การพัฒนาระบบควบคุม TACACS+ Server ผ่าน Web

TACACS+ Server Management System via Web

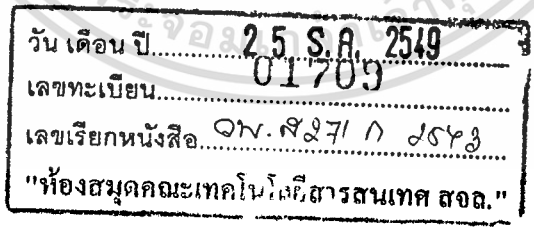
โดย

นายสมภพ วชิรลาภไพฑูรย์

รหัส 41067131

อาจารย์ที่ปรึกษา

อาจารย์ อัครินทร์ คุณกิตติ



รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคการเรียนที่ 1 ปีการศึกษา 2543

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	การพัฒนาระบบควบคุม TACACS+ Server ผ่าน Web
นักศึกษา	นายสมภพ วชิรลาภไพฑูรย์
อาจารย์ที่ปรึกษา	อาจารย์อัครินทร์ คุณกิตติ
ระดับการศึกษา	วิทยาศาสตร์มหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2543

บทคัดย่อ

ในปัจจุบันความต้องการใช้ระบบเครือข่าย เพิ่มขึ้นอย่างรวดเร็ว ทำให้จำนวนอุปกรณ์เครือข่ายมีจำนวนเพิ่มมากขึ้นด้วย จึงมีความจำเป็นในการรวมศูนย์การทำงานด้านความปลอดภัย เพื่อให้มีประสิทธิภาพมากที่สุด โดยใช้หลักการ AAA (Authentication, Authorization และ Accounting) จากผลการศึกษาระบบที่ใช้งานในปัจจุบัน คือ RADIUS Daemon และ TACACS+ Freeware Daemon มี User Interface ที่ใช้งานยาก, ไม่สามารถควบคุม Enable Password ได้ และเก็บข้อมูลใน log file ซึ่งทำให้ยากต่อการจัดการข้อมูลต่างๆ

ดังนั้น โครงการพัฒนาระบบงานนี้จึงนำ TACACS+ Freeware Daemon version 2.1 มาปรับปรุงเพื่อให้สามารถค้นหาข้อมูลผู้ใช้ในฐานข้อมูล, เพิ่มความสามารถด้านการติดต่อผู้บริหารระบบเครือข่ายให้ง่ายขึ้น โดยผ่าน Web Browser และเก็บข้อมูลลงในฐานข้อมูลแทน Log File เพื่อประสิทธิภาพในการจัดการข้อมูล มีหลักการทำงานดังนี้ ผู้ใช้บริการจะติดต่อกับอุปกรณ์เครือข่ายเพื่อขอใช้บริการ อุปกรณ์เครือข่ายจะทำการส่ง AAA packet มายังระบบ ระบบจะทำการตรวจสอบโดยเปรียบเทียบกับข้อมูลที่อยู่ในฐานข้อมูล จากนั้นจะทำการบันทึกข้อมูลในฐานข้อมูล และส่ง AAA packet ตอบกลับไปที่อุปกรณ์เครือข่ายว่า ผ่านหรือไม่ผ่าน อุปกรณ์เครือข่ายจะนำผลที่ได้รับไปปฏิบัติกับผู้ใช้ เช่น อนุญาตให้ใช้บริการ PPP ได้ ผู้บริหารเครือข่ายสามารถเรียกดูหรือแก้ไขข้อมูลต่างๆ โดยใช้ Web Browser ซึ่ง Web Server จะทำการติดต่อกับ Database Server อีกต่อหนึ่ง

Title	TACACS+ Server Management System via Web
Student	Mr.Sompop Wachiralarppaitoon
Advisor	Mr.Akharin Khunkitti
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	2000

ABSTRACT

Now, the demand of computer network service is increase rapidly. So the number of Network Access Server (NAS) is increased. It need centralize security management for more efficiency. We use concept of authentication, authorization and accounting. We implement by using AAA protocol. Now system that we use is RADIUS Daemon and TACACS+ freeware daemon which user interface is not user friendly, can't control enable password per NAS and store accounting information in log file which hard to manage the accounting information.

