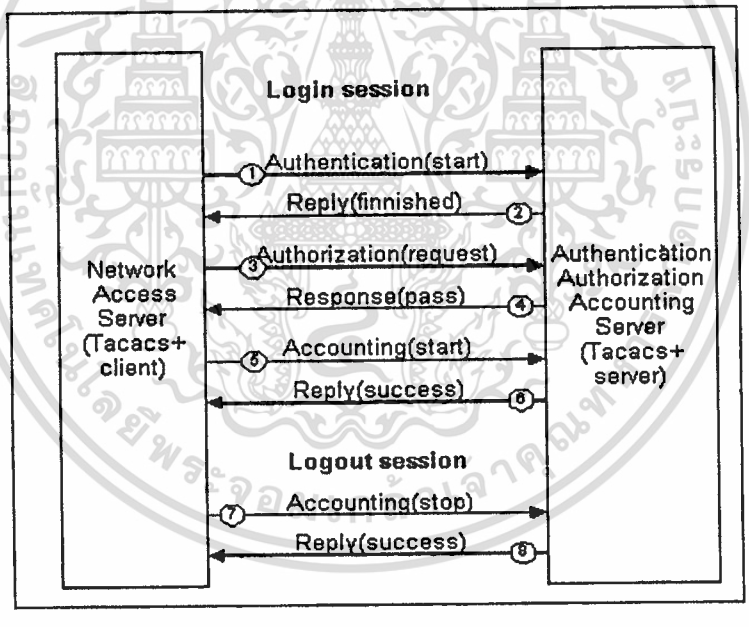
- TACACS+ แบ่งแยกการทำงาน AAA ออกจากกัน
- TACACS+ สนับสนุน การตรวจสอบสิทธิในการใช้คำสั่งของ router
- TACACS+ สนับสนุน privilege level ถึง 16 ระดับ (0-15)
- TACACS+ สนับสนุน การควบคุมบริการต่างๆ เช่น Point-to-Point Protocol (PPP), shell standard login, enable privilege, AppleTalk Remote Access (ARA) protocol, Novell Asynchronous Service Inerface (NASI), remote command (RCMD) และ firewall proxy
- TACACS+ สนับสนุน การจำกัด port ในการให้บริการ เช่น TTY, VTY หรือ Interface ของ router

2.3.2 นิยาม

Session TACACS+ session เป็นลำดับการตรวจสอบสิทธิในการเข้าถึง, ใช้แลกเปลี่ยนในการตรวจสอบสิทธิในการใช้, ข้อมูลอ้างอิงที่ใช้ในการบันทึกข้อมูลของผู้ใช้ session_id มีความสำคัญมากเพราะเป็นส่วนหนึ่งที่ใช้ในการเข้ารหัส และใช้เป็นตัวแบ่งแยกในระบบ Multiple Session ซึ่งทั้ง Server และ Client จะต้องรองรับได้

NAS (Network Access Server) คืออุปกรณ์ใด ๆ ที่ให้บริการติดต่อกับผู้ใช้ (Access Service) ปัจจุบัน NAS ทำหน้าที่มากกว่าเพียงแค่ Terminal Server ซึ่งให้บริการ character mode front end โดยจะอนุญาตให้ผู้ใช้ telnet หรือ rlogin ไปยัง host อื่น ๆ NAS อาจจะสนับสนุน protocol หลายตัวเช่น PPP, ARAP, LAT, XREMOTE และอื่น ๆ

2.3.3 TACACS+ Message Flow



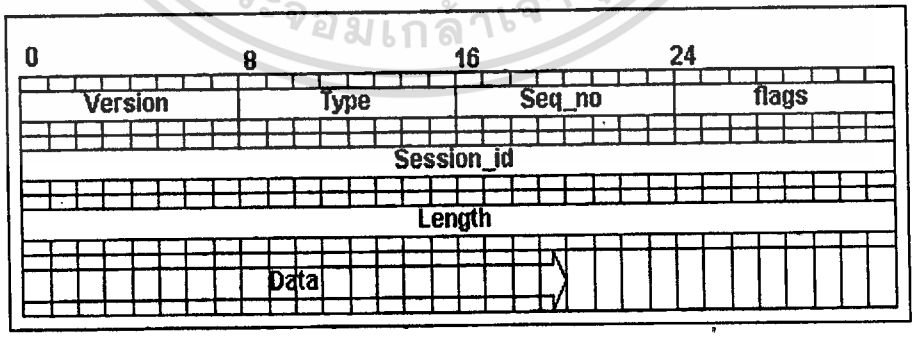
รูปที่ 2.5 แสดงการทำงานของ TACACS+

จากรูปที่ 2.5 อธิบายการทำงานได้ดังนี้

1. เมื่อผู้ใช้ต้องการเข้าสู่ระบบเครือข่ายจะต้องมีการป้อนชื่อและรหัสผ่าน จากนั้น NAS จะส่งข้อมูลพร้อมค่า Attribute ต่าง ๆ ไปยัง TACACS+ Server (Authentication phase) เป็นการเริ่มต้นเพื่อทำการตรวจสอบสิทธิการเข้าถึงของผู้ใช้

2. เมื่อชื่อผู้ใช้และรหัสผ่านถูกต้อง TACACS+ Server จะส่งเฟรม Reply (finished) กับมาที่ NAS
3. เมื่อ NAS ได้รับการตอบกลับจาก Server แล้วจะส่งเฟรม Authorization (request) เพื่อตรวจสอบสิทธิในการใช้งาน
4. Server จะส่งเฟรม Response (Pass) เมื่อผู้ใช้มีสิทธิในการใช้งาน โดยเฟรมข้อมูลจะประกอบไปด้วย ระยะเวลาใช้งาน เป็นต้น
5. NAS จะส่งเฟรม Accounting (Start) เพื่อเข้าสู่ระบบ (Accounting phase)
6. TACACS+ Server จะส่งเฟรม Reply (Success) เมื่อ Accounting Server บันทึกข้อมูลเรียบร้อยแล้ว
7. เมื่อผู้ใช้เลิกใช้งาน NAS จะส่งเฟรม Accounting (Stop) พร้อมกับข้อมูลดังต่อไปนี้ให้กับ TACACS+ Server
   - เวลาเริ่มต้น, เวลาสิ้นสุด
   - ระยะเวลาที่เข้ามาใช้งาน
   - จำนวน Packet และ Byte ที่รับและส่ง
   - สาเหตุที่ผู้ใช้เลิกติดต่อหรือเลิกใช้งาน
8. TACACS+ Server จะส่งเฟรม Reply (Success) กลับไปยัง NAS เมื่อ Accounting ได้บันทึกข้อมูลเรียบร้อยแล้ว

2.3.4 TACACS+ packet header



รูปที่ 2.6 แสดง TACACS+ Packet Format

จากรูปที่ 2.6 TACACS+ Packet ทั้งหมดจะต้องประกอบด้วย 12 bytes header ส่วน header จะไม่เข้ารหัส โดยมีรายละเอียดดังนี้

1. major_version (4 bits) คือ version หลักของ TACACS+ โดยทั่วไป = 0xc
2. minor_version (4 bits) คือ version ย่อยของ TACACS+ โดยทั่วไป = 0x0
3. type (1 bytes) คือ ประเภทของ TACACS+ packet
   - 0x01 คือ การตรวจสอบสิทธิในการเข้าถึง (Ahthentication)
   - 0x02 คือ การตรวจสอบสิทธิในการใช้งาน (Authorization)
   - 0x03 คือ การบันทึกการใช้งานของผู้ใช้ (Accounting)
4. seq_no (1 bytes) คือ ลำดับที่ของ packet โดย packet แรก = 1
5. encryption (1 bytes) คือ กำหนดการเข้ารหัสของ TACACS+ packet body
   - 0x00 คือ body of TACACS+ packet เข้ารหัส
   - 0x01 คือ body of TACACS+ packet ไม่เข้ารหัส
6. session_id (4 bytes) คือ ID ของ TACACS+ session เลือกโดยการสุ่ม
7. length (4 bytes) คือความยาวของ TACACS+ packet body (ไม่รวม header) หน่วยเป็น byte

2.3.5 TACACS+ packet body

ประเภทของ TACACS+ packet body กำหนดจาก header โดยมีกฎเกณฑ์ดังนี้

- Body packet จะถูกป้องกันด้วยการเข้ารหัสที่กำหนดมาจาก header
- ตัวแปรทั้งที่มีความยาวคงที่และไม่คงที่ ที่ไม่ใช้จะมีความยาวเป็น 0
- ข้อมูลและข้อความของ TACACS+ packet ต้องไม่ลงท้ายด้วย null
- ความยาวมีหน่วยเป็น byte

2.3.5.1 การเข้ารหัส packet body

Body of TACACS+ packet อาจจะถูกเข้ารหัส วิธีการเข้ารหัสวิธีเดียวเท่านั้นจะถูกใช้สำหรับ 1 session การเข้ารหัสจะเชื่อถือใน secret key ซึ่งทั้ง Server และ Client จะต้องใช้ secret key เดียวกัน การจัดการเกี่ยวกับ secret key จะเป็นหน้าที่ของ Server

TAC_PLUS_ENCRYPTED หลักการของการเข้ารหัสมีดังนี้

ENCRYPTED { data } == data ^ pseudo_pad (^ = XOR)

Pseudo_pad = { MD5_1, [,MD5_2 [… , MD5_n]] }

ขึ้นอยู่กับความยาวของข้อมูล

MD5_1 = MD5 { session_id, key, version, seq # }

MD5_2 = MD5 { session_id, key, version, seq #, MD5_1 }

.....

MD5_n = MD5 { session_id, key, version, seq #, MD5_n-1 }

MD5 = MD5 hashing function

TAC_PLUS_CLEAR packet body ทั้งหมดจะเป็น cleartext วิธีนี้จะใช้เฉพาะการ debug เท่านั้น

2.3.6 ประเภทของ packet body

packet body จะต้องถูกถอดรหัสก่อนนำมาใช้

2.3.6.1 การตรวจสอบสิทธิในการเข้าถึง (Authentication)

มี 3 ชนิดของ packet ดังนี้ START, CONTINUE และ REPLY มีขั้นตอนการติดต่อดังนี้

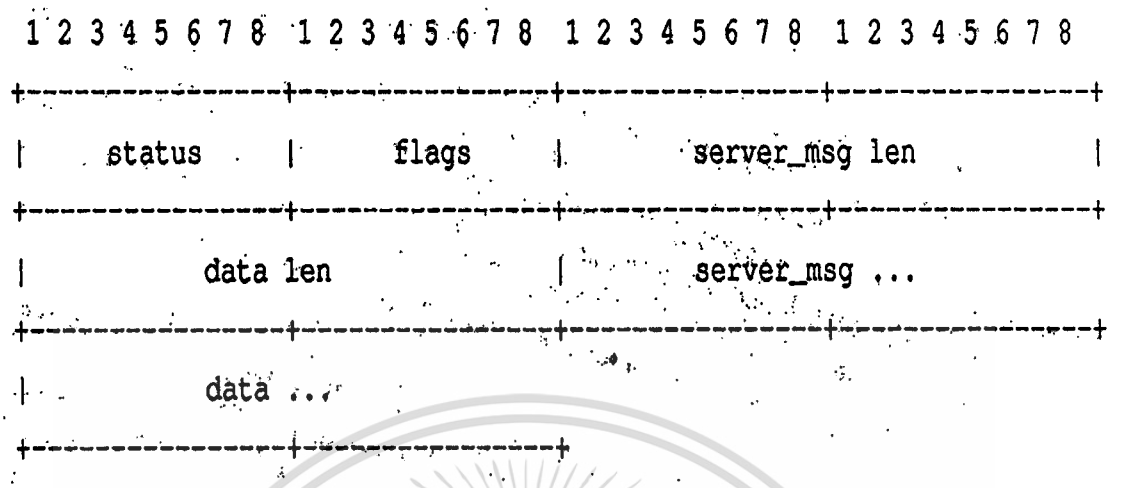
- Client ส่ง START มาที่ Server โดย START มีข้อมูลประเภทของการตรวจสอบสิทธิในการเข้าถึง
- Server ส่ง REPLY ไปที่ Client โดย REPLY จะระบุว่าการตรวจสอบสิทธิในการเข้าถึงจะทำต่อหรือเลิกติดต่อ
- ถ้า REPLY บอกให้ทำต่อ Client จะรับข้อมูลและส่ง CONTINUE ให้ Server
- Server ส่ง REPLY ไปที่ Client เพื่อตอบรับ CONTINUE

```
 1 2 3 4 5 6 7 8  1 2 3 4 5 6 7 8  1 2 3 4 5 6 7 8  1 2 3 4 5 6 7 8
+----------------+----------------+----------------+----------------+
|    action      |    priv_lvl    |  authen_type   |     service    |
+----------------+----------------+----------------+----------------+
|    user len    |    port len    |  rem addr len  |  reserved len  |
+----------------+----------------+----------------+----------------+
|    user ...
+----------------+----------------+----------------+----------------+
|    port ...
+----------------+----------------+----------------+----------------+
|    rem addr ...
+----------------+----------------+----------------+----------------+
|    reserved ...
+----------------+----------------+----------------+----------------+
```

รูปที่ 2.7 แสดงรูปแบบของ AUTH START packet body

จากรูปที่ 2.7 START packet body ประกอบไปด้วย

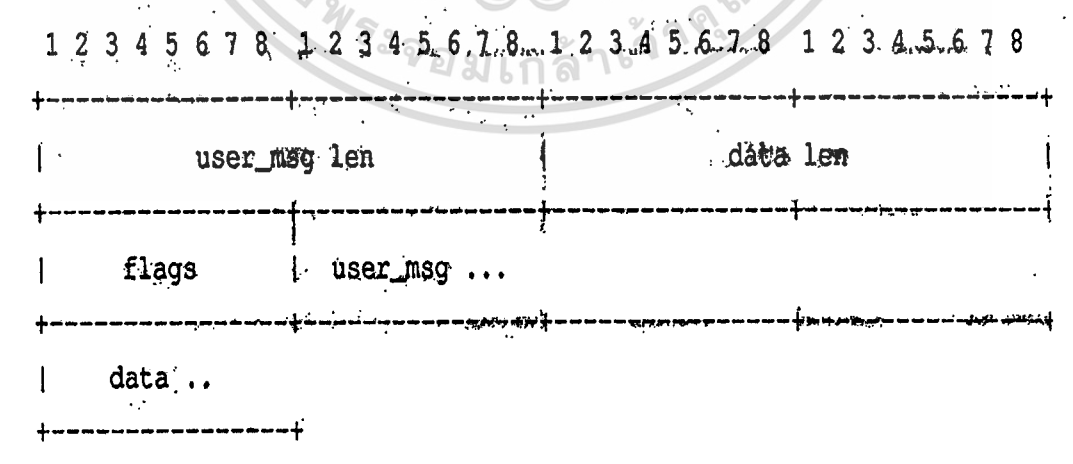
1. action (1 byte) คือ สิ่งที่จะทำ
    - 0x01 คือ LOGIN
    - 0x02 คือ เปลี่ยนรหัสผ่าน
    - 0x03 คือ ส่งรหัสผ่าน โดยจะส่ง username ไปด้วย
2. pri_lvl (1 byte) คือ ระดับของสิทธิของผู้ใช้ (privilege)
    - 0x0f คือ MAX (สิทธิสูงสุดที่อนุญาต)
    - 0x01 คือ USER (สิทธิผู้ใช้ธรรมดา)
    - 0x00 คือ MIN (สิทธิน้อยที่สุด)
3. authen_type (1 byte) คือ ชนิดของการ Authentication
    - 0x01 คือ ชนิด ASCII
    - 0x02 คือ ชนิด PAP
    - 0x03 คือ ชนิด CHAP
4. service (1 byte) คือ บริการของการ Authentication
    - 0x01 คือ บริการ LOGIN
    - 0x02 คือ บริการ ENABLE
    - 0x03 คือ บริการ PPP
5. user len (1 byte) คือ จำนวนตัวอักษรของชื่อผู้ใช้
6. port len (1 byte) คือ จำนวนตัวอักษรของ port
7. rem_addr len (1 byte) คือ ความยาวของ ip-address เครื่องผู้ใช้
8. reserved len (1 byte) คือ จำนวนตัวอักษรของสำรอง
9. user (user len bytes) คือ ชื่อผู้ใช้
10. port (port len bytes) คือ ชื่อ port
11. rem_addr (rem_addr len bytes) คือ ip-address เครื่องผู้ใช้
12. reserved (reserved len) คือ สำรอง



รูปที่ 2.8 แสดงรูปแบบของ AUTHEN CONTINUE packet body

จากรูปที่ 2.8 CONTINUE packet body ประกอบไปด้วย

1. user_msg len (2 bytes) คือ จำนวนตัวอักษรของข้อมูลของผู้ใช้
2. data len (2 bytes) คือ จำนวนตัวอักษรของข้อมูลของผู้ใช้
3. flags (1 byte) : 0x01 คือ ยกเลิก
4. user_msg (user_msg len bytes) คือ ข้อมูลของผู้ใช้
5. data (data len bytes) คือ ข้อมูลของเครื่องผู้ใช้



รูปที่ 2.9 แสดง AUTHEN REPLY packet body

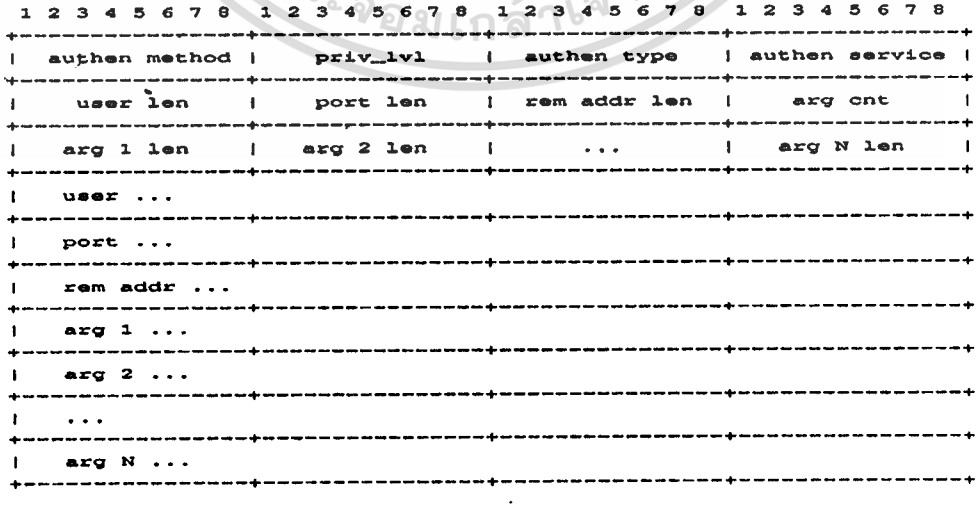
จากรูปที่ 2.9 REPLY packet body ประกอบไปด้วย

1. status (1 byte) คือ สถานะของการตรวจสอบสิทธิในการเข้าถึง
   - 0x01 คือ PASS (ผ่านการ Authentication)
   - 0x02 คือ FAIL (ไม่ผ่านการ Authentication)
   - 0x03 คือ GETDATA (รับข้อมูลเพิ่ม)
   - 0x04 คือ GETUSER (รับชื่อผู้ใช้)
   - 0x05 คือ GETPASS (รับรหัสผ่าน)
2. flags (1 byte) : 0x01 คือ คือจะไม่แสดงสิ่งที่ผู้ใช้พิมพ์ให้เป็น
3. server_msg len (2 bytes) คือความยาวของข้อมูล Server
4. data len (2 bytes) คือ จำนวนตัวอักษรของข้อมูลของผู้ใช้
5. server_msg (server_msg len bytes) คือ ข้อมูลของ Server
6. data (data len bytes) คือ ข้อมูลของเครื่องผู้ใช้

2.3.6.2 การตรวจสอบสิทธิในการใช้งาน (Authorization)

มี packet 2 แบบ REQUEST และ RESPONSE มีขั้นตอนการติดต่อดังนี้

- Client ส่ง REQUEST มาที่ Server โดย REQUEST มีข้อมูลสิทธิในการเข้าถึงของผู้ใช้ และบริการที่ต้องการใช้
- Server ส่ง RESPONSE ไปที่ Client โดย RESPONSE จะระบุว่าอนุญาต หรือไม่อนุญาตในการใช้บริการที่ต้องการใช้

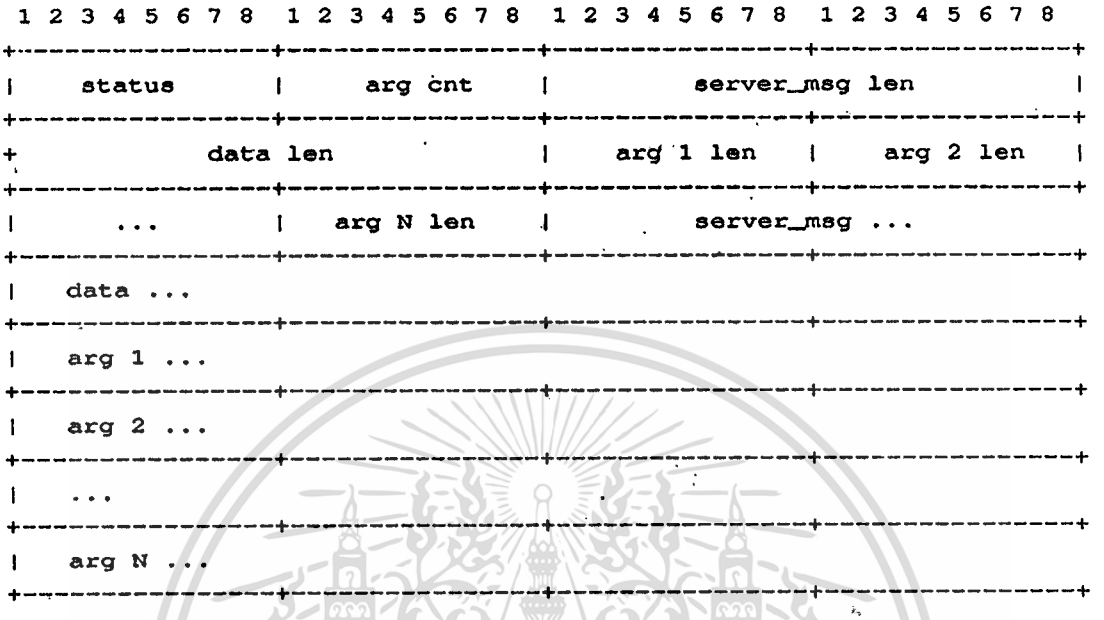


รูปที่ 2.10 แสดงรูปแบบของ AUTHOR REQUEST packet body

จากรูปที่ 2.10 REQUEST packet body ประกอบไปด้วย

1. authen_method (1 byte) คือ วิธีการ Authentication
   - 0x01 คือ NONE (ไม่มีการ Authentication)
   - 0x04 คือ ENABLE (Enable Privilege)
   - 0x05 คือ LOCAL (วิธีท้องถิ่น)
   - 0x06 คือ TACACSPLUS
2. priv_lvl (1 byte) ระดับของสิทธิของผู้ใช้ (privilege) รายละเอียดเหมือนการตรวจสอบสิทธิในการเข้าถึง
3. authen_type (1 byte) คือ ชนิดของการตรวจสอบสิทธิในการเข้าถึง รายละเอียดเหมือนการตรวจสอบสิทธิในการเข้าถึง
4. authen_service (1 byte) คือ บริการของการตรวจสอบสิทธิในการเข้าถึง รายละเอียดเหมือนการตรวจสอบสิทธิในการเข้าถึง
5. user len (1 byte) คือ จำนวนตัวอักษรของชื่อผู้ใช้
6. port len (1 byte) คือ จำนวนตัวอักษรของ port
7. rem_addr len (1 byte) คือ ความยาวของ ip-address ผู้ใช้
8. arg_cnt (1 byte) คือ จำนวน arguments
9. arg 0 … N len (@ 1 byte) คือ ความยาวของแต่ละ argument
10. user (user len bytes) คือ ชื่อผู้ใช้
11. port (port len bytes) คือ ชื่อ port
12. rem addr (rem addr len bytes) คือ ip-address เครื่องของผู้ใช้
13. arg 0 … N (arg 0 … N len bytes) คือ argument แต่ละตัว
    - service คือ บริการต่างๆ เช่น shell, ppp, slip
    - protocol เช่น ip, ipx, lcp
    - cmd คือ คำสั่งของ NAS จะต้องระบุเมื่อ service=shell
    - cmd-arg คือ argument to a shell command
    - addr คือ network address
    - addr-pool คือ NAS จะกำหนดให้ client ใช้
    - routing คือ กำหนดข้อมูลการหาเส้นทางการส่งข้อมูล
    - route คือ กำหนดเส้นทางที่ใช้ในการส่งข้อมูล
    - idletime คือ idle-timeout สำหรับ connection (นาที)