There for this system development project will improve TACACS+ freeware daemon version 2.1 to connect to database server and create new user interface (Web User Interface) for administrator to manage user and NAS configuration. And store user configuration and accounting information in database for more efficiency in manage information. User will request service from NAS. NAS will send AAA packet to system for verify that user and service. System will verify user with information in database. The system will record the result and send AAA packet back to the NAS (pass/fail). NAS will bring the result to process. For example system permit that user to use PPP service. The Network Administrator can manage system's information via web browser and web server will connect to database server.

กิตติกรรมประกาศ

โครงการพัฒนาระบบงานนี้สำเร็จได้เพราะได้รับการส่งเสริม และสนับสนุนจากบุคคลหลายท่าน กระผมจึงใคร่ขอกราบขอบพระคุณ

- บิดาและมารดา ที่ได้อบรมสั่งสอนและสนับสนุนส่งเสียให้ได้เล่าเรียนจบประสบความสำเร็จในการศึกษา
- อาจารย์อัครินทร์ คุณกิตติ ที่ได้ให้ความกรุณาให้คำปรึกษาแนะนำสิ่งต่างๆ ในโครงการพัฒนาระบบงาน
- อาจารย์ทุกๆ ท่านที่ได้ประสิทธิ์ประสาทความรู้ หลักวิชาการต่างๆ เพื่อเป็นพื้นฐานในการดำเนินชีวิตและการทำงาน
- เจ้าหน้าที่คณะเทคโนโลยีสารสนเทศทุกท่านที่ให้ความอำนวยความสะดวก
- สุดท้ายคือ เพื่อนๆ IS6 สมทบ ทุกท่านที่ได้กำลังใจ และให้คำแนะนำดีๆ เสมอมา

นายสมภพ วชิรลาภไพฑูรย์

สารบัญ

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญรูปภาพ

หน้า

ภาพที่

บทที่ 1
บทนำ

1.1 ความเป็นมา

ในปัจจุบันการติดต่อสื่อสาร ได้รับความนิยมอย่างมาก ทำให้ระบบเครือข่ายต้องเพิ่มความจุให้มากขึ้น ทำให้จำนวนอุปกรณ์เครือข่าย (Network Access Server) มากขึ้นตามปริมาณผู้ใช้ทำให้เกิดปัญหาใหม่คือ ทำอย่างไรจึงจะสามารถควบคุมการเข้าออกของผู้ใช้บริการแต่ละคนได้ ตามที่ต้องการ

เราต้องการศูนย์กลางการควบคุมผู้ใช้รวมถึงรหัสผ่าน เพราะถ้ามีการเปลี่ยนแปลงรายชื่อผู้ใช้เพียง 1 คนจะต้องแก้ไข configuration ของ NAS ทุกตัว (10, 30 หรือมากกว่านั้น) เราต้องการทราบว่าผู้ใช้แต่ละคนทำอะไรบ้าง เราอาจจะต้องการอนุญาตให้ผู้ใช้สามารถใช้อะไรได้หรือไม่อนุญาตให้ใช้อะไร หรือรวมถึงเวลาในการใช้งาน

ในระบบเครือข่ายขนาดใหญ่ การเข้มงวดในการรักษาความปลอดภัยมีความสำคัญมาก ผู้ดูแลระบบจะต้องป้องกันระบบเครือข่ายและทรัพยากรของเครือข่ายจากผู้ที่ไม่มีสิทธิ์ใช้ โดยมีหลักการดังนี้ Authentication, Authorization, Accounting หรือ AAA

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

1.3 ขอบเขตของการพัฒนาระบบงาน

- ข้อมูลเกี่ยวกับผู้ใช้จะต้องเก็บอยู่ในฐานข้อมูล
- ระบบสามารถควบคุม Enable Password ของ NAS ได้
- บริการที่ผู้ใช้สามารถใช้ได้มีดังนี้ Shell (EXEC) หรือ PPP
- ผู้ใช้บริการมี password เพียงค่าเดียวใช้กับทุกบริการ เช่น Shell (EXEC) หรือ PPP
- ระบบสามารถควบคุมการใช้งานคำสั่งต่างๆ ของผู้ใช้ได้
- ระบบติดต่อผู้บริหารระบบเครือข่ายผ่าน Web Browse
- ระบบสามารถสืบค้นข้อมูลการใช้งานของผู้ใช้ย้อยหลังได้
- ระบบมี Secret Key เพียงค่าเดียว ใช้กับ NAS ทุกตัว

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 : Solaris 2.7 for x86
- Web Server : Apache 1.3.12
- DBMS : MySQL 3.22.32
- Web Browser : Internet Explorer 5.00
- Tool : PHP 3.0.16 with MySQL Client API , C API for MySQL

บทที่ 2

AAA Protocol

2.1 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 ซึ่งสามารถทำการแก้ไขเพื่อใช้งานกับระบบรักษาความปลอดภัยในปัจจุบัน ที่มีอยู่ในตลาดได้ RADIUS

2.1.1 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 ตัวอื่นได้ หรือเป็น Authentication เพื่อจุดประสงค์อื่นๆ

- Network Security

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

- วิธี Authentication ที่ยืดหยุ่น

  RADIUS Server สนับสนุนวิธี Authentication นอกเหนือจากวิธีพื้นฐาน ได้แก่ PPP, PAP หรือ CHAP , UNIX login และอื่นๆ

- สามารถเพิ่มขยายได้

ข้อมูลที่รับส่งนั้น ประกอบไปด้วยตัวแปรต่างๆ ซึ่งสามารถเพิ่มเติมได้โดยไม่รบกวนการพัฒนา protocol

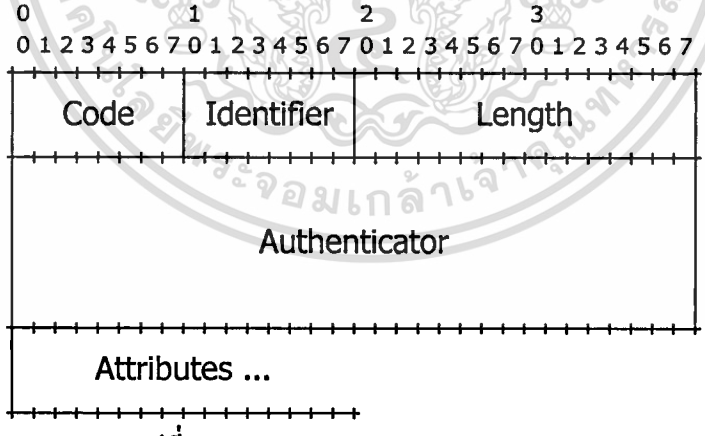
2.1.2 นิยาม

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

NAS (Network Access Server) คืออุปกรณ์ใดๆที่ให้บริการติดต่อกับผู้ใช้ (Access Service) ปัจจุบัน NAS ทำหน้าที่มากกว่าเพียงแค่ Terminal Server ซึ่งให้บริการ character mode front end โดยจะอนุญาตให้ผู้ใช้ telnet หรือ rlogin ไปยัง host อื่นๆ NAS อาจจะสนับสนุน protocol หลายตัวเช่น PPP, ARAP, LAT, XREMOTE และอื่นๆ