- autocmd คือ การกำหนดคำสั่งที่จะทำงานโดยอัตโนมัติ



รูปที่ 2.11 แสดง AUTHOR RESPONSE packet body

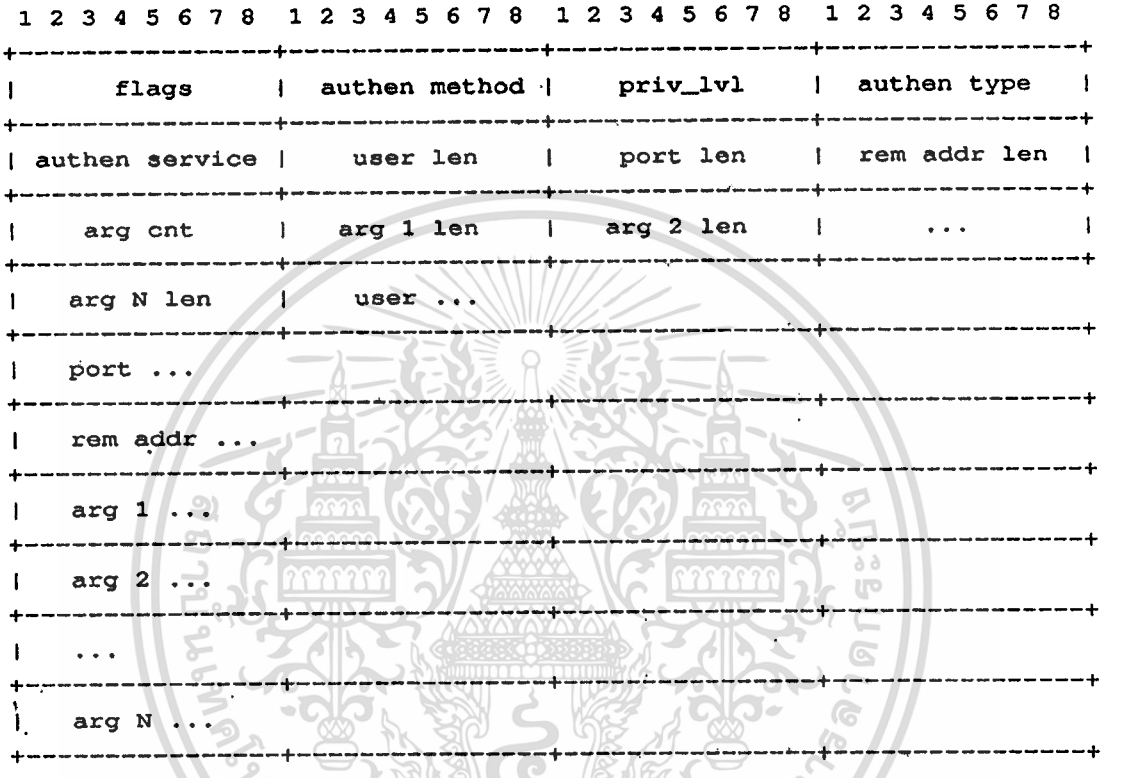
จากรูปที่ 2.11 RESPONSE packet body ประกอบไปด้วย

1. status (1 byte) คือสถานะของการ Authorization
   - 0x01 คือ PASS_ADD (อนุญาตให้ใช้ได้โดยเพิ่ม arg)
   - 0x02 คือ PASS_REPL (อนุญาตให้ใช้ได้โดยแทน arg)
   - 0x03 คือ ไม่อนุญาตให้ใช้งาน
2. arg cnt (1 byte) คือ จำนวน argument
3. server_msg len (2 bytes) คือ ความยาวข้อความของ Server
4. data len (2 bytes) คือ จำนวนตัวอักษรข้อมูลการจัดการ
5. arg 1 ... N len (@ 1 byte) คือ ความยาวของแต่ละ argument
6. server_msg (server_msg len bytes) คือ ข้อความของ Server
7. data (data len bytes) คือ ข้อมูลการจัดการ
8. arg 1 ... N (arg 1 ... N len bytes) คือ argument แต่ละตัว

2.3.6.3 การบันทึกข้อมูลของผู้ใช้ (Accounting)

มี packet 2 ชนิด ดังนี้ REQUEST และ REPLY มีขั้นตอนการติดต่อดังนี้

- Client ส่ง REQUEST มาที่ Server โดย REQUEST มีข้อมูลเกี่ยวกับการใช้บริการของผู้ใช้
- Server ส่ง REPLY ไปที่ Client โดย REPLY จะระบุว่าการบันทึกสำเร็จหรือไม่

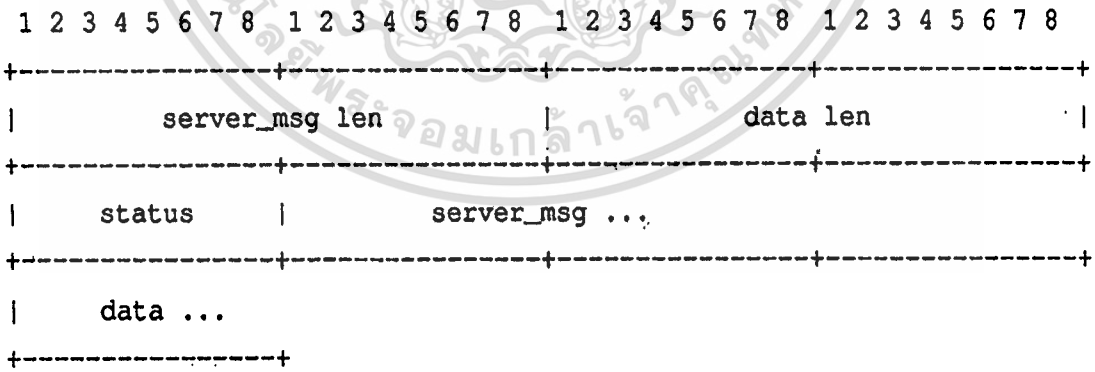


รูปที่ 2.12 แสดงรูปแบบของ ACCT REQUEST packet body

จากรูปที่ 2.12 REQUEST packet body ประกอบไปด้วย

1. flags (1 byte)
   - 0x02 คือ START (ระบุว่า packet นี้เป็น start accounting messages)
   - 0x04 คือ STOP (ระบุว่า packet นี้เป็น stop accounting messages)
2. authen method (1 byte) คือ วิธีการตรวจสอบสิทธิในการเข้าถึงรายละเอียดเหมือนการตรวจสอบสิทธิในการเข้าถึง
3. priv_lvl (1 byte) คือ ระดับของสิทธิของผู้ใช้ (privilege) รายละเอียดเหมือนการตรวจสอบสิทธิในการเข้าถึง
4. authen type (1 byte) คือ ชนิดของการตรวจสอบสิทธิในการเข้าถึงรายละเอียดเหมือนการตรวจสอบสิทธิในการเข้าถึง

5. authen service (1 byte) คือ บริการของการตรวจสอบสิทธิในการเข้าถึงรายละเอียดเหมือนการตรวจสอบสิทธิในการเข้าถึง
6. user len (1 byte) จำนวนตัวอักษรของชื่อผู้ใช้
7. port len (1 byte) จำนวนตัวอักษรของ port
8. rem addr len (1 byte) คือ จำนวนตัวอักษรของ ip-address เครื่องผู้ใช้
9. arg cnt (1 byte) คือ จำนวน argument
10. arg 1 ... N len (@ 1 bytes) คือ ความยาวของ แต่ละargument
11. user (user len bytes) คือ ชื่อผู้ใช้
12. port (port len bytes) คือ ชื่อ port
13. rem addr (rem addr len bytes) คือ ip-address เครื่องผู้ใช้
14. arg 1 ... N (arg 1 ... N len bytes) คือ argument แต่ละตัว
    - task_id คือ id ของการ start และ stop เหตุการณ์เดียวกันจะต้องมี id เหมือนกัน
    - start_time คือ เวลาเริ่มเป็นจำนวนวินาทีนับจาก 12:00 AM Jan 1, 1970
        - timezone คือ เขตเวลา
        - service คือ บริการที่ใช้
        - elapsed_time คือ จำนวนวินาทีที่ใช้



รูปที่ 2.13 แสดง ACCT REPLY packet body

จากรูปที่ 2.13 REPLY packet body ประกอบไปด้วย

1. server_msg len (2 bytes) คือ ความยาวข้อความจาก Server
2. data len (2 bytes) คือจำนวนตัวอักษรของข้อความการจัดการ

3. status (1 byte) คือ สถานะของการบันทึกการใช้งานของผู้ใช้
    - 0x01 คือ สำเร็จ (SUCCESS)
    - 0x02 คือ ไม่สำเร็จ (ERROR)
4. server_msg (server_msg len bytes) คือ ข้อความจาก Server
5. data (data len bytes) คือ ข้อความการจัดการ

2.3.7 สรุปการทำงาน

มีขั้นตอนการทำงานดังนี้

1. NAS -> Server (Authentication / START / LOGIN) เพื่อขอ Authentication จาก Server
2. Server -> NAS (Authentication / REPLY / GETUSER) Server ส่ง Authentication Prompt (User Access Verification) ไปให้และบอกให้ส่ง username มาได้
3. NAS -> Server (Authentication / CONTINUE / USER) NAS ส่ง username ให้ server
4. Server -> NAS (Authentication / REPLY / GETPASS) Server บอกว่าได้รับ username แล้วให้ส่ง password มาได้
5. NAS -> Server (Authentication / CONTINUE / PASSWORD) NAS ส่ง password ไปให้ Server
6. Server -> NAS (Authentication / REPLY / PASS) Server พิจารณาusername, password กับข้อมูลที่เก็บอยู่ และ ส่งผลที่ได้ไปที่ NAS
7. NAS -> Server (Authorization / REQUEST / SERVICE) NAS ส่งข้อมูล username และบริการที่ขอใช้ เพื่อให้ Server ตรวจสอบสิทธิในการใช้งาน (Authorization)
8. Server -> NAS (Authorization / RESPONSE / PASS_ADD) Server ทำการตรวจสอบข้อมูลที่ NAS ส่งมา กับข้อมูลที่ config ไว้ จากนั้นส่งผลไปที่ NAS
9. NAS -> Server (Accounting / REQUEST / START) NAS ส่งข้อมูลของผู้ใช้ บริการที่ใช้ port และเวลา มาที่ Server เมื่อเริ่มใช้บริการ
10. Server -> Router (Accounting / REPLY / SUCCESS) Server เมื่อได้รับข้อมูล accounting จาก NAS จะทำการบันทึกไว้จากนั้นจะส่งข้อความไปบอกผลการบันทึกกับ NAS
11. NAS -> Server (Accounting / REQUEST / STOP) NAS ส่งข้อมูลของผู้ใช้ บริการที่ใช้ port และเวลา มาที่ Server เมื่อเริ่มใช้บริการ

12. Server -> Router (Accounting / REPLY / SUCCESS) เมื่อได้รับข้อมูล accounting จาก NAS จะทำการบันทึกไว้จากนั้นจะส่งข้อความไปบอกผลการบันทึกกับ NAS

2.4 เปรียบเทียบ TACACS+ protocol กับ RADIUS protocol

2.4.1 การใช้ UDP หรือ TCP

RADIUS ใช้ UDP ในการส่ง-รับข้อมูล ในขณะที่ TACACS+ ใช้ TCP โดยทฤษฎีแล้วการส่ง-รับข้อมูลแบบ TCP มีความได้เปรียบกว่า UDP มาก เช่น TCP จะให้บริการแบบ connection-oriented transport ขณะที่ UDP จะให้แค่ best effort delivery RADIUS จำเป็นต้องมีตัวแปรเพิ่มเติมเพื่อทำงาน ด้าน retransmit และ timeout แต่ก็ยังขาดคุณสมบัติบางอย่างเช่น

- TCP แยกแยะ Acknowledge จาก request ที่ได้รับภายในค่า Network RTT และ ปริมาณ load ของ server , ความช้าเร็วในการประมวลผล Authentication (TCP ACK)
- TCP สามารถแสดงให้ทราบได้ว่า server crashed หรือ server ไม่สามารถให้บริการได้แล้ว (RST packet)
- การใช้ TCP keepalive การตรวจสอบ server crash สามารถทำได้โดย actual request การเชื่อมต่อไปยัง server หลายๆตัวสามารถทำได้อย่างต่อเนื่อง

2.4.2 Packet Encryption

RADIUS จะ encrypt เฉพาะส่วน password ใน access-request packet ส่งจาก client ไป server ส่วนที่เหลือไม่ได้ encrypt เป็น clear text ได้แก่ username, authorized service และ accounting ซึ่งสามารถดักจับดูได้ RADIUS สามารถใช้ encrypt password โดยใช้ UNIX /etc/passwd อย่างไรก็ตามกระบวนการนี้ใช้เวลามาก เป็นผลให้ต้องรอนาน

TACACS+ จะ encrypt ทั้ง body packet จะเหลือเฉพาะ standard TACACS+ header ซึ่งภายในจะเก็บค่าว่า body packet ได้ทำการ encrypt หรือไม่ เพื่อประโยชน์ในการ debugging body packet สามารถทำให้เป็น clear text ได้ แต่ภาวะปกติ body packet จะถูก encrypt ทั้งหมด เพื่อความปลอดภัยของข้อมูล

2.4.3 Authentication และ Authorization

RADIUS ได้รวมหน้าที่ authentication และ authorization ใน access-accept packet ซึ่งจะถูกส่งจาก RADIUS server ไปยัง client ซึ่งจะกำหนดข้อมูล authorization มาด้วยเป็นการยาก ที่จะแยกหน้าที่ส่วน authentication และ authorization

TACACS+ ในสถาปัตยกรรม AAA ซึ่งแยก authentication, authentication และ accounting ออกจากกัน ทำให้สามารถแยกหน้าที่ authentication ไปใช้ protocol อื่น ๆ ได้เช่น Kerberos ส่วน authorization และ accounting ยังคงใช้ TACACS+ ได้ คือหลังจากที่ NAS (Network Access Server, TACACS+ Client) ทำการ authentication กับ Kerberos server แล้ว NAS จะร้องขอข้อมูล authorization จาก TACACS+ server โดยไม่ต้องทำการ authentication ใหม่อีกครั้ง

2.4.4 Multiprotocol Support

RADIUS ไม่รองรับ protocol ต่อไปนี้

- AppleTalk Remote Access (ARA) protocol
- NetBIOS Frame Protocol Control protocol
- Novell Asynchronous Services Interface (NASI)
- Packet assembler/disassembler (PAD) connection

TACACS+ สามารถรองรับได้หลาย protocol

2.4.5 Router Management

RADIUS ไม่อนุญาตให้มีการควบคุมผู้ใช้ว่า ให้ใช้คำสั่งใน router ใดได้บ้าง และไม่ให้ใช้คำสั่งใดบ้าง

TACACS+ ได้เตรียมวิธีการในการควบคุมผู้ใช้ว่า ให้ใช้คำสั่งใน router ใดได้บ้าง และไม่ให้ใช้คำสั่งใดบ้าง เป็นรายบุคคล

- แนวทางแรกคือการกำหนด privilege level สำหรับผู้ใช้ โดย router จะทำการตรวจสอบกับ TACACS+ Server ว่าผู้ใช้คนนี้มี authorize สำหรับ privilege level นั้นหรือเปล่า
- แนวทางที่ 2 คือการกำหนดให้ชัดเจนเลยว่า ให้ใช้คำสั่งใน router ใดได้บ้าง และไม่ให้ใช้คำสั่งใดบ้าง

2.5 สรุป

RADIUS Protocol จะรวม Authentication และ Authorization Packet เข้าด้วยกัน แต่ TACACS+ Protocol จะแยกทั้งสามส่วนออกจากกัน รวมทั้งมีการเข้ารหัสทั้ง Body Packet ทำให้มีความปลอดภัยสูงกว่า RADIUS Protocol และใช้ TCP ในการรับส่งข้อมูล ในขณะที่ RADIUS ใช้ UDP โดย

ระบบที่พัฒนาขึ้นมานี้จะใช้ TACACS+ Protocol ด้วยเหตุผลทางด้านความปลอดภัยและความสามารถที่สูงกว่า RADIUS Protocols ดังรายละเอียดที่นำเสนอในหัวข้อที่ผ่านมา

2.6 Internet Roaming

2.6.1 Remote Access Server

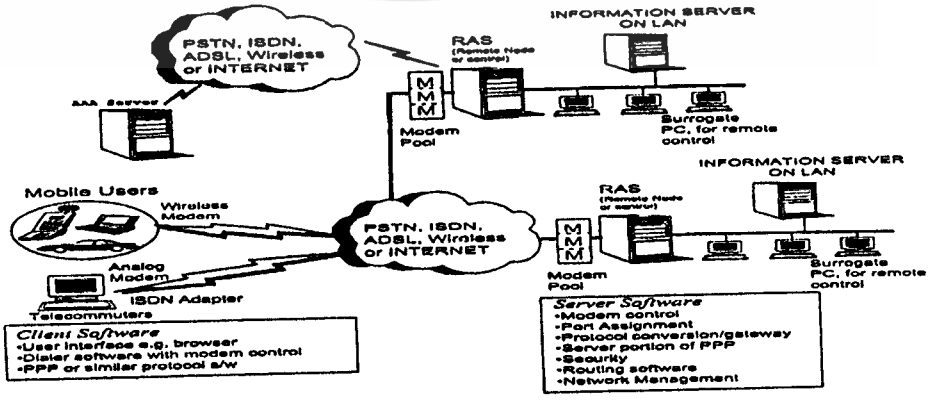
Remote Access Server คือการเข้าใช้งานเซิร์ฟเวอร์จากระยะไกล โดยการ dial-up เข้าไปใช้งานผ่านระบบเครือข่าย โดยผู้ใช้จะเข้าใช้งานได้จะต้องทำการลงเบียนกับเซิร์ฟเวอร์นั้น ๆ ก่อน และต้องมีการกำหนดเงื่อนไขในการเข้ามาใช้งานกับเซิร์ฟเวอร์ที่ลงทะเบียนด้วย เช่น อนุญาตให้ใช้ shell, PPP เป็นต้น

เมื่อผู้ใช้ dial-up เข้ามาที่เซิร์ฟเวอร์ ๆ จะทำการตรวจสอบสิทธิในการเข้าถึง (Authentication) เมื่อมีสิทธิในการเข้าถึงแล้วนั้นจะทำการตรวจสอบสิทธิในการใช้งาน (Authorization) ว่าผู้ใช้คนนี้ใช้งานอะไรได้บ้างและขั้นตอนสุดท้ายหลังจากที่ผ่าน 2 ขั้นตอนแล้วคือการบันทึกการใช้งานของผู้ใช้ (Accounting) เพื่อเป็นข้อมูลทางสถิติหรืออื่น ๆ ที่จะเป็นประโยชน์กับผู้ดูแลระบบ

2.6.2 Internet Roaming

Internet Roaming เป็นแนวทางการพัฒนาการใช้งานอินเตอร์เน็ตที่มีการกำหนดข้อตกลงที่จะใช้งานเซิร์ฟเวอร์ร่วมกัน โดยผู้ใช้ไม่ต้องไปลงทะเบียนทุกที่ แต่องค์กรที่ให้บริการเช่น ISP ต่าง ๆ จะต้องกำหนดลักษณะของการเข้าถึงและถ้าไม่พบผู้ใช้ใน Local Server นั้น ๆ จะต้องไปตรวจสอบที่ Server ใดตามเงื่อนไขของการ roaming ที่ได้ตกลงร่วมกัน