2.1.3 Packet Format

RADIUS ส่ง packet แบบ UDP port 1812 มีรูปแบบดังนี้



รูปที่ 2.1 แสดง RADIUS data format

Code - กำหนดชนิดของ RADIUS packet มีขนาด 8 bits

1 Access-Request

2 Access-Accept

3 Access-Reject

4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

Identifier - กำหนดว่าเป็น Request และ Reply packet เดียวกัน

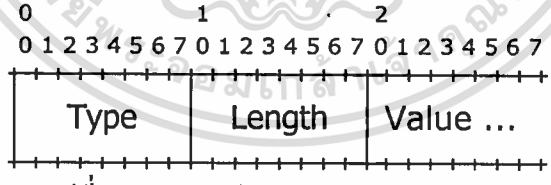
Length - กำหนดความยาวของ packet รวมทั้ง Code, Identifier, Length และ Attribute field ถ้า packet ที่มีความยาวสั้นกว่าที่ค่า Length field ให้เพิกเฉย packet นั้น ความยามที่น้อยที่สุดคือ 20 ความยาวมากที่สุด คือ 4096

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

Attribute - กำหนดค่าของ Attribute ต่างๆ

2.1.4 Attrubites

RADIUS Attribute แสดงถึงข้อมูลที่ใช้ในการ Authentication, Authorization และ Accounting มีรูปแบบดังนี้



รูปที่ 2.2 แสดงรูปแบบของ Attributes

RADIUS Client / Server จะเพิกเฉยต่อ Attribute ที่มี type ไม่มีในรายชื่อต่อไปนี้

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
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	Vendor-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	reserved for accounting)
60	CHAP-Challenge
61	AS-Port-Type
62	Port-Limit
63	Login-LAT-Port

2.1.5 การทำงาน

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 ได้รับข้อมูลแล้ว จะทำการสร้าง 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 จะทำการตรวจสอบกรณีที่ Access Request มาจาก client ที่ RADIUS server ไม่มี shared secret อยู่ Request นั้นจะถูกเพิกเฉย ส่วนกรณีที่ RADIUS server มี shared secret ของ client นั้นๆ 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 พร้อมส่งข้อมูลจากผู้ใช้และ สถานะของ attribute จาก Access-Challenge ซึ่งจะมีค่า 0 หรือ 1 เท่านั้น จากนั้น server สามารถตอบรับ Access-Request ใหม่นี้ โดยการส่ง Access-Accept, Access-Reject หรือ Access-Challenge อื่นๆ

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

2.2 TACACS+ protocol

TACACS+ คือ TACACS (Terminal Access Controller Access Control System) ที่ถูกพัฒนาต่อมาล่าสุด TACACS คือ protocol ที่ใช้ควบคุมการเข้าถึงทรัพยากร ที่ใช้ UDP อย่างง่ายๆ 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

2.2.1 ลักษณะเด่น

- TACACS+ แบ่งแยกการทำงาน AAA ออกจากกัน
- TACACS+ สนับสนุน การตรวจสอบสิทธิในการใช้คำสั่งของ router
- TACACS+ สนับสนุน privilege level ถึง 16 ระดับ (0-15)

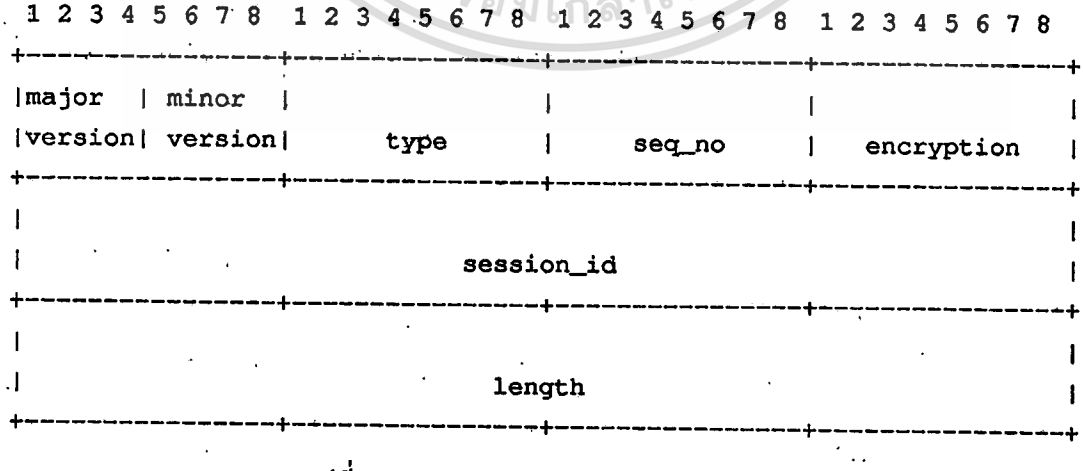
- TACACS+ สนับสนุน การควบคุมบริการต่างๆ เช่น Point-to-Point Protocol (PPP), shell standard login, enable privilege, AppleTalk Remote Access (ARA) protocol, Novell Asynchronous Service Inerface (NASI), remote command (RCMD) และ firewall proxy
- TACACS+ สนับสนุน การจำกัด port ในการให้บริการ เช่น TTY, VTY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