2.6.2.1 Roaming Architecture

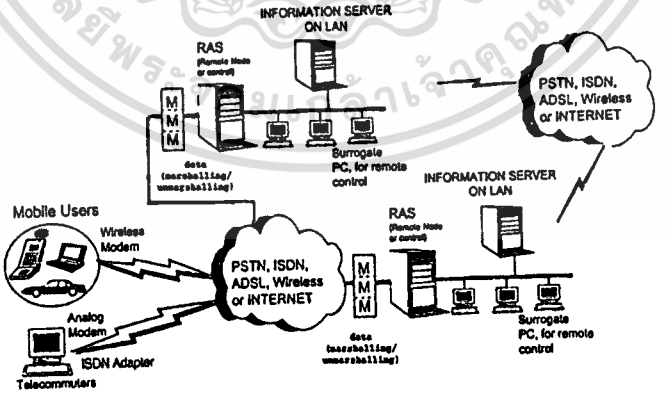


รูปที่ 2.14 แสดงสถาปัตยกรรมของระบบ

จากรูปที่ 2.14 แสดงถึงสถาปัตยกรรมของระบบเครือข่ายที่เชื่อมต่อกัน ซึ่งเซิร์ฟเวอร์ติดต่อกันได้โดยผ่านระบบเครือข่าย สำหรับผู้ใช้ที่จะใช้งานเซิร์ฟเวอร์จากระยะไกลนั้นจะต้องติดต่อโดยผ่านทางโมเด็ม โดยผู้ใช้จะต้องมีชื่อและรหัสผ่านเพื่อทำการตรวจสอบและสิทธิในการเข้าใช้งานตามขบวนการ Authentication, Authorization and Accounting โดยระบบที่ใช้ข้อตกลงร่วมกันนั้น (Roaming) เซิร์ฟเวอร์แต่ละตัวจะต้องรู้จักผู้ใช้ในเซิร์ฟเวอร์อื่น ๆ ที่ได้ทำการตกลงร่วมกัน กล่าวคือเมื่อไม่สามารถตรวจสอบผู้ใช้คนนี้ได้จากเซิร์ฟเวอร์ที่ผู้ใช้ติดต่อเข้าไปในครั้งแรก เซิร์ฟเวอร์จะต้องมีขบวนการที่จะทำการตรวจสอบสิทธิของผู้ใช้จากเซิร์ฟเวอร์อื่น ๆ ที่ได้ทำการตกลงร่วมกันในระบบเครือข่าย สำหรับวิธีการนั้นจะใช้วิธีการใดนั้นจะได้นำเสนอในหัวข้อถัดไป

2.6.2.2 Condition of Roaming

เนื่องจากระบบเครือข่ายในแต่ละระบบนั้นมีการจัดการกับข้อมูลที่เหมือนหรือไม่เหมือนกัน โดยเฉพาะรูปแบบของข้อมูลและลำดับในการส่งข้อมูล ดังนั้นในการส่งข้อมูลที่ต้องข้ามเครือข่ายกันจะต้องมีการทำข้อตกลงร่วมกันก่อนการส่งข้อมูลออกไปยังระบบเครือข่ายให้เป็นรูปแบบมาตรฐานซึ่งขบวนการนี้เรียกว่า marshalling และเมื่อข้อมูลไปถึงปลายทางก็จะทำการแปลงข้อมูลมาตรฐานกลับเป็นข้อมูลของตนเองที่จะนำไปใช้งานได้ซึ่งขบวนการนี้เรียกว่า unmarshalling ดังแสดงในรูปที่ 2.15



รูปที่ 2.15 แสดงการรับส่งข้อมูลข้ามเครือข่าย

2.6.2.3 Methodology of Roaming

วิธีการที่ใช้ในการกำหนดข้อตกลงร่วมกันหลังจากที่มีการกำหนดรูปแบบของข้อมูลที่จะรับส่งข้ามระบบเครือข่ายกันนั้น สิ่งหนึ่งที่สำคัญสำหรับการตรวจสอบผู้ใช้และรหัสผ่านคือต้องสามารถรู้ได้ว่าเมื่อไม่สามารถตรวจสอบผู้ใช้จากเครื่องที่ผู้ใช้ติดต่อเข้าไปในครั้งแรกนั้นแล้วจะทำการตรวจสอบได้จากเซิร์ฟเวอร์เครื่องใดที่ได้ทำการตกลงร่วมกันในระบบเครือข่าย โดยกระบวนการนี้สามารถทำได้โดยดูจาก hostname, domainname ที่มากับ e-mail ของผู้ใช้เช่นผู้ใช้มี e-mail เป็น t_man2000@computer.rink.ac.th และได้ทำการ dial-up เข้ามาที่เครื่องชื่อ ocirink.rink.ac.th ซึ่งเป็นเครื่องที่ทำหน้าที่เป็น Access Server และตรวจสอบไม่เจอ ที่เครื่อง ocirink ก็จะทำการตรวจสอบที่เครื่อง computer ต่อไป จากจุดนี้จะเห็นว่าวิธีการที่ใช้คือดูจาก hostname และ domainname ที่เป็นส่วนประกอบใน e-mail address จากตัวอย่างที่ได้กล่าวมานี้สามารถแยกวิธีการที่จะหาเซิร์ฟเวอร์หรือขบวนการ roaming ได้ดังนี้

1. Peer-to-Peer

   วิธีการนี้เซิร์ฟเวอร์แต่ละตัวจะมีตารางข้อมูล (คล้าย ๆ กับ Router Table) ที่ใช้ในการ Mapping โดยhostname และ domainname ที่มาจาก e-mail address ของผู้ใช้ (สำหรับการ roaming) แต่ถ้ามีชื่อผู้ใช้ใน Local Server ก็ไม่ต้องไปตรวจสอบที่เซิร์ฟเวอร์อื่น

   ข้อดีคือมีความรวดเร็วในการตรวจสอบสิทธิในการเข้าถึงของผู้ใช้

   ข้อเสียคือจะต้องคอย Update Table Configuration ที่จะใช้สำหรับการ roaming บ่อย ๆ

   Server Name/Domain Name : ocirink.rink.ac.th

   E-mail Address : t_man2000@computer.rink.ac.th

Server/Domain Name	IP Address
computer.rink.ac.th	202.29.48.20
math.rink.ac.th	202.29.48.18
physic.rink.ac.th	202.29.48.17

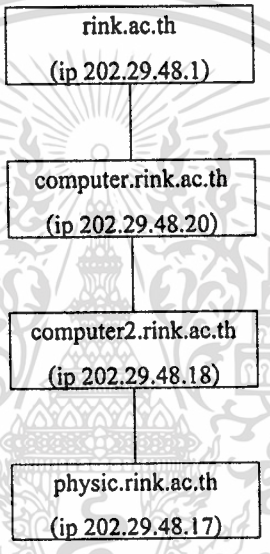
ตารางที่ 2.3 แสดงตัวอย่างตาราง Roaming แบบ Peer-To-Peer

2. Hierarchy

วิธีการนี้เซิร์ฟเวอร์แต่ละตัวจะเก็บชื่อเซิร์ฟเวอร์ที่จะให้ทำการตรวจสอบสิทธิในการเข้าถึงของผู้ใช้ลำดับถัดไป(แค่ชื่อเดียวเท่านั้น) และเซิร์ฟเวอร์ถัดไปก็จะเก็บชื่อเซิร์ฟเวอร์ลำดับถัดไปเป็นอย่างนี้ไปเรื่อย ๆ ซึ่งจะเห็นได้ว่าจะทำการเก็บเป็นลำดับชั้น ๆ ไป

ข้อดีคือไม่ต้องคอย Update Table Configuration ที่ใช้สำหรับการ roaming

ข้อเสียคือเสียเวลาในการทำการตรวจสอบ ในกรณีที่มีลำดับใช้สูง ๆ



รูปที่ 2.16 แสดงตัวอย่างตาราง Roaming แบบ Hierachy

2.7 สรุป

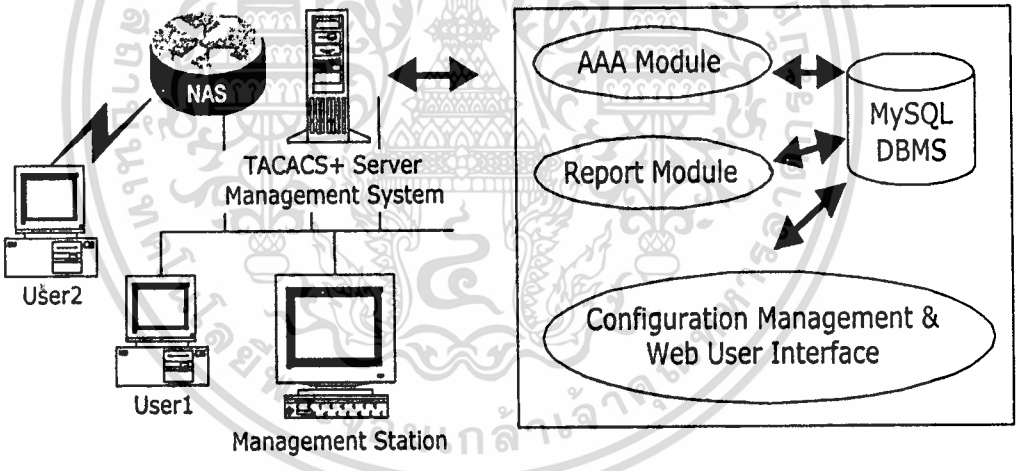
จากการศึกษาทฤษฎีและหลักการทำงานของ RADIUS และ TACACS+ Protocol ทำให้เข้าใจถึงวิธีการ Authentication, Authorization และ Accounting โดยนำหลักการ AAA มาประยุกต์ใช้เป็นลักษณะของงาน Internet Roaming ที่ให้มีความสามารถใช้งานข้ามเครื่องได้ตามที่เซิร์ฟเวอร์แต่ละเซิร์ฟเวอร์ได้ทำการตกลงร่วมกันตามตารางของการ Roaming สำหรับระบบที่พัฒนาขึ้นมานี้จะใช้วิธีการ Roaming แบบ Peer-to-Peer

บทที่ 3
ผลการศึกษาระบบงานเดิม

โปรแกรมควบคุม TACACS+ Server ผ่าน web พัฒนาโดยคุณสมภพ วชิรลาภไพฑูรย์ โดยมีการเก็บ Configuration file และ Accounting file ลงฐานข้อมูลของ mySQL ทำให้ง่ายต่อการนำข้อมูลไปใช้งาน เช่น เป็นข้อมูลทางสถิติ สำหรับการบริหารระบบนั้นจะมีส่วนการทำงานผ่านทาง Web Browser ดังมีรายละเอียดต่อไปนี้

3.1 โปรแกรมควบคุม TACACS+ Server ผ่าน Web

3.1.1 องค์ประกอบของระบบ



รูปที่ 3.1 แสดงองค์ประกอบของระบบ

จากรูปที่ 3.1 สามารถแบ่งส่วนการทำงานต่าง ๆ ได้ดังนี้

- TACACS+ Server Management System
- ผู้ใช้บริการ (USER1 & USER2)
- NAS (Network Access Server)
- Management Station

3.1.2 การทำงานของระบบ

3.1.2.1 TACACS+ Server Management System

- **AAA Module** ทำหน้าที่ติดต่อกับ NAS และตรวจสอบผู้ใช้ตามหลัก AAA (Authentication, Authorization และ Accounting) โดยจะติดต่อกับ Database Module เพื่อเก็บข้อมูลต่าง ๆ เช่น ข้อมูลผู้ใช้ ข้อมูลบริการที่ใช้เวลาที่ใช้งาน เป็นต้น โดยใช้ TACACS+ Protocol ที่ติดตั้งบนระบบปฏิบัติการ Solaris 2.7 for x86
- **Configuration Management & Web User Interface** ทำหน้าที่ติดต่อกับผู้บริหารระบบเครือข่ายเพื่อ เพิ่ม, แก้ไข และลบ รายละเอียดทั้งหมดเกี่ยวกับผู้ใช้ พัฒนาโดยใช้ภาษา PHP (Version 3.0)
- **Report Module** ทำหน้าที่แสดงรายงานต่าง ๆ เช่นรายชื่อผู้ใช้งานในระบบในปัจจุบัน รายงานจำนวนชั่วโมง ต่อเดือน หรือ สัปดาห์ เรียงตามบริการที่ใช้ และตามรายชื่อผู้ใช้บริการ พัฒนาโดยใช้ภาษา PHP (Version 3.0)
- **Database Module** ติดต่อกับทั้ง 3 Module เพื่อสนับสนุนข้อมูลต่าง ๆ ดังต่อไปนี้ ข้อมูลเกี่ยวกับผู้ใช้ ข้อมูลเกี่ยวกับ NAS, ข้อมูลเกี่ยวกับบัญชี เป็นต้น โดยใช้ MySQL (Version 3.22.32)

3.1.2.2 ผู้ใช้บริการ (USER1 & USER2)

- ติดต่อกับ NAS เพื่อขอใช้บริการเครือข่ายเช่น Shell, PPP, SLIP และอื่น ๆ
- ส่งข้อมูลของผู้ใช้ และบริการที่ต้องการใช้ให้ NAS เพื่อทำการ Authentication & Authorization

3.1.2.3 NAS (Network Access Server)

- ติดต่อระหว่างผู้ใช้บริการ และ TACACS+ Server Management System
- รับข้อมูลจากผู้ใช้บริการ แล้วส่งต่อให้ TACACS+ Server Management System เพื่อ Authentication & Authorization
- นำผลการ Authentication & Authorization ที่ได้จาก NAS มาปฏิบัติ เช่นอนุญาตให้ใช้ Shell ได้ หรือ ไม่อนุญาตให้ใช้
- ส่งข้อมูล Accounting ให้กับ TACACS+ Server Management System เพื่อบันทึก

3.1.2.4 Management Station (Web Browser)

- เป็นเครื่องของผู้บริหารระบบเครือข่าย เพื่อใช้ในการติดต่อกับ TACACS+ Server Management System ผ่าน Configuration Management & Web User Interface เพื่อจัดการเรื่อง configuration ของระบบ
- เป็นเครื่องของผู้บริหารระบบเครือข่าย เพื่อใช้ในการติดต่อกับ TACACS+ Server Management System ผ่าน Report Module เพื่อเรียกดูรายงานต่าง ๆ ของระบบ

3.1.3 สรุปผลการศึกษา

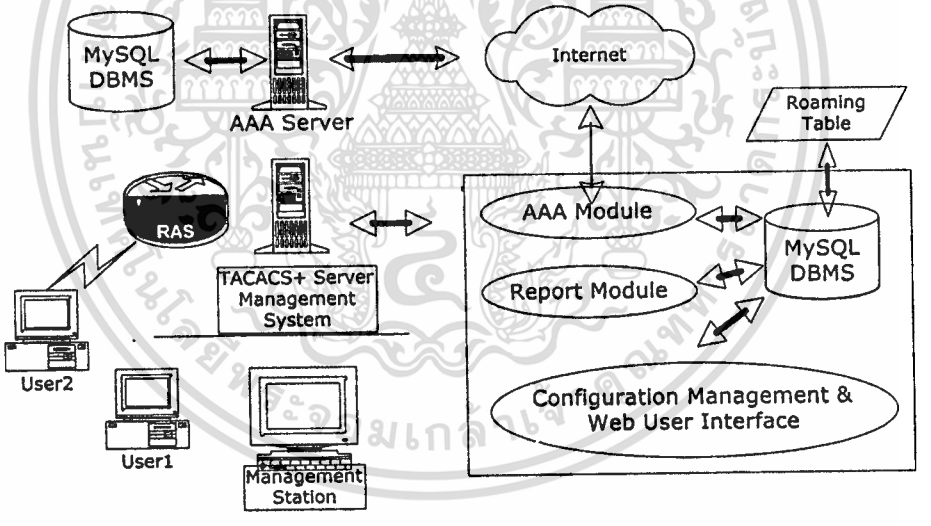
- ระบบควบคุม TACACS+ Server ผ่าน Web ถูกพัฒนาโดยคุณสมภพ วชิรลาภไพฑูรย์ IS6 ภาคสมทบ ที่พัฒนาต่อจากเวอร์ชั่น Freeware ของ Cisco System ที่ให้ load ฟรี พร้อม Source Code (ftp://ftpeng.cisco.com) แต่ไม่มีการรับประกัน และสนับสนุนอย่างเป็นทางการ
- ใช้ TACACS+ protocol ในการ authentication, authorization และ accounting
- AAA packet มีความปลอดภัยมากขึ้นเนื่องจากถูก encrypt ทุก packet
- อ่านค่า Configuration จากฐานข้อมูล
- Output หรือออกรายงาน โดยดึงข้อมูลจากฐานข้อมูล
- ติดต่อกับผู้ใช้งาน (Administrator) ผ่าน Web Browser
- Statistic เก็บไว้ในฐานข้อมูลทำให้สามารถนำข้อมูลต่าง ๆ มาจัดการได้ง่าย เช่น ข้อมูลทางสถิติ
- มีการจัดการเรื่องเวลาการใช้งานคือสามารถใช้งานได้หรือไม่ได้ในช่วงวันและเวลาใด

บทที่ 4

โปรแกรมควบคุมการใช้งานอินเตอร์เน็ตจากระยะไกลแบบใช้ข้อตกลงร่วมกัน

โปรแกรมควบคุมการใช้งานอินเตอร์เน็ตจากระยะไกลแบบใช้ข้อตกลงร่วมกันพัฒนาโดยมีพื้นฐานมาจากโปรแกรมควบคุม TACACS+ Server ผ่าน Web ที่มีการเก็บ Configuration file และ Accounting file ลงฐานข้อมูล mySQL และมีส่วนการติดต่อกับผู้บริหารระบบผ่าน Web Browser โดยปรับเปลี่ยนโปรแกรมให้มีคุณสมบัติของการ Roaming หมายถึงให้ใช้งานข้ามเครื่องได้ภายใต้ข้อตกลงร่วมกันตามตารางการ Roaming ที่ใช้วิธีการแบบ Peer-to-Peer ดังรายละเอียดต่อไปนี้

4.1 องค์ประกอบของระบบ



รูปที่ 4.1 แสดงองค์ประกอบของระบบ

องค์ประกอบของโปรแกรมควบคุมการใช้งานอินเตอร์เน็ตจากระยะไกลแบบใช้ข้อตกลงร่วมกันประกอบไปด้วย

- TACACS+ Server Management System/AAA Server
- ผู้ใช้บริการ (USER1 & USER2)
- NAS (Network Access Server)
- Management Station

4.1.1 TACACS+ Server Management System

- **AAA Module** ทำหน้าที่ติดต่อกับ NAS และตรวจสอบผู้ใช้ตามหลัก AAA (Authentication, Authorization และ Accounting) โดยจะติดต่อกับ Database Module เพื่อเก็บข้อมูลต่าง ๆ เช่น ข้อมูลผู้ใช้ ข้อมูลบริการที่ใช้เวลาที่ใช้งาน เป็นต้นและข้อมูลการ Roaming ในกรณีที่ผู้ใช้งานเข้าบริการแบบ Roaming เพื่อให้สามารถทำการ AAA ได้ตามที่เซิร์ฟเวอร์มีการตกลงร่วมกันไว้
- **Configuration Management & Web User Interface** ทำหน้าที่ติดต่อกับผู้บริหารระบบเครือข่ายเพื่อ เพิ่ม, แก้ไข และลบ รายละเอียดทั้งหมดเกี่ยวกับผู้ใช้ รวมถึงกำหนดเวลาการใช้งานเช่น จำนวนครั้งในการติดต่อในแต่ละวัน, จำนวนชั่วโมงการใช้งานต่อเดือน
- **Report Module** ทำหน้าที่แสดงรายงานต่าง ๆ เช่นรายชื่อผู้ใช้งานในระบบในปัจจุบัน รายงานจำนวนชั่วโมง ต่อเดือน หรือ สัปดาห์ เรียงตามบริการที่ใช้ และตามรายชื่อผู้ใช้บริการ รวมทั้งรายงานในรูปแบบของการ Roaming
- **Database Module** ติดต่อกับทั้ง 3 Module เพื่อสนับสนุนข้อมูลต่าง ๆ ดังนี้ ข้อมูลเกี่ยวกับผู้ใช้ ข้อมูลเกี่ยวกับ NAS, ข้อมูลเกี่ยวกับบัญชี เป็นต้น

4.1.2 ผู้ใช้บริการ (USER1 & USER2)

- ติดต่อกับ NAS เพื่อขอใช้บริการเครือข่ายเช่น Shell, PPP, SLIP และอื่น ๆ
- ส่งข้อมูลของผู้ใช้ และบริการที่ต้องการใช้ให้ NAS เพื่อทำการ Authentication & Authorization

4.1.3 NAS (Network Access Server)

- ติดต่อระหว่างผู้ใช้บริการ และ TACACS+ Server Management System
- รับข้อมูลจากผู้ใช้บริการ แล้วส่งต่อให้ TACACS+ Server Management System เพื่อ Authentication & Authorization
- นำผลการ Authentication & Authorization ที่ได้จาก NAS มาปฏิบัติ เช่นอนุญาตให้ใช้ Shell ได้ หรือ ไม่อนุญาตให้ใช้
- ส่งข้อมูล Accounting ให้กับ TACACS+ Server Management System เพื่อบันทึกไว้

4.1.4 Management Station (Web Browser)

- เป็นเครื่องของผู้บริหารระบบเครือข่าย เพื่อใช้ในการติดต่อกับ TACACS+ Server Management System ผ่าน Configuration Management & Web User Interface เพื่อจัดการเรื่อง configuration ของระบบ
- เป็นเครื่องของผู้บริหารระบบเครือข่าย เพื่อใช้ในการติดต่อกับ TACACS+ Server Management System ผ่าน Report Module เพื่อเรียกดูรายงานต่าง ๆ ของระบบ

4.2 การออกแบบระบบ

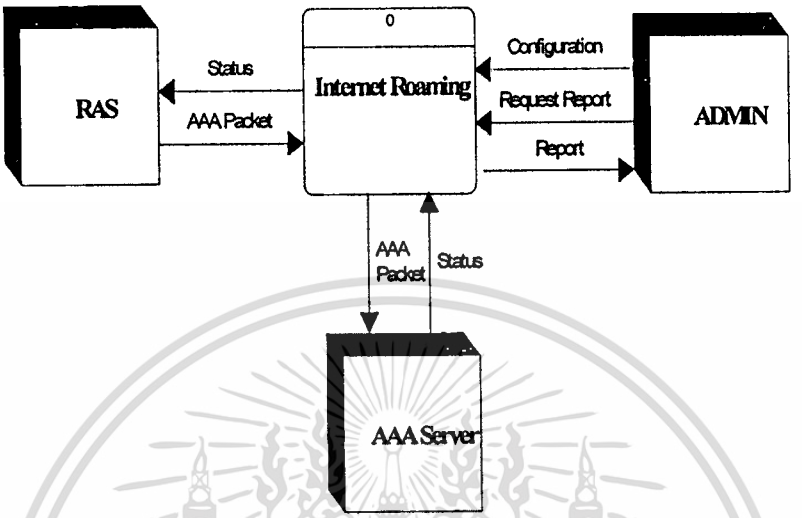
Roaming เป็นการทำข้อตกลงร่วมกันระหว่างเซิร์ฟเวอร์กับเซิร์ฟเวอร์ โดยเมื่อผู้ใช้ (ติดต่อโดยใช้ e-mail address) เข้ามาใช้งานจะทำการตรวจสอบที่ local server ก่อน เมื่อไม่พบจะไปตรวจสอบที่ตาราง Roaming ที่ได้กำหนดข้อตกลงกันไว้ ถ้าพบ (ดูจาก domain name ที่มาจากชื่อผู้ใช้) จะทำการตรวจสอบตามเครื่องที่ผู้ใช้ได้ลงทะเบียนไว้ และหากไม่ได้กำหนดข้อตกลงร่วมกันผู้ใช้รายนั้นจะไม่สามารถเข้ามาใช้งานใด ๆ ได้ ดังรายละเอียดความต้องการระบบดังต่อไปนี้

4.2.1 ความต้องการของระบบ

- ทำการ Authentication, Authorization และ Accounting ในรูปแบบ Roaming
- เก็บข้อมูลของผู้ใช้บริการโดยสามารถเลือกได้ว่าจะใช้บริการแบบ Roaming หรือไม่เป็นแบบ Roaming
- ผู้ใช้แต่ละคนสามารถเข้ามาใช้งานในแต่ละวันตามจำนวนครั้งที่ถูกกำหนดไว้
- ผู้ใช้แต่ละคนสามารถเข้ามาใช้งานตามจำนวนเวลา (นาที) ต่อเดือนที่ถูกกำหนดไว้
- กำหนดเซิร์ฟเวอร์เพื่อทำการ Roaming ซึ่งเก็บลงในฐานข้อมูล
- ระบบติดต่อผู้บริหารระบบเครือข่ายผ่าน Web Browser โดยสามารถตรวจสอบเวลาในการใช้งานและจำนวนครั้งที่เคยเข้ามาใช้งาน
- แสดงรายงานต่าง ๆ โดยแยกเป็นแบบ Roaming หรือไม่เป็นแบบ Roaming เช่น รายงานรายชื่อผู้ใช้ในปัจจุบัน, รายงานจำนวนเวลาในการใช้งาน, รายงานคำสั่งที่ใช้งาน, รายการการเข้าใช้งานตาม NAS เป็นต้น
- แสดงรายงานในกรณีที่ผู้ใช้ไม่สามารถติดต่อเข้ามาใช้งานได้ เช่น ไม่มีรายชื่อใน Server นั้น หรือไม่ได้อยู่ในเงื่อนไขของการทำ Roaming

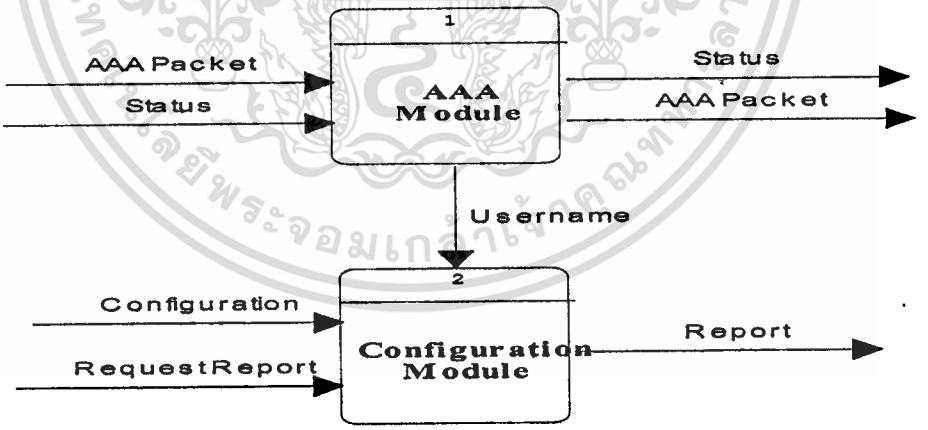
4.2.2 Process Modeling

4.2.2.1 Data Flow Diagram (Context Diagram)



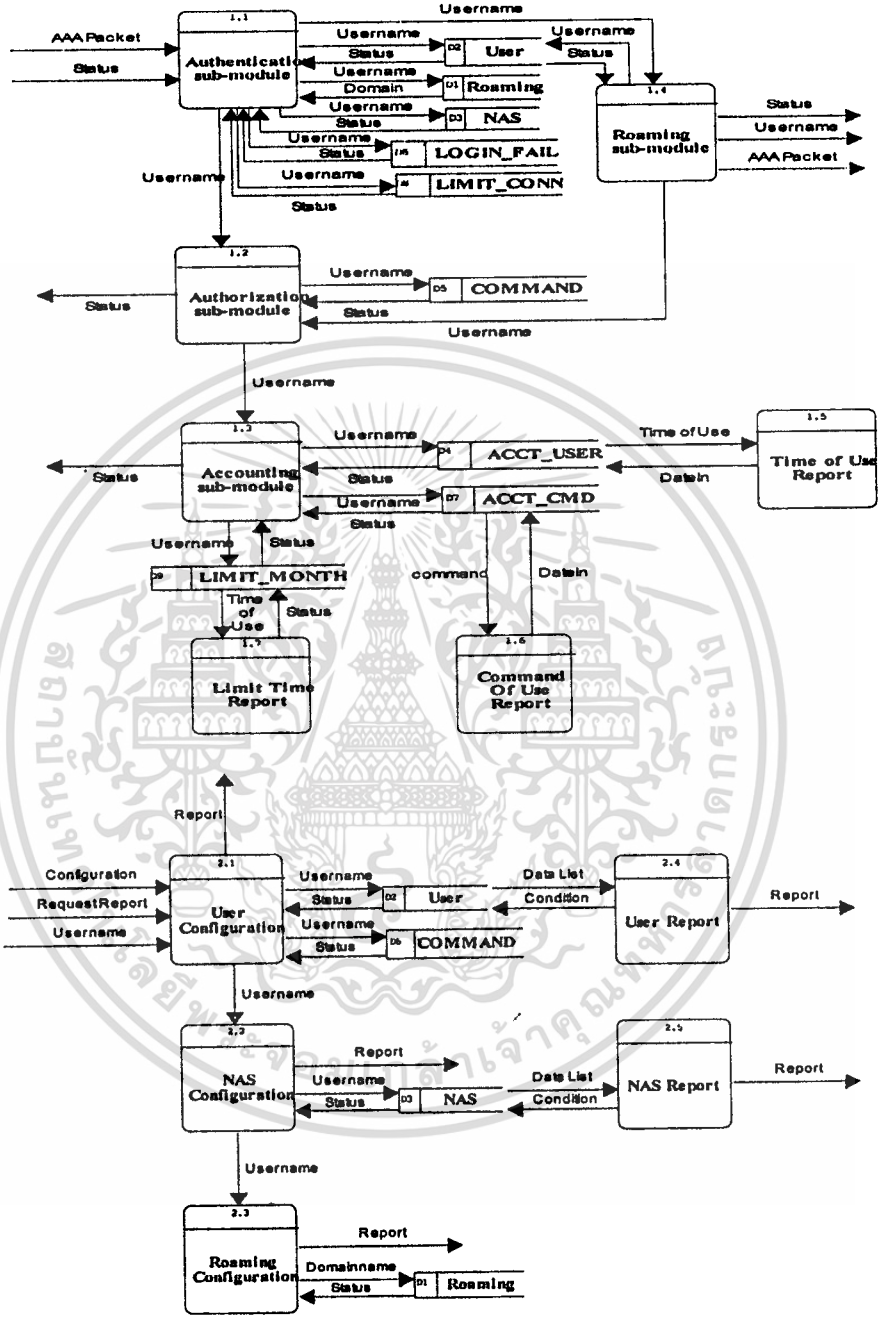
รูปที่ 4.2 แสดง Data Flow Diagram (Context Diagram)

4.2.2.2 Data Flow Diagram (Level 1)



รูปที่ 4.3 แสดง Data Flow Diagram (Level 1)

4.2.2.3 Data Flow Diagram (Level 2)



รูปที่ 4.4 แสดง Data Flow Diagram (Level 2)

4.2.2.4 หน้าที่ของแต่ละ Process

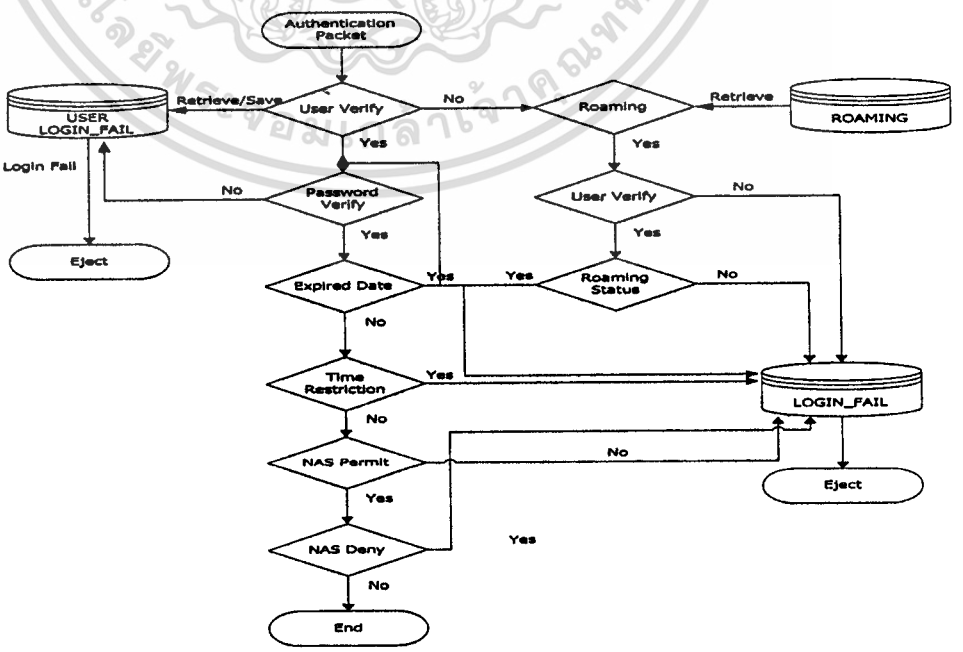
จากรูปที่ 4.2 ถึง 4.4 อธิบายการทำงานได้ดังนี้

Process 1 : AAA Module

รับข้อมูลจาก RAS และทำการตรวจสอบกับฐานข้อมูล จากนั้นส่งผลที่ได้กลับไปให้ RAS

Process 1.1 : Authentication Process อธิบายการทำงานได้ดังนี้

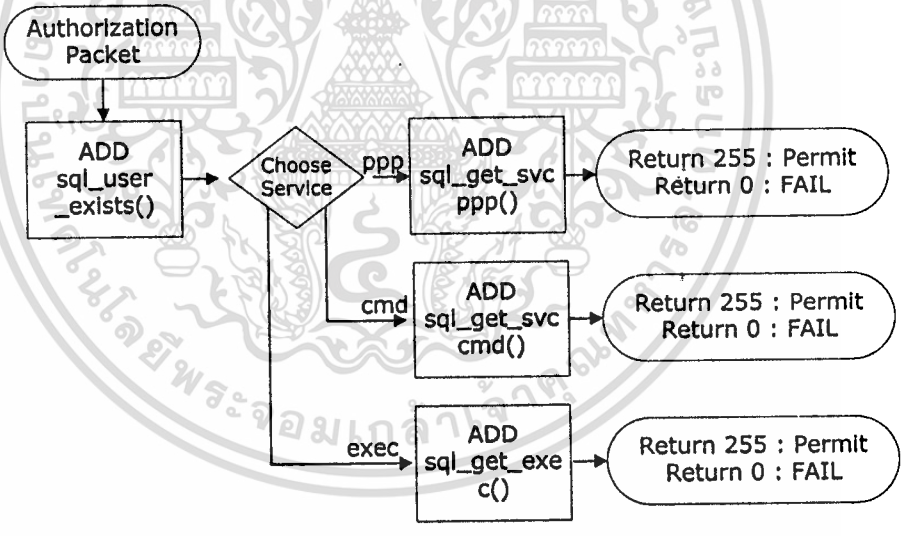
- เมื่อ LOGIN เข้ามาในระบบจะรับข้อมูล Authentication Packet มาทำการตรวจสอบ USERNAME/PASSWORD ว่าตรงกันหรือไม่ โดย PASSWORD เก็บอยู่ในรูปของ UNIX encrypted เปรียบเทียบระหว่าง encrypted password กับ crypt (enter password, salt), TIME_RESTRICTION ว่าสามารถใช้งานได้ในวันเวลาปัจจุบันได้หรือไม่, EXPIRE_DATE หมดอายุหรือยัง, ข้อจำกัดในเรื่องเวลาการติดต่อ, เวลาการใช้บริการต่อเอือน, NAS_PERMIT/DENY อนุญาตให้ใช้งานที่ NAS หรือไม่ ถ้าไม่ผ่านให้เก็บข้อมูลไว้ด้วยที่ LOGIN_FAIL (function sql_authen())
- กรณี ENABLE รับข้อมูล Authentication Packet มาทำการตรวจสอบ ENABLE PASSWORD ว่าตรงกับในฐานข้อมูลหรือไม่ โดยเก็บเหมือนกับ User Password (function sql_enable())
- กรณีที่ไม่พบชื่อผู้ใช้ใน Local Server จะไปทำงานที่ Process ในส่วนการ Roaming ต่อ (สำหรับผู้ใช้บริการแบบ Roaming) ดังแสดงในรูปที่ 4.5



รูปที่ 4.5 แสดง Authentication Process

Process 1.2 : Authorization Process อธิบายการทำงานได้ดังนี้

- รับข้อมูล Authorization packet มาทำการตรวจสอบ SERVICE, CMD, CMD-ARG ว่าอนุญาตให้ใช้งานได้หรือไม่
- sql_user_exists() ตรวจสอบว่ามีรายชื่อผู้ใช้อยู่ในฐานข้อมูลหรือไม่
- sql_get_svc_ppp() ตรวจสอบว่าอนุญาตให้ผู้ใช้สามารถใช้บริการ PPP ได้หรือไม่
- sql_get_svc_exec() ตรวจสอบว่าอนุญาตให้ผู้ใช้สามารถใช้บริการ EXEC ได้หรือไม่
- sql_get_svc_cmd() ตรวจสอบว่าอนุญาตให้ผู้ใช้สามารถใช้คำสั่งนั้นๆ ได้หรือไม่ โดยจะทำการตรวจสอบว่า Command permit = "*" หรือไม่ ถ้าใช่จากนั้นทำการตรวจสอบ Command deny ต่อไปหรือจะทำการทดสอบ Command Argument permit = "*" หรือไม่ ถ้าใช่จะทำการตรวจสอบ Command deny ต่อไป หรือถ้าไม่ได้กำหนดไว้ ให้ตรวจสอบ Command deny เลย

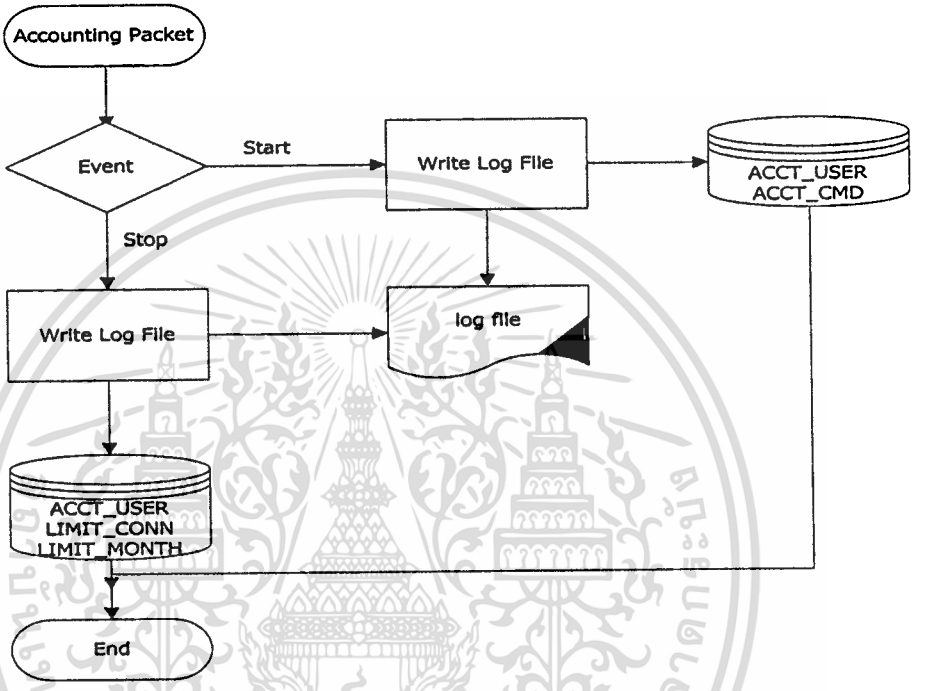


รูปที่ 4.6 แสดง Authorization Process

Process 1.3 : Accounting Process อธิบายการทำงานได้ดังนี้

- กรณี ACC_TYPE = START เก็บข้อมูลที่ NAS ส่งมา ลงฐานข้อมูล ACCT_USER และปรับปรุงฐานข้อมูล UTILIZATION (จำนวนผู้ใช้งานในระบบสะสม) และ CURRENT (รายชื่อผู้ใช้งานในระบบเวลาปัจจุบัน)

- กรณี ACCT_TYPE = STOP เก็บข้อมูล elapsed_time ใน record ที่ task_id & NAS & username & start_time เท่ากัน
- กรณีมีค่า CMD ให้เก็บข้อมูล CMD, CMD-ARG และอื่น ๆ ในฐานข้อมูล ACCT-CMDและออกรายงานตาม Process 1.5, 1.6 และ 1.7



รูปที่ 4.7 แสดง Accounting Process

Process 1.4 : Roaming Sub-Module อธิบายการทำงานได้ดังนี้

- เมื่อตรวจสอบชื่อผู้ใช้ไม่พบใน Local Server ตาม Process 1.1 นั้นจะพิจารณาจากชื่อผู้ใช้ที่อยู่ในรูปแบบ e-mail address ซึ่งจะดูข้อมูลจากตาราง Roaming และทำ AAA ตามเซิร์ฟเวอร์นั้น ๆ
- เมื่อตรวจสอบพบก็ทำ Process 1.2 และ Process 1.3 ต่อไป ถ้าไม่พบก็จะทำการเก็บข้อมูลไว้ที่ตาราง LOGIN_FAIL

Process 2 : Configuration Module อธิบายการทำงานได้ดังนี้

- เพิ่ม / แก้ไข / ลบ ข้อมูลผู้ใช้ และ ข้อจำกัดเกี่ยวกับ RAS, คำสั่งต่าง ๆ (CMD) โดย user.php, user-submit.php
- เพิ่ม / แก้ไข / ลบ ข้อมูล RAS โดย nas.php, nas-submit.php

- นำข้อมูลจากฐานข้อมูลออกมาแสดงผลในรูปของรายงานผ่านทาง Web Browser โดย report.php, report-submit.php

Process 2.1 : User Configuration อธิบายการทำงานได้ดังนี้

- เมื่อผู้ใช้ (Admin) Login เข้าสู่ระบบจะตรวจสอบว่ามีชื่อในฐานข้อมูล USER หรือไม่ ถ้ามีก็จะสามารถทำรายการเพิ่ม, แก้ไข, ลบและกำหนดเงื่อนไขอื่น ๆ สำหรับผู้ใช้ในแต่ละคนได้และรองรับการบริการแบบ Roaming
- หลังจากกำหนดค่าต่าง ๆ แล้วสามารถนำไปออกเป็นรายงานเบื้องต้นได้ดัง Process ที่ 2.4

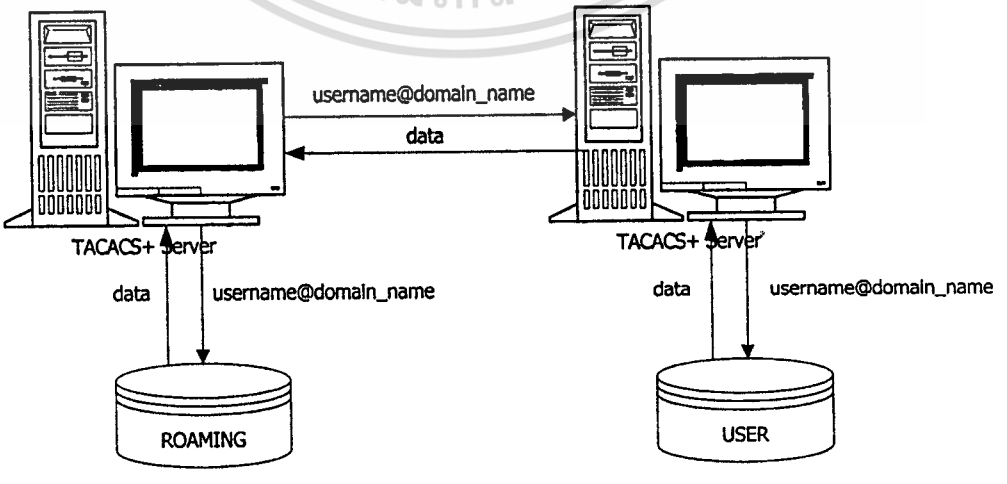
Process 2.2 : NAS Configuration อธิบายการทำงานได้ดังนี้

- เป็นการกำหนดค่า NAS ว่าอนุญาตให้ผู้ใช้สามารถใช้งานได้หรือไม่ได้
- หลังจากกำหนดค่าต่าง ๆ แล้วก็สามารถนำไปออกเป็นรายงานเบื้องต้นได้ดัง Process 2.5

Process 2.3 : Roaming Configuration อธิบายการทำงานได้ดังนี้

- เป็นการกำหนดชื่อ Server ที่ทำการตกลงร่วมกันไว้ โดยเมื่อไม่พบผู้ใช้ใน Local Server จะไปตรวจสอบที่ Server ใดซึ่งจัดเก็บในตาราง ROAMING

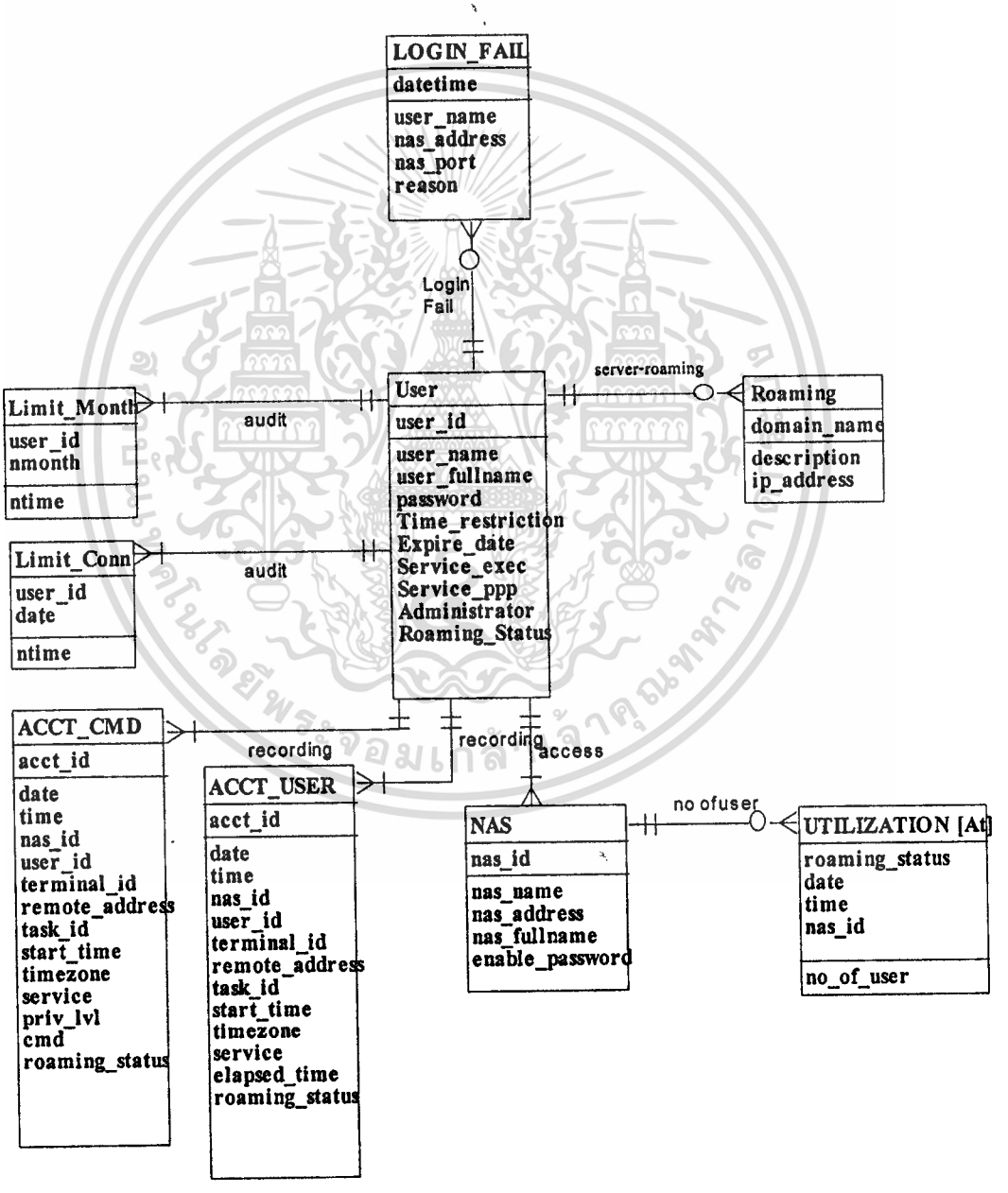
4.2.2 การรับส่งข้อมูลระหว่างเครื่อง (ในกรณี Roaming)



รูปที่ 4.8 แสดงการส่งข้อมูลระหว่างเครื่อง (ในกรณี Roaming)

จากรูปที่ 4.8 เมื่อเข้าสู่เงื่อนไข Roaming นั้นโปรแกรมจะส่งชื่อผู้ใช้ (อยู่ในรูป e-mail address) เพื่อตรวจสอบ Domain Name ในตาราง Roaming โดยถ้าพบจะส่งชื่อผู้ใช้ไปทำการตรวจสอบกับอีกเครื่องที่ทำข้อตกลงร่วมกันไว้และในกรณีที่ไม่พบ Domain Name ในตาราง Roaming จะไม่ส่งชื่อผู้ใช้ไปตรวจสอบกับอีกเครื่อง

4.2.3 ER-Diagram



รูปที่ 4.9 แสดง Entity Relationship Diagram

จากรูปที่ 4.9 แสดงความสัมพันธ์ระหว่างตารางข้อมูลนั้นสามารถนำมาออกแบบตารางข้อมูลได้ดังต่อไปนี้

- ตาราง ROAMING เก็บข้อมูลของเซิร์ฟเวอร์ต่าง ๆ ที่ได้ทำการตกลงร่วมกันไว้เพื่อทำการ Authentication, Authorization และ Accounting ได้
- ตาราง USER เก็บข้อมูลของผู้ใช้ ได้แก่ รหัสผู้ใช้ ชื่อผู้ใช้ Password ข้อจำกัดด้านเวลา (เก็บเป็นรายชั่วโมงในสัปดาห์ 24x7 Y/N) บริการต่าง ๆ ความสามารถในการแก้ไขข้อมูลระบบ,บริการแบบปกติหรือแบบ Roaming
- ตาราง NAS เก็บข้อมูลของ NAS ได้แก่ รหัส NAS ชื่อ NAS Enable Password และ IP Address ของ NAS
- ตาราง NAS_PERMIT เก็บข้อมูลว่าอนุญาตให้ผู้ใช้ใช้บริการที่ NAS ใดบ้าง
- ตาราง NAS_DENY เก็บข้อมูลว่าไม่อนุญาตให้ผู้ใช้ใช้บริการที่ NAS ใดบ้าง
- ตาราง CMD_PERMIT เก็บข้อมูลว่าอนุญาตให้ผู้ใช้ใช้คำสั่งใดบ้าง
- ตาราง CMD_DENY เก็บข้อมูลว่าไม่อนุญาตให้ผู้ใช้ใช้คำสั่งใดบ้าง
- ตาราง CURRENT เก็บรายชื่อผู้ใช้งาน ณ ปัจจุบัน โดยแบ่งเป็นแบบปกติและแบบ Roaming
- ตาราง UTILIZATION เก็บจำนวนผู้ใช้งานใน NAS ใด ๆ ณ วันที่กำหนดเพื่อนำไปทำรายงานจำนวนผู้ใช้งานในระบบ
- ตาราง LOGIN_FAIL เก็บข้อมูลกรณีที่ผู้ใช้ Login Fail โดยจะเก็บเหตุผลด้วยว่า Fail เนื่องมาจากสาเหตุใด เช่นไม่มีชื่อผู้ใช้อยู่ในระบบ password ผิด หมดอายุ
- ตาราง ACCT-USER เก็บข้อมูลการใช้งานของผู้ใช้ ได้แก่วันที่เวลา NAS ที่ใช้งาน Terminal No. IP Address ของผู้ใช้เอง Task ID เวลาเริ่มใช้งาน Time Zone บริการที่ใช้งาน และระยะเวลาที่ใช้งาน (Elapsed Time), สถานะบริการแบบ Roaming หรือไม่
- ตาราง ACCT-CMD เก็บข้อมูลการใช้งานของผู้ใช้เกี่ยวกับคำสั่งต่างๆ ได้แก่วันที่เวลา NAS ที่ใช้งาน Terminal No. IP Address ของผู้ใช้เอง Task ID เวลาเริ่มใช้งาน Time Zone บริการที่ใช้งาน และคำสั่งที่ใช้งาน, สถานะบริการแบบ Roaming หรือไม่
- ตาราง LIMIT_CONN เก็บข้อมูลจำนวนการติดต่อเข้ามาใช้บริการต่อวัน ใช้สำหรับตรวจสอบในกรณีที่จำกัดจำนวนครั้งในการใช้บริการต่อวันของผู้ใช้ในแต่ละราย
- ตาราง LIMIT_MONTH เก็บข้อมูลจำนวนเวลาการใช้งาน (หน่วยเป็นนาที) ต่อเดือน ใช้ในกรณีที่จำกัดเวลาในการใช้บริการต่อเดือนสำหรับผู้ใช้ในแต่ละราย

4.2.4 Data Dictionary

Attribute	Data Type	Description	Key	P/FK Ref.
DOMAIN_NAME	Char(50)	Domain AAA Server	PK.	
IP Address	Char(15)	IP Address		
Description	Char(100)	รายละเอียด		

ตารางที่ 4.1 แสดง Data Dictionary ของ TABLE ROAMING

Attribute	Data Type	Description	Key	P/FK Ref.
USER_ID	Int(3)	รหัสผู้ใช้	PK.	
USER_NAME	Char(32)	ชื่อผู้ใช้		
USER_FULLNAME	Char(80)	ชื่อผู้ใช้เต็ม		
PASSWORD	Char(13)	รหัสผ่าน		
TIME_RESTRICTION	Char(168)	ข้อจำกัดเรื่องวันเวลา เก็บค่า Y หรือ N ตามเวลาที่มีแต่ละวันและจำนวนวันในสัปดาห์ (24*7 Y=ใช้งานได้,N=ใช้งานไม่ได้)		
EXPIRE_DATE	Date	วันหมดอายุ		
SERVICE_EXEC	Char(1)	Y = บริการ EXEC		
SERVICE_PPP	Char(1)	Y = บริการ PPP		
ADMINISTRATOR	Char(1)	Y = เป็นผู้ควบคุมระบบ		
ROAMING_STATUS	Char(1)	Y = ใช้บริการ Roaming		
NCONNECT	Int(3)	จำนวนครั้งที่ติดต่อได้/วัน		
NSECOND	Int(7)	จำนวนนาทีที่ใช้งานได้/เดือน		

ตารางที่ 4.2 แสดง Data Dictionary ของ TABLE USER

Attribute	Data Type	Description	Key	P/FK Ref.
NAS_ID	Int(3)	รหัส NAS	PK.	
NAS_NAME	Char(32)	ชื่อ NAS		
NAS_ADDRESS	Char(15)	IP Address ของ NAS		
NAS_FULLNAME	Char(80)	ชื่อของ NAS		
ENABLE_PASSWORD	Char(13)	ENABLE_PASSWORD		

ตารางที่ 4.3 แสดง Data Dictionary ของ TABLE NAS

Attribute	Data Type	Description	Key	P/FK Ref.
USER_ID	Int(3)	รหัสผู้ใช้	PK.	USER
NAS_ID	Int(3)	รหัส NAS	PK.	NAS

ตารางที่ 4.4 แสดง Data Dictionary ของ TABLE NAS_PERMIT

Attribute	Data Type	Description	Key	P/FK Ref.
USER_ID	Int(3)	รหัสผู้ใช้	PK.	USER
NAS_ID	Int(3)	รหัส NAS	PK.	NAS

ตารางที่ 4.5 แสดง Data Dictionary ของ TABLE NAS_DENY

Attribute	Data Type	Description	Key	P/FK Ref.
USER_ID	Int(3)	รหัสผู้ใช้	PK.	USER
CMD	Char(255)	คำสั่ง	PK.	
CMD_ARG	Char(255)	Argument ของคำสั่ง		

ตารางที่ 4.6 แสดง Data Dictionary ของ TABLE CMD_PERMIT

Attribute	Data Type	Description	Key	P/FK Ref.
USER_ID	Int(3)	รหัสผู้ใช้	PK.	USER
CMD	Char(255)	คำสั่ง	PK.	
CMD_ARG	Char(255)	Argument ของคำสั่ง		

ตารางที่ 4.7 แสดง Data Dictionary ของ TABLE CMD_DENY

Attribute	Data Type	Description	Key	P/FK Ref.
DATE	Date	วันที่	PK.	
TIME	Time	เวลา	PK.	
USER_ID	Int(3)	รหัสผู้ใช้	PK.	USER
NAS_ID	Int(3)	รหัส NAS	PK.	NAS
NAS_PORT	Char(20)	หมายเลข Port ที่ต่อเข้ามา	PK.	
ROAMING_STATUS	Char(1)	0 หรือ 1 = บริการ Roaming		

ตารางที่ 4.8 แสดง Data Dictionary ของ TABLE CURRENT

Attribute	Data Type	Description	Key	P/FK Ref.
ROAMING_STATUS	Char(1)	0 หรือ 1 = บริการ Roaming	PK.	
DATE	Date	วันที่	PK.	
Time	Time	เวลา	PK.	
NAS_ID	Int(3)	รหัส NAS	PK.	NAS
NO_OF_USER	Int(3)	จำนวนผู้ใช้บริการ		

ตารางที่ 4.9 แสดง Data Dictionary ของ TABLE UTILIZATION

Attribute	Data Type	Description	Key	P/FK Ref.
DATETIME	DateTime	วันที่/เวลา	PK.	
USER_NAME	Char(32)	ชื่อผู้ใช้		

Attribute	Data Type	Description	Key	P/FK Ref.
NAS_ADDRESS	Char(15)	หมายเลข IP ของ NAS		
NAS_PORT	Char(20)	หมายเลข Port ที่ต่อเข้ามา		
REASON	Char(20)	เหตุผล		

ตารางที่ 4.10 แสดง Data Dictionary ของ TABLE LOGIN_FAIL

Attribute	Data Type	Description	Key	P/FK Ref.
ACCT_ID	Int(4)	รหัส Acct	PK.	
DATE	Date	วันที่		
TIME	Time	เวลา		
NAS_ID	Int(3)	รหัส NAS	FK.	NAS
USER_ID	Int(3)	รหัสผู้ใช้	FK.	USER
TERMINAL_ID	Char(10)	หมายเลข Terminal		
REMOTE_ADDRESS	Char(15)	IP Address ของผู้ใช้		
TASK_ID	Char(255)	Task ID		
START_TIME	Char(255)	เวลาเริ่มต้น		
TIMEZONE	Char(255)	Timezone		
SERVICE	Char(255)	บริการที่ใช้		
ELAPSED_TIME	Char(255)	เวลาที่ใช้งาน		
ROAMING_STATUS	Char(1)	0 หรือ 1 = บริการ Roaming		

ตารางที่ 4.11 แสดง Data Dictionary ของ TABLE ACCT_USER

Attribute	Data Type	Description	Key	P/FK Ref.
ACCT_ID	Int(4)	รหัส Acct	PK.	
DATE	Date	วันที่		
TIME	Time	เวลา		
NAS_ID	Int(3)	รหัส NAS	FK.	NAS

Attribute	Data Type	Description	Key	P/FK Ref.
USER_ID	Int(3)	รหัสผู้ใช้	FK.	USER
TERMINAL_ID	Char(10)	หมายเลข Terminal		
REMOTE_ADDRESS	Char(15)	IP Address ของผู้ใช้		
TASK_ID	Char(255)	Task ID		
START_TIME	Char(255)	เวลาเริ่มต้น		
TIMEZONE	Char(255)	Timezone		
SERVICE	Char(255)	บริการที่ใช้		
PRIV_LVL	Int(1)	ระดับความสามารถ		
CMD	Char(255)	คำสั่ง		
ROAMING_STATUS	Char(1)	0 หรือ 1 = บริการ Roaming		

ตารางที่ 4.12 แสดง Data Dictionary ของ TABLE ACCT_CMD

Attribute	Data Type	Description	Key	P/FK Ref.
USER_ID	Int(3)	รหัสผู้ใช้	PK.	USER
DATE	Date	วันที่	PK.	
NTIME	Int(3)	จำนวนครั้งที่ติดต่อเข้ามาใช้งานได้ต่อวัน		

ตารางที่ 4.13 แสดง Data Dictionary ของ TABLE LIMIT_CONN

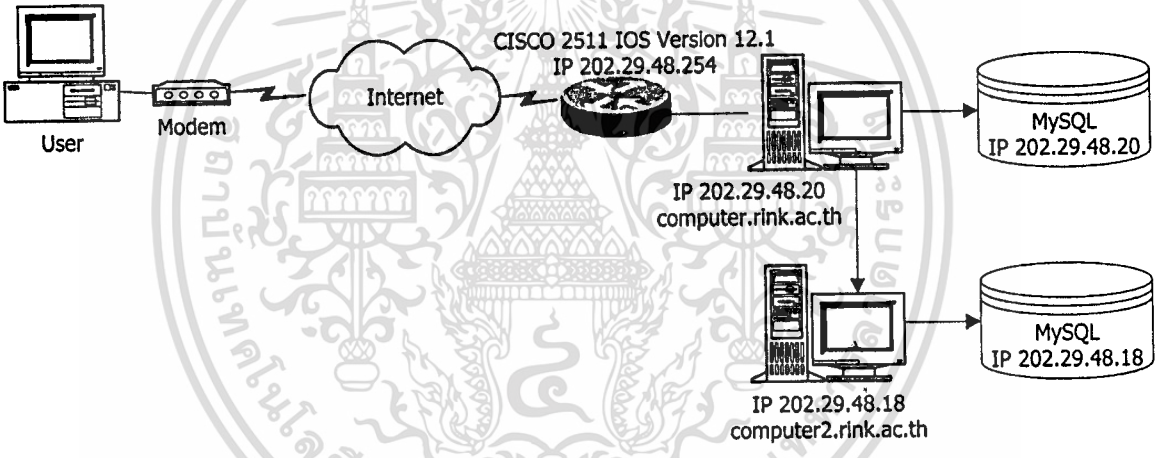
Attribute	Data Type	Description	Key	P/FK Ref.
USER_ID	Int(3)	รหัสผู้ใช้	PK.	USER
NMONTH	Char(6)	ปี/เดือน	PK.	
NTIME	Int(3)	จำนวนนาทีที่สามารถใช้งานได้ต่อเดือน		

ตารางที่ 4.14 แสดง Data Dictionary ของ TABLE LIMIT_MONTH

บทที่ 5

การพัฒนาระบบและทดลอง

การพัฒนาโปรแกรมควบคุมการใช้อินเตอร์เน็ตจากระยะไกลแบบใช้ข้อตกลงร่วมกัน พัฒนาโดยใช้ TACACS+ Protocol เป็น Protocol ที่ติดต่อระหว่าง AAA Server ด้วยภาษาซีที่มี mySQL เป็น Database Server และทำงานภายใต้ระบบปฏิบัติการ Linux RedHat 6.1 Thai ในส่วนของผู้ใช้ที่เป็นผู้บริหารระบบ (Admin) พัฒนาด้วยภาษา PHP สำหรับ NAS ใช้ของ Cisco Systems, Inc. รุ่น Cisco 2511 Software IOS Version 12.1 ดังรูปที่ 5.1



รูปที่ 5.1 แสดงการติดต่อไปยังระบบ

5.1 การกำหนดค่าเริ่มต้นของ NAS

5.1.1 ค่าเริ่มต้น

- กำหนด local user ไว้กรณี TACACS+ Server Down ใช้คำสั่งดังนี้

  NAS(config)#user local-username password local-password

- เพิ่มความสามารถด้าน AAA ใช้คำสั่งดังนี้

  NAS(config)#aaa new-model

- กำหนด ip address ของ TACACS+ Server ใช้คำสั่งดังนี้

  NAS(config)#tacacs-server host <ip_address> port <port_number>

- กำหนด shared secret key ใช้ encrypt ข้อมูลระหว่าง NAS – TACACS+ Server ใช้คำสั่งดังนี้

  NAS(config)#tacacs-server key <yourkey>

5.1.2 Authentication

- วิธี Authentication มีดังนี้
  - enable ใช้ enable password
  - line ใช้ line password
  - local ใช้ local username database
  - none ไม่ต้อง Authentication
  - tacacs+ ใช้ TACACS+ Authentication
- กำหนด login authentication ด้วยวิธี tacacs+ และเมื่อไม่สามารถติดต่อ TACACS+ Server ได้ให้ใช้วิธี local data ใช้คำสั่งดังนี้

  NAS(config)#aaa authentication login default group tacacs+ local
- กำหนดให้ login จาก async ppp port ต้อง authentication ด้วยวิธี tacacs+ และเมื่อไม่สามารถติดต่อ TACACS+ Server ได้ให้ใช้วิธี local data ใช้คำสั่งดังนี้

  NAS(config)#aaa authentication ppp default if-needed group tacacs+ local

  NAS(config)#interface Group-Async1

  NAS(config-line)#encapsulation ppp

  NAS(config-line)#ppp authentication pap
- กำหนดให้ เมื่อต้องการ enable privilege ต้อง authentication ด้วยวิธี tacacs+ และเมื่อไม่สามารถติดต่อ TACACS+ Server ได้ให้ใช้วิธี local enable ใช้คำสั่งดังนี้

  NAS(config)# aaa authentication enable default group tacacs+ enable

5.1.3 Authorization

- Keyword บริการต่างๆ

  Network บริการ SLIP, PPP, PPP NCPs, และ ARA

  Exec บริการ shell

  Command level การใช้คำสั่งต่างๆ ใน privilege level นั้นๆ
- วิธี Authorization มีดังนี้

  tacacs+ ใช้ TACACS+ Authentication

if-authenticated อนุญาตให้ผู้ใช้ที่ผ่าน authentication แล้ว

none ไม่ต้อง Authorization

local ใช้ local database สำหรับ authorization

- กำหนดให้ผู้ใช้ที่ต้องการใช้บริการ EXEC ต้อง authorization ด้วยวิธี tacacs+ และเมื่อไม่สามารถติดต่อ TACACS+ Server ได้ ไม่ต้อง authorization ใช้คำสั่งดังนี้

NAS(config)#aaa authorization exec default group tacacs+ local

- กำหนดให้ผู้ใช้ที่ต้องการใช้บริการ Network ต้อง authorization ด้วยวิธี tacacs+ และเมื่อไม่สามารถติดต่อ TACACS+ Server ได้ ไม่ต้อง authorization ใช้คำสั่งดังนี้

NAS(config)#aaa authorization network default group tacacs+ local

- กำหนดให้ผู้ใช้ที่ต้องการใช้คำสั่งที่มี privilege 1 ต้อง authorization ด้วยวิธี tacacs+ และเมื่อไม่สามารถติดต่อ TACACS+ Server ได้ ไม่ต้อง authorization ใช้คำสั่งดังนี้

NAS(config)#aaa authorization commands 1 default group tacacs+
if-authenticated none

- กำหนดให้ผู้ใช้ที่ต้องการใช้คำสั่งที่มี privilege 15 ต้อง authorization ด้วยวิธี tacacs+ และเมื่อไม่สามารถติดต่อ TACACS+ Server ได้ ให้ดูที่ Local ใช้คำสั่งดังนี้

NAS(config)#aaa authorization commands 15 default group tacacs+
if-authenticated local

5.1.4 Accounting

- Event Type คือประเภทของเหตุการณ์ที่ให้มีการส่ง Accounting packet

system กรณีเกิด event system-level เช่น reload

network บริการ SLIP, PPP, PPP NCPs และ ARA

connection บริการ outbound telnet และ rlogin

exec บริการ shell

command level การใช้คำสั่งต่างๆ ใน privilege level นั้นๆ

- Keyword

stop-only ส่ง ACCT pkt เมื่อเลิกใช้บริการเท่านั้น

start-stop ส่ง ACCT pkt เมื่อเริ่มและเลิกใช้บริการ

wait-start เหมือน start-stop แต่จะไม่ให้บริการจนกว่าจะได้รับ packet ยืนยันจาก Server ก่อน

- กำหนดให้มีการส่ง Account packet กรณีที่เริ่มและเลิกใช้บริการ Shell ใช้คำสั่งดังนี้

  NAS(config)#aaa accounting exec default start-stop group tacacs+

- กำหนดให้มีการส่ง Account packet กรณีที่เริ่มและเลิกใช้บริการ Network (PPP) ใช้คำสั่งดังนี้

  NAS(config)#aaa accounting network default start-stop group tacacs+

- กำหนดให้มีการส่ง Account packet กรณีที่ใช้คำสั่งในระดับ privilege 1 ใช้คำสั่งดังนี้

  NAS(config)#aaa accounting commands 1 default start-stop group tacacs+

- กำหนดให้มีการส่ง Account packet กรณีที่ใช้คำสั่งในระดับ privilege 15 (สูงสุด) ใช้คำสั่งดังนี้

  NAS(config)#aaa accounting commands 15 default start-stop group tacacs+

- กำหนดให้มีการส่ง Account packet กรณีเกิด event system-level ให้ใช้คำสั่งดังนี้

  NAS(config)#aaa accounting system default start-stop group tacacs+

5.1.5 สรุปการ Configuration

```
!
user local-username password local-password
!
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authentication ppp default if-needed group tacacs+ local
!
aaa authorization exec default group tacacs+ local
aaa authorization network default group tacacs+ local
!
aaa authorization commands 1 default group tacacs+ if-authenticated none
aaa authorization commands 15 default group tacacs+ if-authenticated local
!
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
```

```
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
interface Group-Async1
    encapsulation ppp
    ppp authentication pap
!
tacacs-server host <ip_address> port <port_number>
tacacs-server key <yourkey>
```

5.2 การติดตั้ง AAA DEAMON

- การติดตั้ง AAA Deamon ทำได้โดยใช้คำสั่งดังนี้

  $AAA_DIR/tac_plus –C tac_plus.conf

ในกรณีที่ต้องการติดตั้งแบบอัตโนมัติเมื่อเริ่มเปิดเครื่องให้เพิ่มคำสั่งไว้ที่ไฟล์ /etc/rc.d/rc.local

- Configuration AAA Demon ให้กำหนดค่าที่ไฟล์ tac_plus.conf ดังนี้

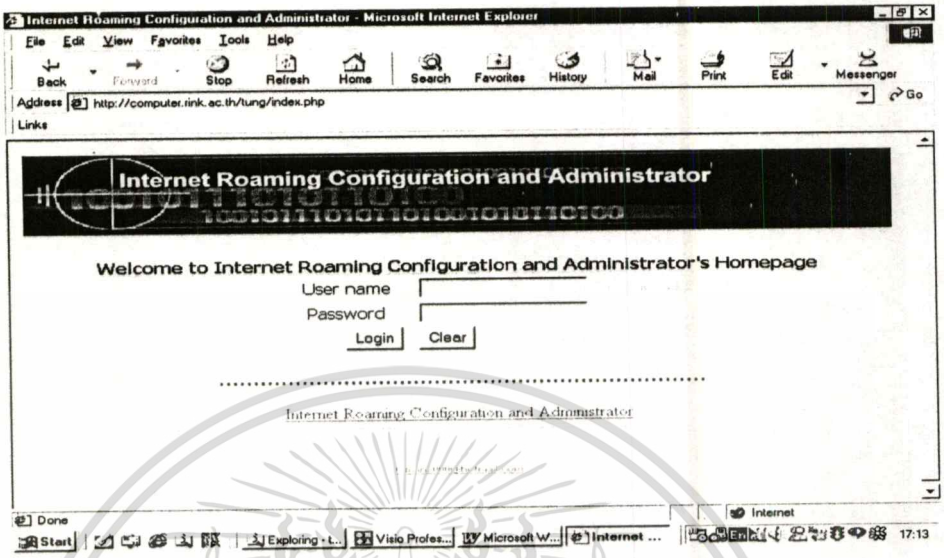
  key = <yourkey>

  ใช้สำหรับเข้ารหัสข้อมูล โดยจะต้องกำหนดค่าให้ตรงกับ tacacs-server key ที่กำหนดไว้ใน Router

5.3 หน้าจอที่ติดต่อกับผู้ใช้ (Admin)

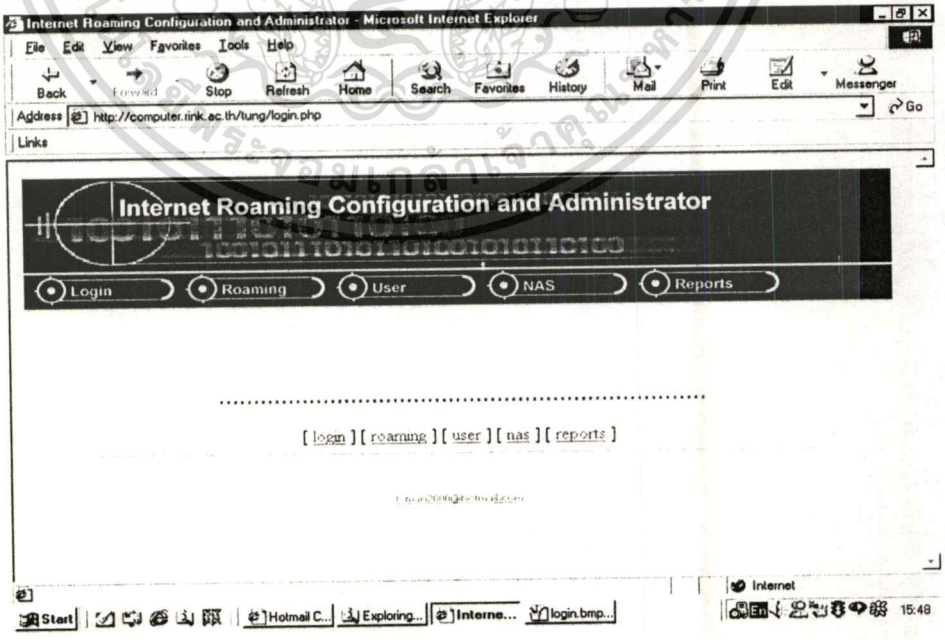
Web Interface ของระบบใช้สำหรับผู้ใช้ที่เป็น Admin เพื่อเพิ่มเติมเงื่อนไขต่าง ๆ เช่น เงื่อนไขการ Roaming, การเพิ่มชื่อผู้ใช้, NAS เป็นต้น และออกรายงานต่าง ๆ ดังมีรายละเอียดและหน้าจอการแสดงผลดังต่อไปนี้

5.3.1 Login



รูปที่ 5.2 แสดงหน้าจอก่อนเข้าระบบ

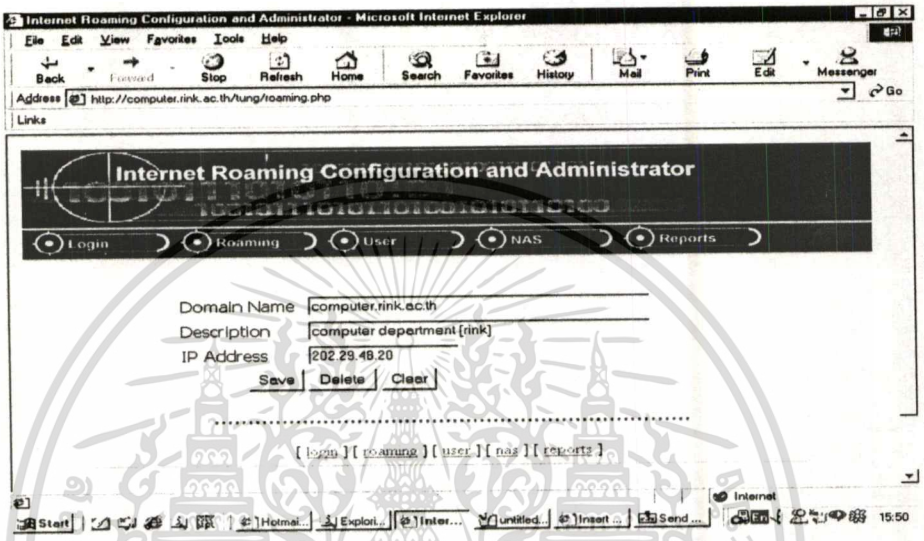
สำหรับผู้บริหารระบบ (Admin) โดยผู้ใช้จะต้องมีชื่ออยู่ในฐานข้อมูลของระบบและเป็น Admin เท่านั้น โดยให้ป้อนชื่อผู้ใช้เป็นลักษณะ e-mail address หลังจาก Login ผ่านแล้วจะแสดงหน้าจอดังรูปที่ 5.3 เพื่อให้ทำรายการอื่น ๆ ต่อไป



รูปที่ 5.3 แสดงหน้าจอหลังจากการ Login

5.3.2 Roaming Configuration

คือส่วนของการกำหนดข้อตกลงร่วมกันระหว่างเซิร์ฟเวอร์ ใช้ในกรณีที่ผู้ใช้เป็นแบบ Roaming โดยเมื่อระบบค้นหาชื่อผู้ใช้ไม่พบใน Local เซิร์ฟเวอร์แล้วจะไปค้นหาที่เซิร์ฟเวอร์ใด ดังแสดงตามรูปที่ 5.4



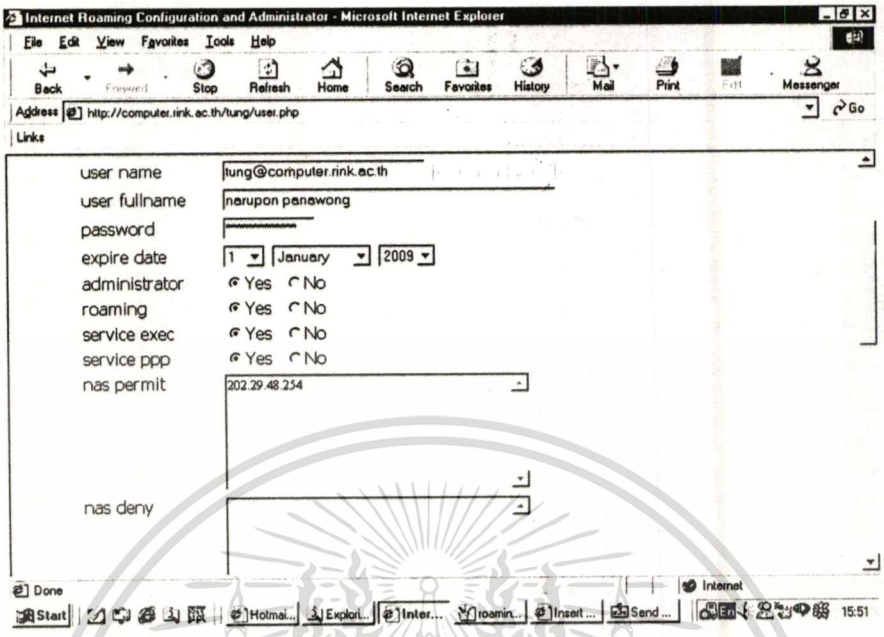
รูปที่ 5.4 แสดงหน้าจอกำหนดค่า Roaming

ตามรูปที่ 5.4 มีรายละเอียดของการกำหนดค่าดังนี้

- Domain Name ชื่อ domain name
- Description รายละเอียด
- IP Address หมายเลข IP ของเซิร์ฟเวอร์ที่ตกลงร่วมกันไว้

5.3.3 User Information

คือส่วนในการกำหนดชื่อผู้ใช้และเงื่อนไขการใช้งาน (Admin, PPP, Roaming), เงื่อนไขของเวลา (วันหมดอายุ, จำนวนครั้งที่เข้ามาได้ต่อวัน, จำนวนชั่วโมงที่ใช้บริการต่อเดือน), เงื่อนไขในการใช้หรือไม่ให้ใช้ NASและเงื่อนไขในการใช้หรือไม่ใช้คำสั่ง ดังแสดงในรูปที่ 5.5



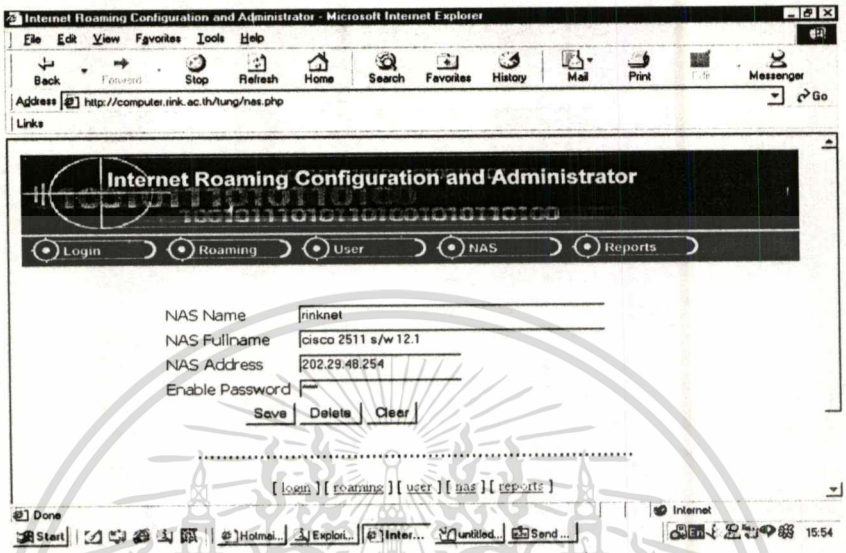
รูปที่ 5.5 แสดงหน้าจอรายละเอียดของผู้ใช้

ตามรูปที่ 5.5 มีรายละเอียดของการกำหนดค่าดังนี้

- User Name ชื่อผู้ใช้ให้ป้อนเป็น e-mail address
- User Fullname ชื่อเต็มของผู้ใช้
- Password รหัสผ่าน
- Expire Date วันที่หมดอายุ
- Administrator เป็น Admin หรือไม่
- Roaming บริการ Roaming หรือไม่
- Service Exec บริการ Exec หรือไม่
- Service PPP บริการ PPP หรือไม่
- NAS Permit NAS ที่อนุญาตให้ใช้งานได้
- NAS Deny NAS ที่ไม่อนุญาตให้ใช้งานได้
- Command Permit คำสั่งที่อนุญาตให้ใช้งานได้
- Command Deny คำสั่งไม่อนุญาตให้ใช้งาน
- Time Restriction ช่วงเวลาที่อนุญาตให้ใช้งานหรือไม่ให้ใช้งาน
- Connect Per Time จำนวนครั้งที่เข้ามาใช้บริการได้ต่อวัน
- Time of Use Per Month จำนวนเวลาที่ใช้บริการได้ (หน่วยเป็นนาที)

5.3.4 NAS Configuration

คือใช้สำหรับอนุญาตให้ใช้ NAS ได้หรือไม่ได้ ดังแสดงในรูปที่ 5.6



รูปที่ 5.6 แสดงหน้าจอการกำหนด NAS

ตามรูปที่ 5.6 มีรายละเอียดของการกำหนดค่าดังนี้

- NAS Name ชื่อ NAS
- NAS Fullname ชื่อเต็มของ NAS
- NAS Address หมายเลข IP ของ NAS
- Enable Password Enable Privilege Password

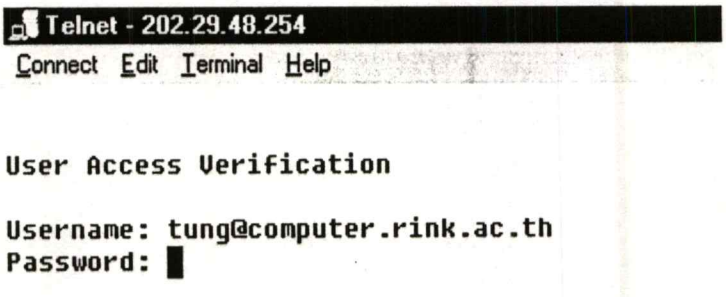
5.4 การทดสอบ

การทดสอบระบบทำได้ 2 วิธีคือ

1. Telnet

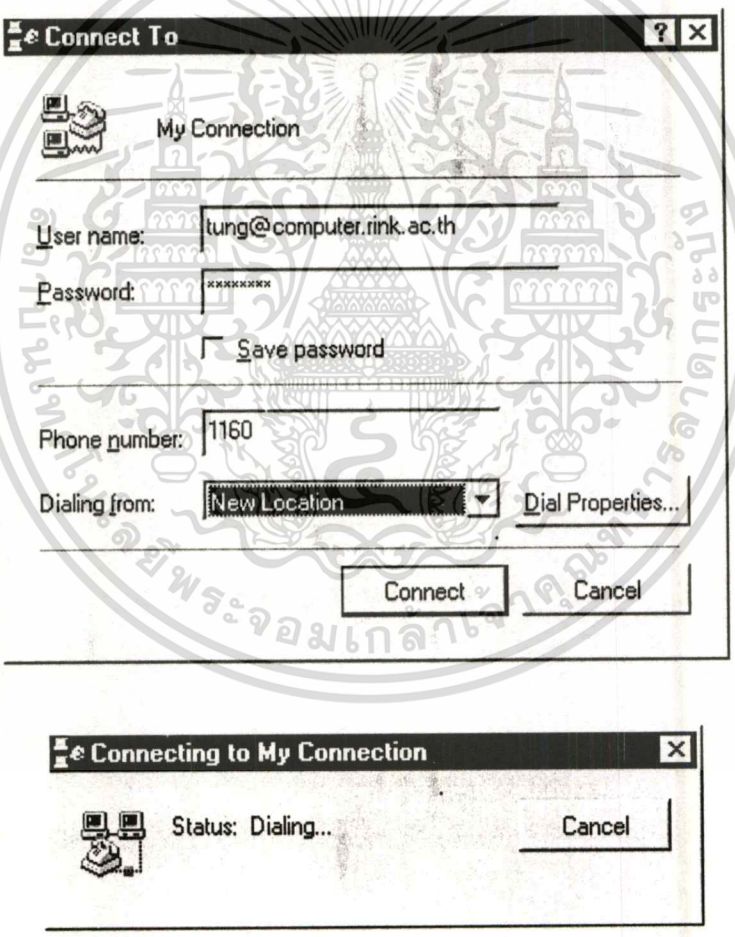
   #telnet <router>

   ป้อนชื่อเป็นลักษณะของ e-mail address แล้วลองใช้คำสั่งต่าง ๆ คำสั่งจะใช้งานได้หรือไม่ได้นั้นขึ้นอยู่กับการกำหนดค่าในส่วนของรายละเอียดผู้ใช้งาน ดังแสดงตามรูปที่ 5.7



รูปที่ 5.7 แสดงหน้าจอตัวอย่างการใช้งาน telnet

2. Modem

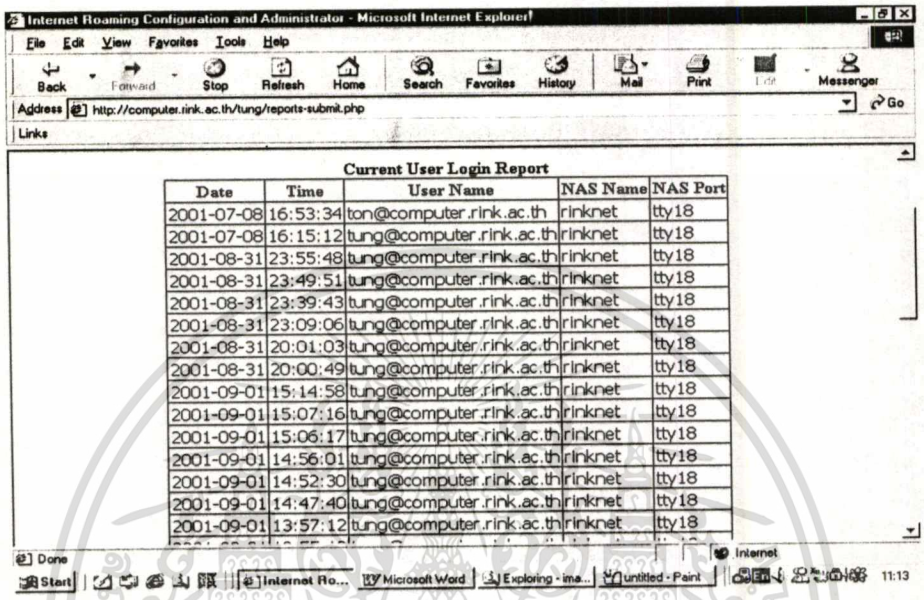


รูปที่ 5.8 แสดงหน้าจอตัวอย่างการใช้งานผ่าน modem

5.5 รายงาน

5.5.1 รายงานการเข้าใช้งานของผู้ใช้

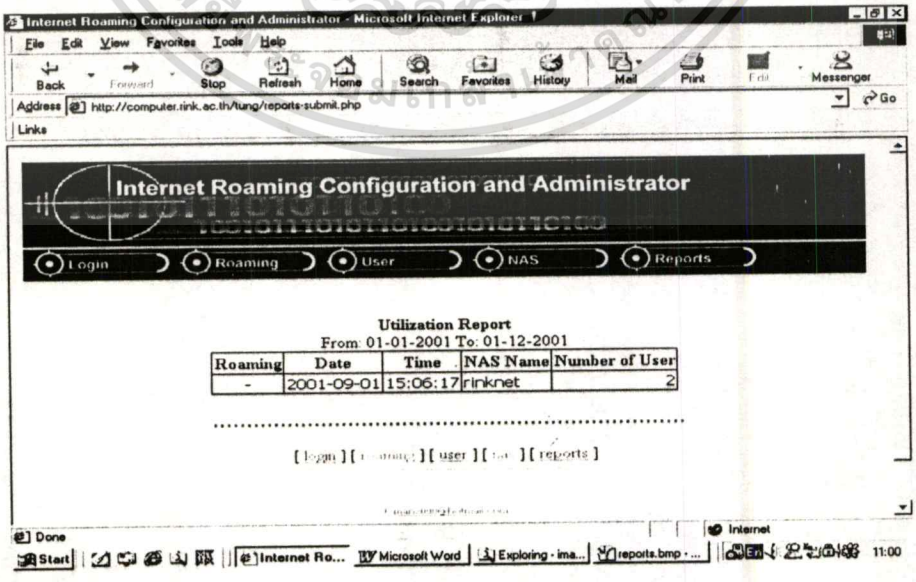
เป็นรายงานที่แสดงรายชื่อผู้ใช้งานในระบบ ณ เวลาปัจจุบัน



รูปที่ 5.9 แสดงรายงานผู้เข้าใช้งาน

5.5.2 รายงานการเข้าใช้งาน NAS

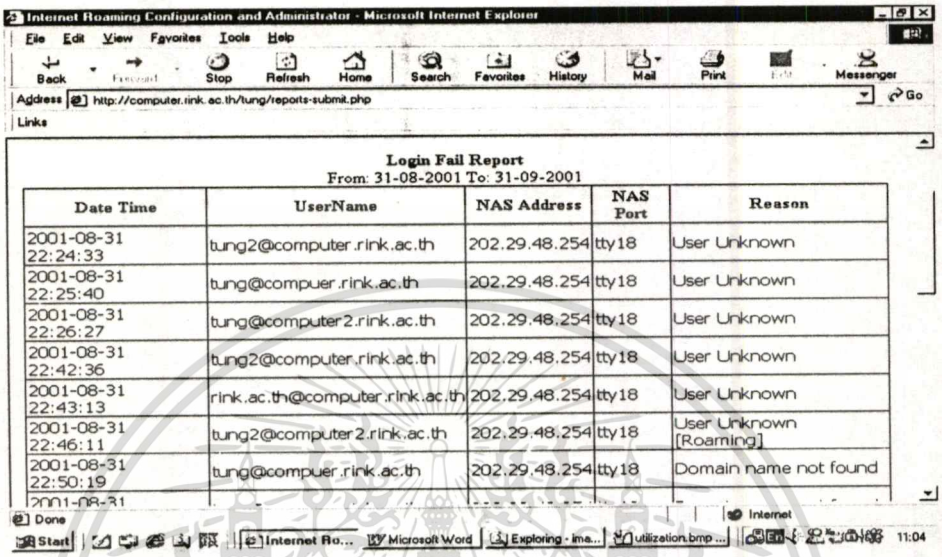
เป็นรายงานที่แสดงจำนวนผู้ใช้งาน โดยสามารถเลือกเวลาที่ต้องการและ NAS ได้



รูปที่ 5.10 แสดงรายงานการเข้าใช้งาน NAS

5.5.3 รายงาน Login Fail

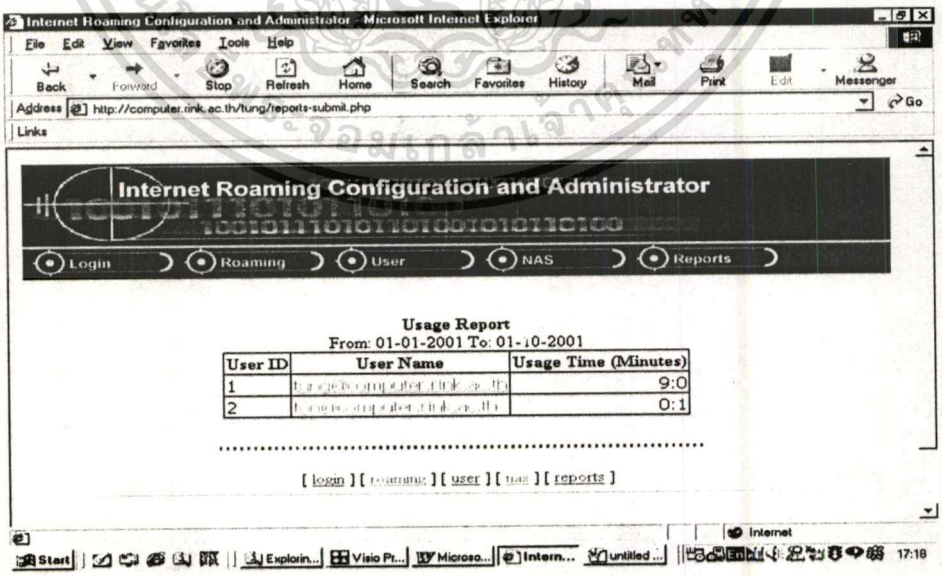
เป็นรายงานที่แสดงรายชื่อผู้ใช้งานที่ไม่สามารถติดต่อเข้ามาใช้งานได้



รูปที่ 5.11 แสดงรายงาน Login Fail

5.5.4 รายงานการเข้าใช้งานของผู้ใช้

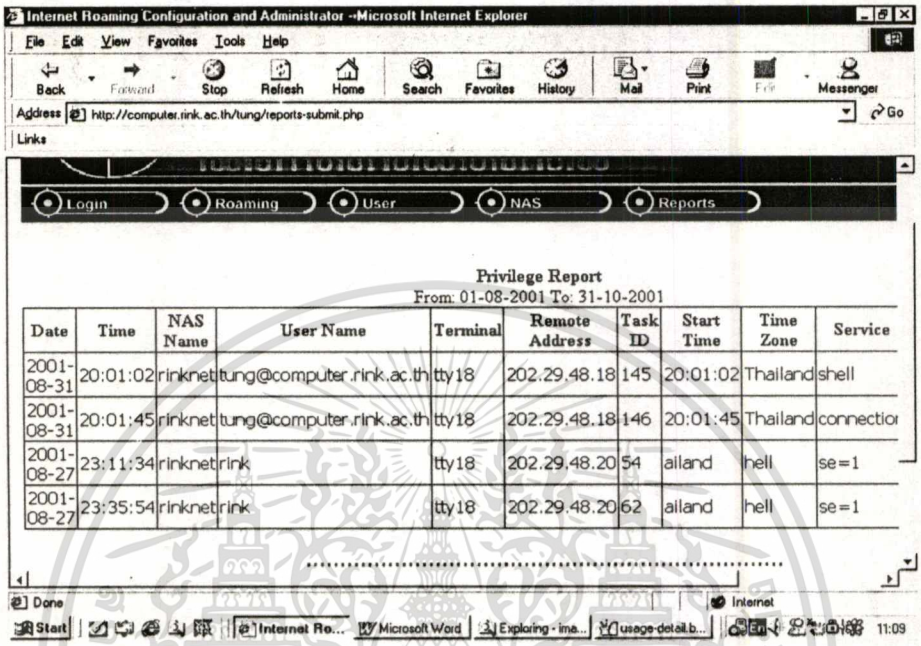
เป็นรายงานชื่อแสดงรายชื่อผู้ใช้งานและจำนวนชั่วโมงที่ใช้งาน



รูปที่ 5.12 แสดงรายงานการเข้าใช้งานของผู้ใช้

5.5.5 รายงานการใช้คำสั่งของผู้ใช้

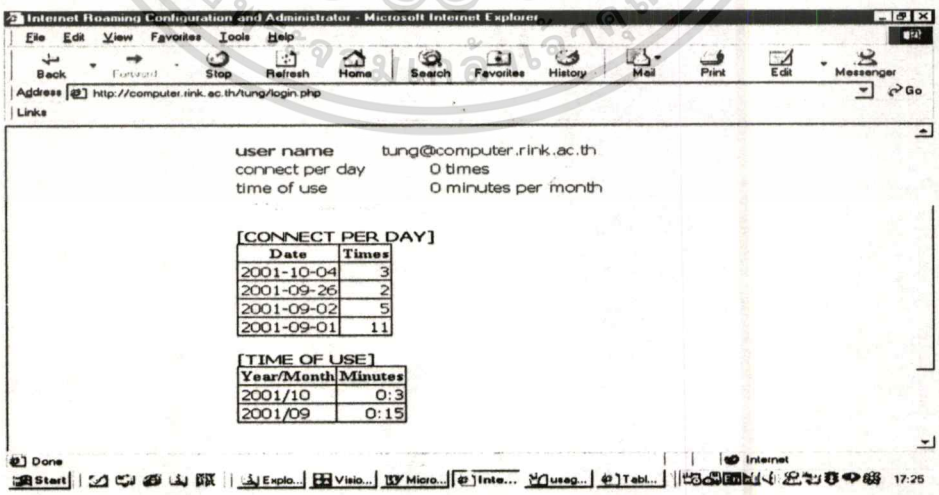
เป็นรายงานที่แสดงรายชื่อผู้ใช้งาน, วันเวลาและคำสั่งที่ใช้งาน



รูปที่ 5.13 แสดงรายงานการใช้คำสั่งของผู้ใช้

5.5.6 รายงานการตรวจสอบเวลาใช้งาน

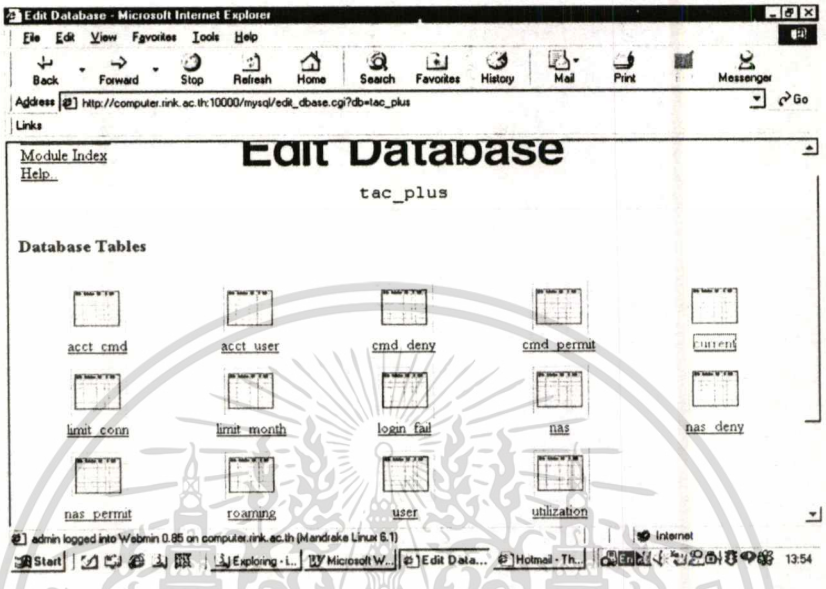
เป็นรายงานที่แสดงเวลาที่ใช้งานเพื่อให้ผู้ใช้สามารถตรวจสอบเวลาและจำนวนการใช้งาน



รูปที่ 5.14 แสดงรายงานการตรวจสอบเวลาใช้งาน

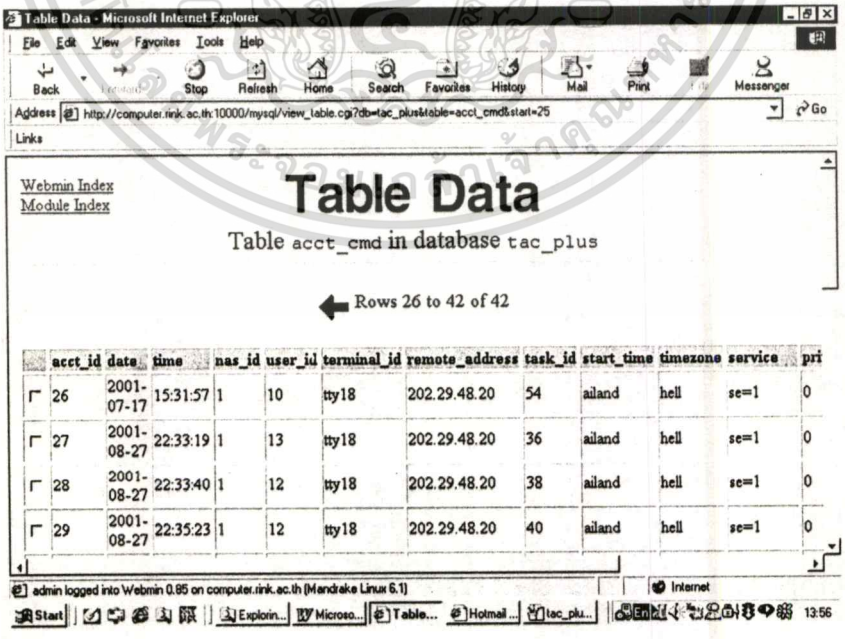
5.6 ตัวอย่างฐานข้อมูล

5.6.1 ตารางข้อมูลทั้งหมดที่อยู่ในฐานข้อมูล tac_plus



รูปที่ 5.15 แสดงตารางข้อมูลทั้งหมดที่อยู่ในฐานข้อมูล tac_plus

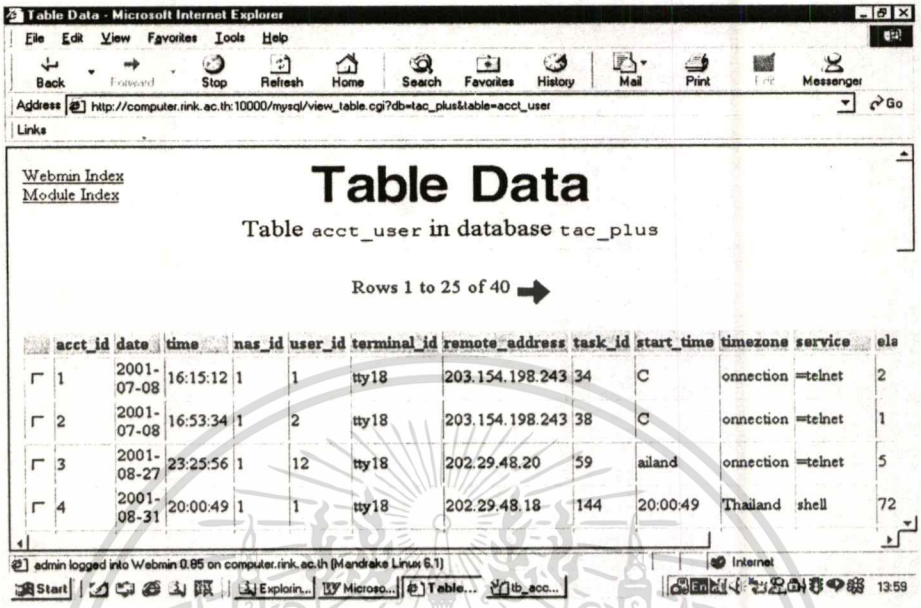
5.6.2 ตาราง acct_cmd



acct_id	date	time	nas_id	user_id	terminal_id	remote_address	task_id	start_time	timezone	service	pri
26	2001-07-17	15:31:57	1	10	tty18	202.29.48.20	54	ailand	hell	se=1	0
27	2001-08-27	22:33:19	1	13	tty18	202.29.48.20	36	ailand	hell	se=1	0
28	2001-08-27	22:33:40	1	12	tty18	202.29.48.20	38	ailand	hell	se=1	0
29	2001-08-27	22:35:23	1	12	tty18	202.29.48.20	40	ailand	hell	se=1	0

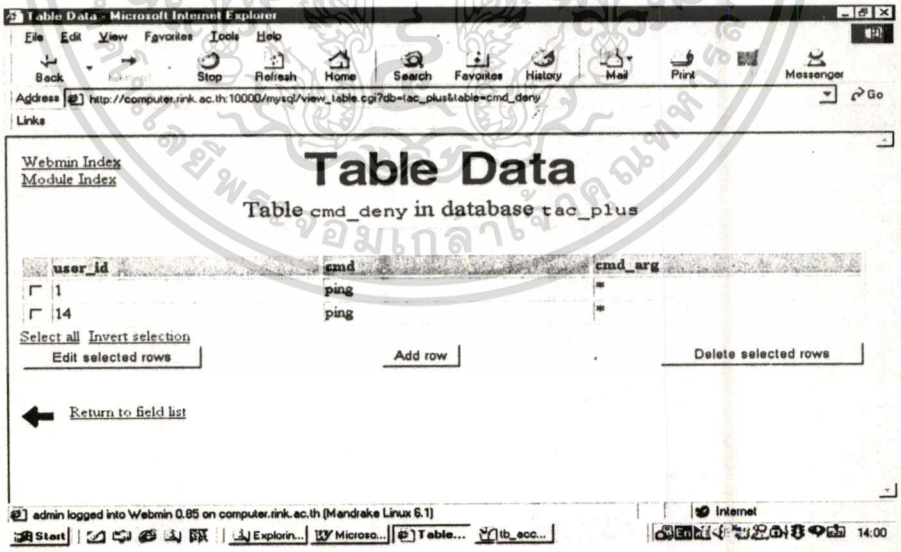
รูปที่ 5.16 แสดงข้อมูลในตาราง acct_cmd

5.6.3 ตาราง acc_user



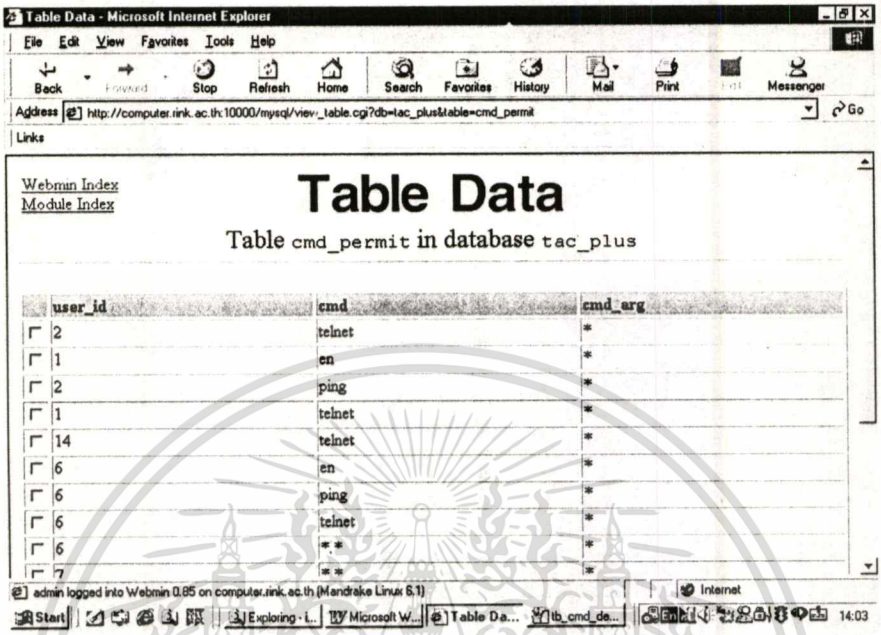
รูปที่ 5.17 แสดงข้อมูลในตาราง acct_user

5.6.4 ตาราง cmd_deny



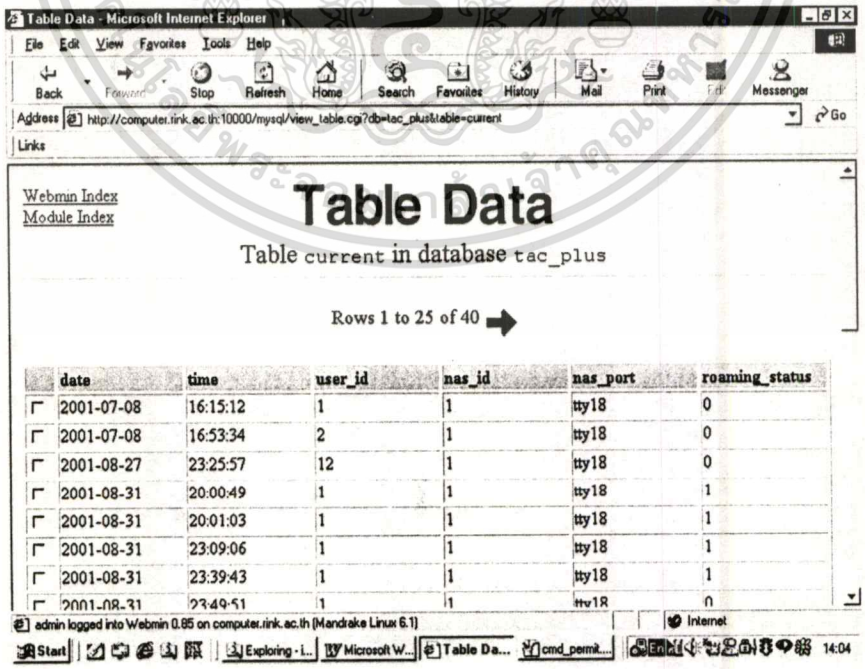
รูปที่ 5.18 แสดงข้อมูลในตาราง cmd_deny

5.6.5 ตาราง cmd_permit



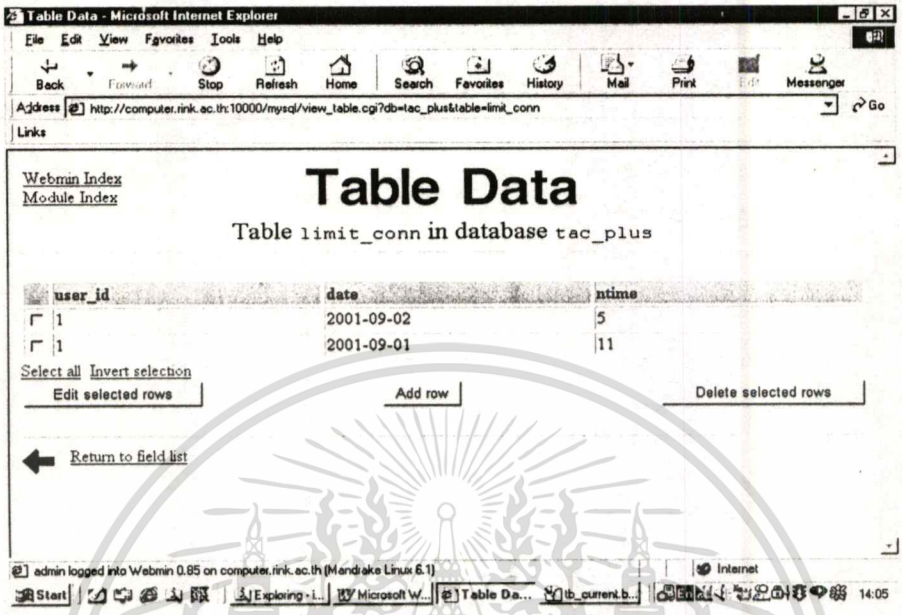
รูปที่ 5.19 แสดงข้อมูลในตาราง cmd_permit

5.6.6 ตาราง current



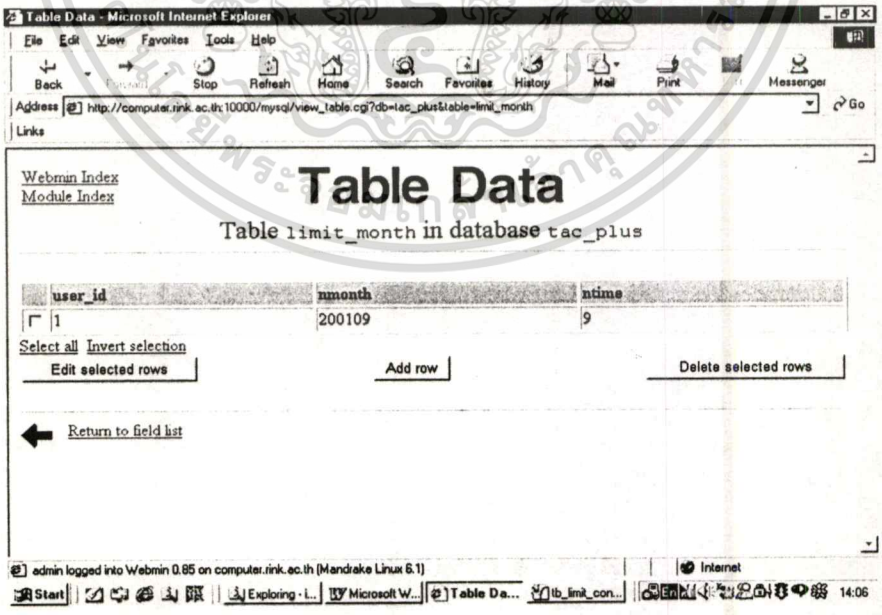
รูปที่ 5.20 แสดงข้อมูลในตาราง current

5.6.7 ตาราง limit_conn



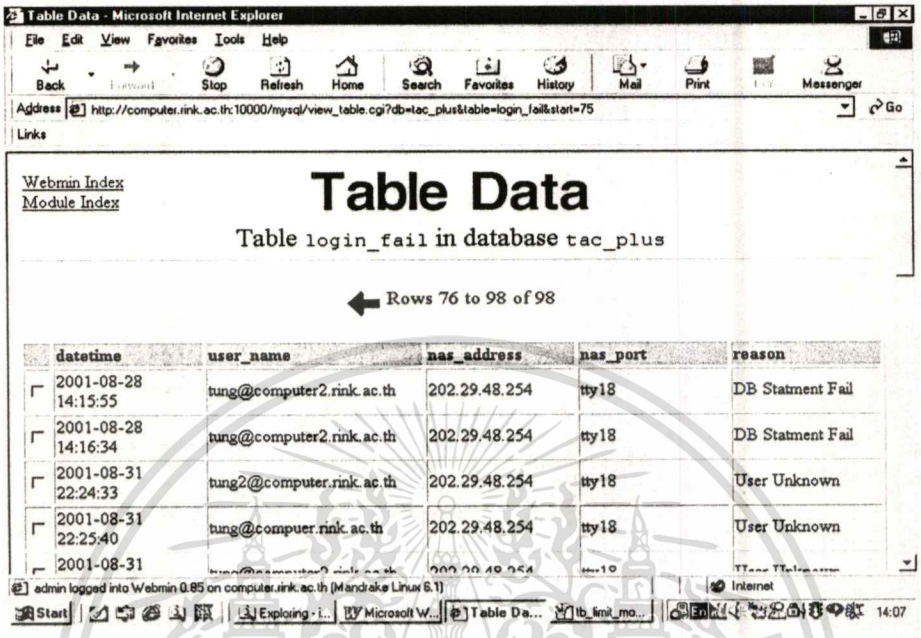
รูปที่ 5.21 แสดงข้อมูลในตาราง limit_conn

5.6.8 ตาราง limit_month



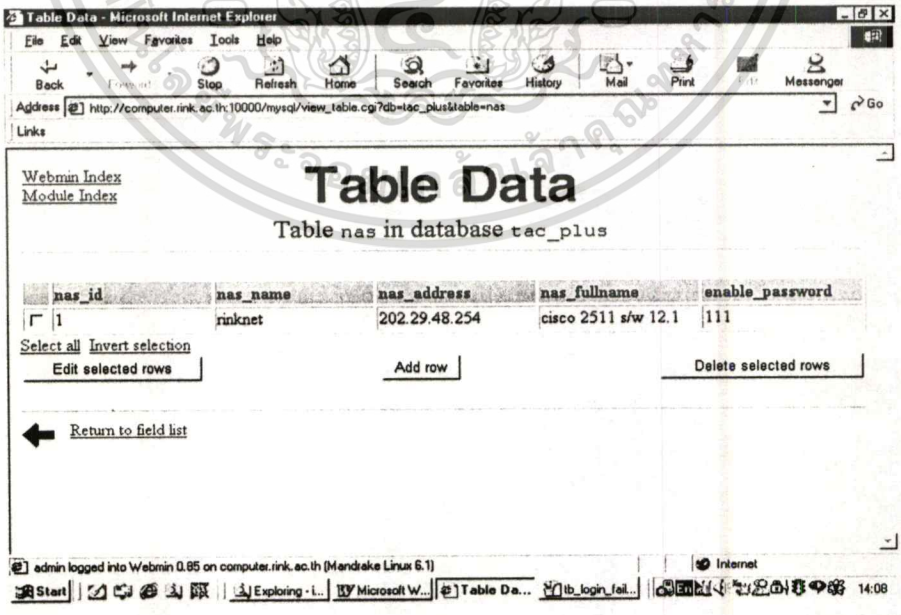
รูปที่ 5.22 แสดงข้อมูลในตาราง limit_month

5.6.9 ตาราง login_fail



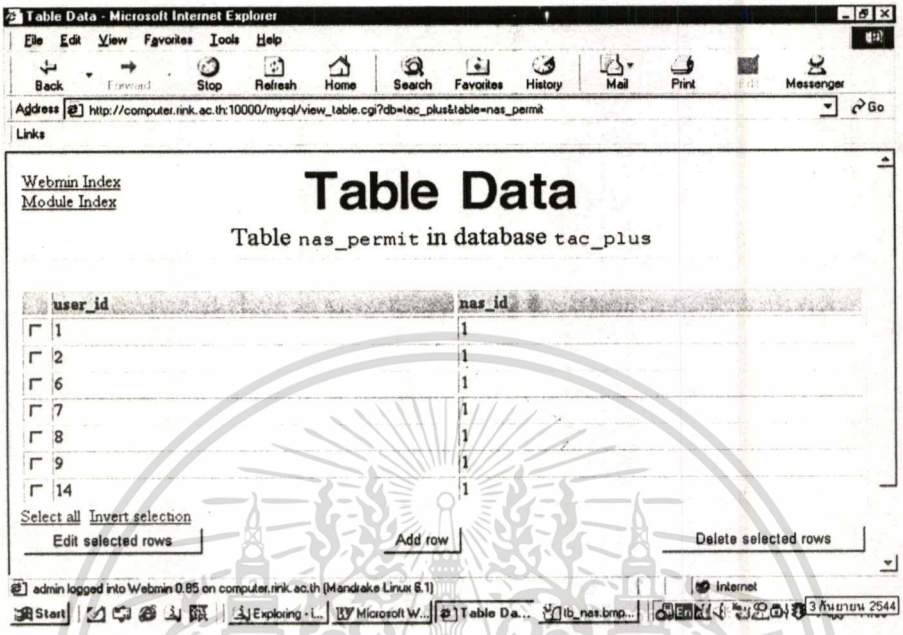
รูปที่ 5.23 แสดงข้อมูลในตาราง login_fail

5.6.10 ตาราง nas



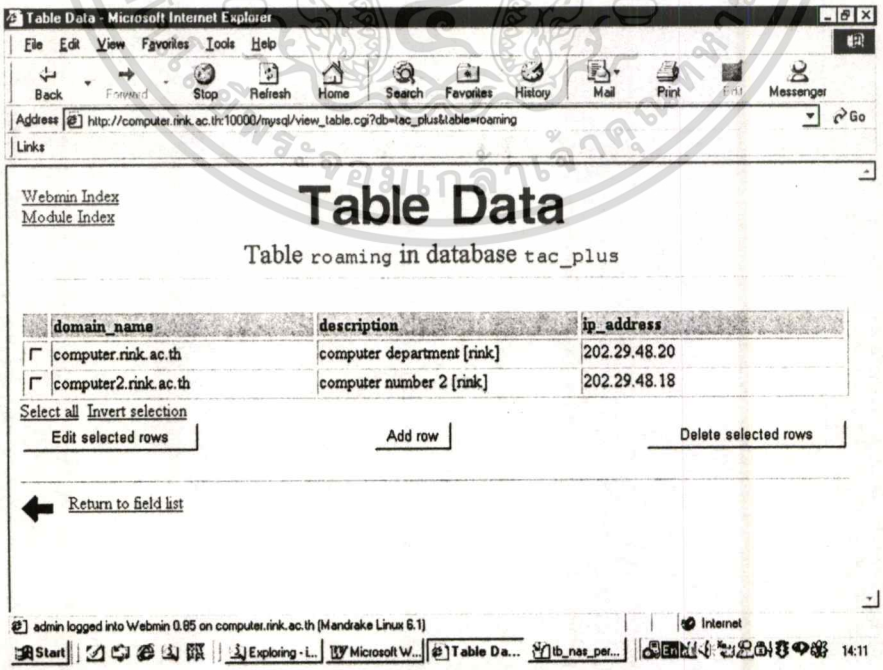
รูปที่ 5.24 แสดงข้อมูลในตาราง nas

5.6.11 ตาราง nas_permit



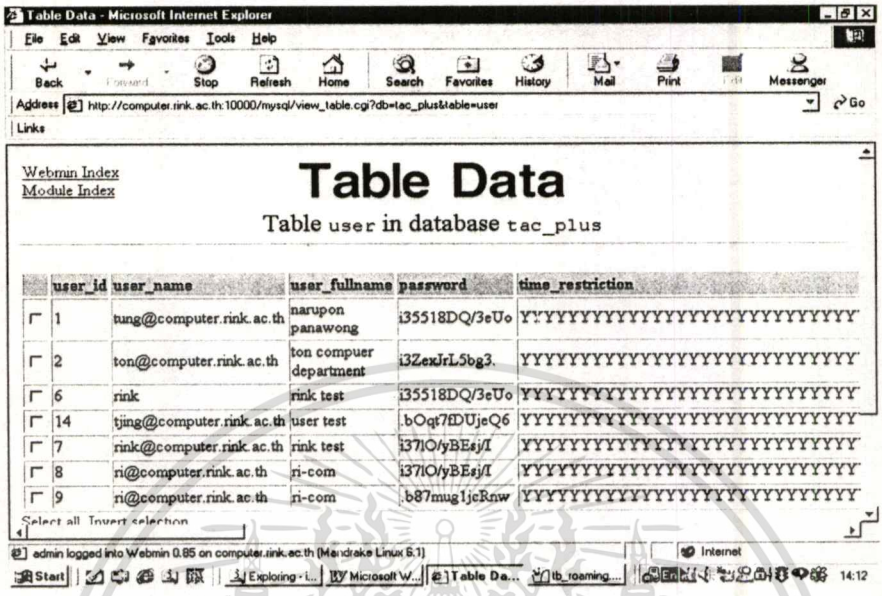
รูปที่ 5.25 แสดงข้อมูลในตาราง nas_permit

5.6.12 ตาราง roaming



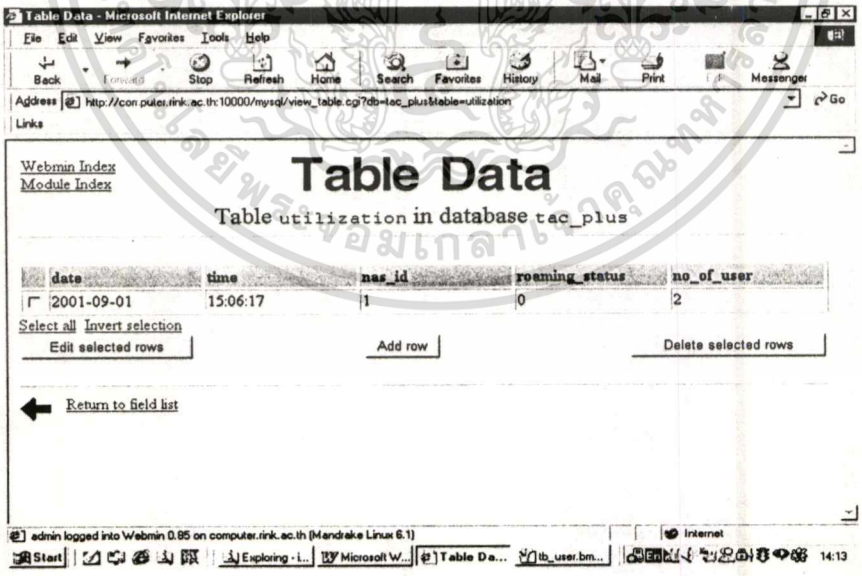
รูปที่ 5.26 แสดงข้อมูลในตาราง roaming

5.6.13 ตาราง user



รูปที่ 5.27 แสดงข้อมูลในตาราง user

5.6.14 ตาราง utilization



รูปที่ 5.28 แสดงข้อมูลในตาราง utilization

บทที่ 6
สรุปและข้อเสนอแนะ

6.1 สรุปผลการพัฒนาระบบ

จากการพัฒนาโปรแกรมควบคุมการใช้งานอินเตอร์เน็ตจากระยะไกลแบบใช้ข้อตกลงร่วมกันมีดังนี้

- มีความง่ายในการติดต่อเข้ามาขอใช้บริการในกรณีผู้ใช้ไม่ได้มีชื่ออยู่ในเซิร์ฟเวอร์ที่เข้าไปขอใช้งาน (Roaming) โดยใช้รหัสเดียวคือ e-mail address
- มีความง่ายในการใช้งานในส่วนของผู้บริหารระบบทั้งนี้เพราะติดต่อผ่าน Web Browser
- มีความง่ายในการนำข้อมูลไปใช้งานในด้านต่าง ๆ ได้ ทั้งนี้เพราะเก็บไว้ในฐานข้อมูล
- สามารถกำหนดนโยบายเกี่ยวกับความสามารถของผู้ใช้ได้มากขึ้นโดยเฉพาะอย่างยิ่งเรื่องคำสั่งที่อนุญาตให้ใช้ได้หรือไม่ เช่น อนุญาตให้ใช้คำสั่ง show configuration ไม่ให้ใช้คำสั่ง show running-config เป็นต้น
- สามารถกำหนด Account Expire ได้ เช่นหมดอายุตั้งแต่วันที่ 10 ธันวาคม 2544 ทำให้ผู้ใช้ไม่สามารถใช้งานได้หลังจากวันที่ดังกล่าว เป็นต้น
- สามารถกำหนดข้อจำกัดการใช้งานตามวันและเวลาได้ เช่นไม่อนุญาตให้ใช้งานวันเสาร์ เวลา 13.00 น. และเวลา 20.00 น. เวลาอื่นอนุญาตให้ใช้งานได้เป็นต้น
- สามารถกำหนดจำนวนครั้งในการเข้ามาใช้บริการต่อวันได้
- สามารถกำหนดจำนวนเวลาเข้ามาใช้บริการต่อเดือนได้
- สามารถกำหนดข้อจำกัดการใช้งานตาม NAS แต่ละตัวได้ เช่น อนุญาตให้ใช้งานที่ NAS – (c2511) ได้ ตัวอื่นไม่อนุญาต เป็นต้น
- การส่งข้อมูลผ่านเครือข่ายมีความปลอดภัยมากขึ้น เพราะมีการ encrypt ข้อมูลที่ส่งและรับทั้ง packet body ตามมาตรฐานของ TACACS+ Protocol

6.2 ข้อเสนอแนะ

เนื่องจากระบบยังคงมีข้อจำกัด ด้านการจัดการ Secret Key คือระบบจะใช้ Secret Key เพียง Key เดียวกับ NAS ทุกตัว ดังนั้นถ้า NAS ทุกตัวอยู่ภายใต้ผู้ดูแลระบบเครือข่ายเดียวกันก็ไม่น่ามีปัญหา แต่กรณีที่ NAS แต่ละตัวมีผู้ดูแลคนละคนกัน หรือต้องการให้เพิ่มระดับการรักษาความปลอดภัยให้มากขึ้นก็ควรพัฒนาระบบจัดการ Secret Key เพิ่มขึ้น ให้สามารถใช้ Secret Key ของแต่ละ NAS ได้ และถ้าจะให้สมบูรณ์ยิ่งขึ้นระบบควรติดต่อกับ Protocol อื่น ๆ ได้เช่น RADIUS Protocol

บรรณานุกรม

สมภพ วชิรลาภไพฑูรย์ 2543. "การพัฒนาโปรแกรมควบคุม TACACS+ Server ผ่าน Web," คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

Carrel and Grant 1996. "The TACACS+ Protocol Version 1.76," IETF Internet Draft, Internet Engineering Task Force.

Chander Dhawan 1998. "Remote Access Network," McGraw-Hill.

Cisco System Inc. 1999. "TACACS+ and RADIUS Comparison," [Online]. Available http://www.cisco .com/warp/customer/480/10.html

Cisco System Inc. 1999. "CiscoSecure Global Roaming Server," [Online]. Available http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_grs/

Rigney et. al. 1997. "Remote Authentication Dial In User Service (RADIUS)," Request for Comments: 2138, Livington Incorporation.

ภาคผนวก

การติดตั้งระบบ

1. **ติดตั้ง Linux Redhat 6.1 Thai**
2. **ติดตั้ง Apache**

หากไม่มีสามารถ download ได้ที่ http://www.apache.org/dist เมื่อทำการ download มาแล้วให้ทำการติดตั้ง โดยใช้คำสั่งดังนี้

tar -zvxf apache_x.tar.gz (x = version ที่ download มา)

cd apache_x

./configure --sysconfdir=/etc/httpd --datadir=/home/httpd --logfiledir=/var/log/httpd

enable-module=most --enable-shared=max --disable-rule=WANTHSREGEX

make

make install (ควร login เป็น root หรือใช้คำสั่ง su เพื่อเป็น root)

คำสั่งข้างบนเป็นการบอกให้ Apache เก็บไฟล์ Config ไว้ที่ /etc/httpd และกำหนดไฟล์ข้อมูล (HTML, CGI_BIN) ไว้ที่ /home/httpd และ ให้ Enable เพื่อสนับสนุน DSO ซึ่งจะช่วยให้สามารถเพิ่มและลบ Module ออกจาก Apache ได้โดยไม่ต้องทำการ config ใหม่

3. **ติดตั้ง PHP**

หากไม่มีสามารถ download ได้ที่ http://www.php.net/downloads.php เมื่อทำการ download มาแล้วให้ทำการติดตั้ง โดยใช้คำสั่งดังนี้

tar -zvxf php-x.tar.gz (x = version ที่ download มา)

cd php-x

./configure --with-apxs=/usr/local/apache/bin/apxs --with-config-file-path=/etc/httpd --with-mysql= --with-system-regex

make

make install (ควร login เป็น root หรือใช้คำสั่ง su เพื่อเป็น root)

4. ติดตั้ง MySQL

หากไม่มีสามารถ download ได้ที่ http://www.mysql.com/downloads เมื่อทำการ download มาแล้วให้ทำการติดตั้ง โดยใช้คำสั่งดังนี้

คัดลอกไฟล์มาไว้ที่ /usr/local

tar -zvxf mysql-x.tar.gz (x = version ที่ download มา)

cd mysql-x

ln -s mysql-x mysql (เปลี่ยนชื่อจาก mysql-x เป็น mysql เพื่อความง่ายในการเรียก)

5. กำหนดการ Startup แบบ Automatic ของ Apache และ MySQL

กำหนดข้อความดังต่อไปนี้ไว้ที่ไฟล์ /etc/rc.d/rc.local

#Start Apache

/usr/local/apache/bin/apachectl start #Start Apache

#Start MySQL

/usr/local/mysql/support-files/mysql.server start (Start MySQL)

6. การติดตั้งโปรแกรมและกำหนดค่าเริ่มต้น (Installation and Configuration)

- คัดลอกโปรแกรม tac_plus.gz ไว้ใน directory ที่ต้องการ (อาจไว้ใน /usr/local/bin)

  #tar –xvf tac_plus.gz
- ติดตั้ง AAA Deamon ดังนี้

  #tac_plus –C tac_plus.conf
- ในกรณีที่ต้องการติดตั้งแบบอัตโนมัติเมื่อเริ่มเปิดเครื่องให้เพิ่มคำสั่งดังกล่าวไว้ที่ไฟล์ /etc/rc.d/rc.local

7. ตัวอย่างการกำหนดค่าระบบ

- การกำหนดค่าโปรแกรม AAA Deamon โดยกำหนดค่าไว้ที่ไฟล์ tac_plus.conf ดังนี้

  key="111"
- แสดงการกำหนดค่าของ Router โดยใช้คำสั่ง show configuration ดังนี้

  rinknet#show configuration

  Using 3069 out of 32762 bytes

  !

```
version 12.1
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname rinknet
!
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authentication ppp default if-needed group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa authorization commands 1 default group tacacs+ if-authenticated none
aaa authorization commands 15 default group tacacs+ if-authenticated local
aaa authorization network default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
enable password 7 045E05150A335A4B1B
!
username admin password 7 050A0F1B
username local-username password 7 12150A14130741142B38373F3C2726
!
!
!
clock timezone Thailand 12 58
ip subnet-zero
```

```
no ip finger
ip domain-name rink.ac.th
ip name-server 202.29.48.1
!
ip dhcp pool local
  network 10.0.0.0 255.0.0.0
  default-router 10.0.0.1
  domain-name rink.ac.th
  dns-server 202.29.48.1 202.29.48.2
  lease 0 2
!
async-bootp dns-server 202.29.48.1
!
!
!
interface Ethernet0
 ip address 10.0.0.1 255.0.0.0 secondary
 ip address 203.154.198.9 255.255.255.0 secondary
 ip address 202.29.48.254 255.255.255.0
 ip broadcast-address 0.0.0.0
 ip nat inside
!
interface Serial0
 ip address 202.28.29.110 255.255.255.252
 ip broadcast-address 0.0.0.0
 ip nat outside
!
interface Serial1
 no ip address
 shutdown
```

```
 no cdp enable
!
interface Group-Async1
 ip unnumbered Ethernet0
 encapsulation ppp
 ip tcp header-compression passive
 no ip mroute-cache
 async mode interactive
 peer default ip address pool dialup
 no fair-queue
 no cdp enable
 ppp authentication pap
 group-range 1 16
!
ip local pool dialup 202.29.48.237 202.29.48.253
ip nat pool rinknet 202.29.48.150 202.29.48.236 netmask 255.255.255.0
ip nat inside source list 1 pool rinknet overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
ip route 203.154.198.0 255.255.255.0 Ethernet0
no ip http server
!
access-list 1 permit 10.0.0.0 0.255.255.255
tacacs-server host 202.29.48.20 port 49
tacacs-server key 111
snmp-server community public RO
snmp-server community read RO
snmp-server community wite RW
radius-server host 202.29.48.6 auth-port 1645 acct-port 1646
radius-server retransmit 3
```

```
radius-server key RinkNet
!
line con 0
 transport input none
line 1
 autoselect during-login
 autoselect ppp
 modem InOut
 modem autoconfigure type usr_sportster
 autocommand  ppp
 transport input all
 escape-character BREAK
 speed 115200
 flowcontrol hardware
line 2 16
 autoselect during-login
 autoselect ppp
 modem InOut
 modem autoconfigure type hayes_optima
 autocommand  ppp
 transport input all
 escape-character BREAK
 autoselect ppp
 modem InOut
 modem autoconfigure type usr_sportster
 autocommand  ppp
 transport input all
 escape-character BREAK
 speed 115200
 flowcontrol hardware
```

```
line 2 16
 autoselect during-login
 autoselect ppp
 modem InOut
 modem autoconfigure type hayes_optima
 autocommand  ppp
 transport input all
 escape-character BREAK
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
 password 7 01120F10
!
end
```

ประวัติผู้เขียน

ชื่อ-สกุล	นายนฤพนธ์ พนาวงศ์
สถานที่เกิด	นครราชสีมา
ประวัติการศึกษา	วท.บ. (วิทยาการคอมพิวเตอร์)
	สถาบันราชภัฏนครราชสีมา
ประวัติการทำงาน	บริษัทซอฟต์สแควร์ 1999 จำกัด
	สถาบันราชภัฏนครสวรรค์