2.2.2 นิยาม

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

NAS (Network Access Server) คืออุปกรณ์ใดๆที่ให้บริการติดต่อกับผู้ใช้ (Access Service) ปัจจุบัน NAS ทำหน้าที่มากกว่าเพียงแค่ Terminal Server ซึ่งให้บริการ character mode front end โดยจะอนุญาตให้ผู้ใช้ telnet หรือ rlogin ไปยัง host อื่นๆ NAS อาจจะสนับสนุน protocol หลายตัวเช่น PPP, ARAP, LAT, XREMOTE และอื่นๆ

2.2.3 TACACS+ packet header



รูปที่ 2.3 แสดง TACACS+ packet header

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

2.2.4 TACACS+ packet body

ประเภทของ TACACS+ packet body กำหนดจาก header โดยมีกฎเกณฑ์ดังนี้

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

2.2.4.1 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

2.2.5 ประเภทของ packet body

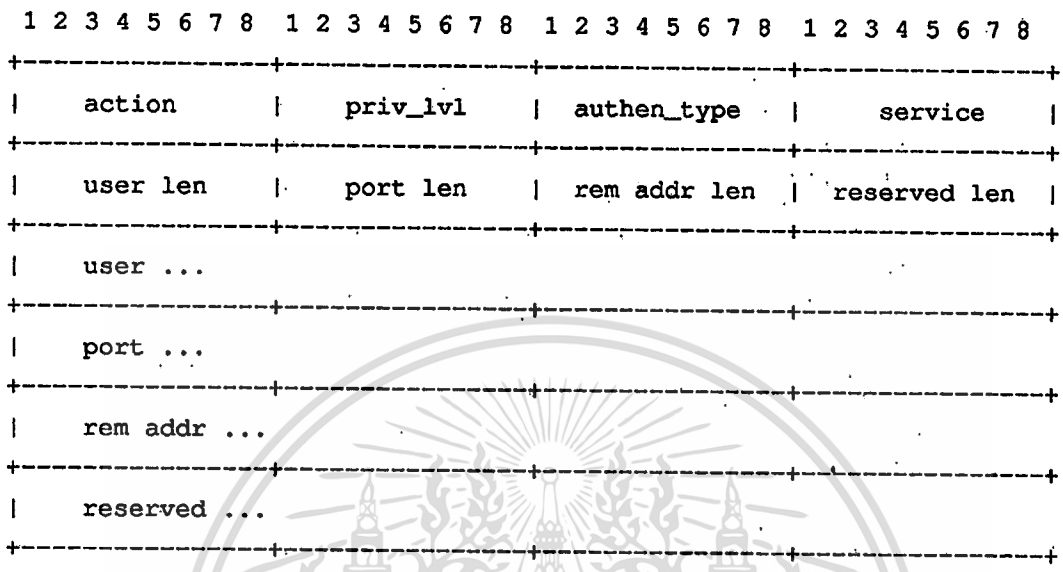
packet body จะต้องถูกถอดรหัสก่อนนำมาใช้

2.2.5.1 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

START packet body ประกอบไปด้วย



รูปที่ 2.4 แสดงรูปแบบของ AUTH START packet body

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 (สิทธิสูงสุดที่อนุญาติ)

: 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

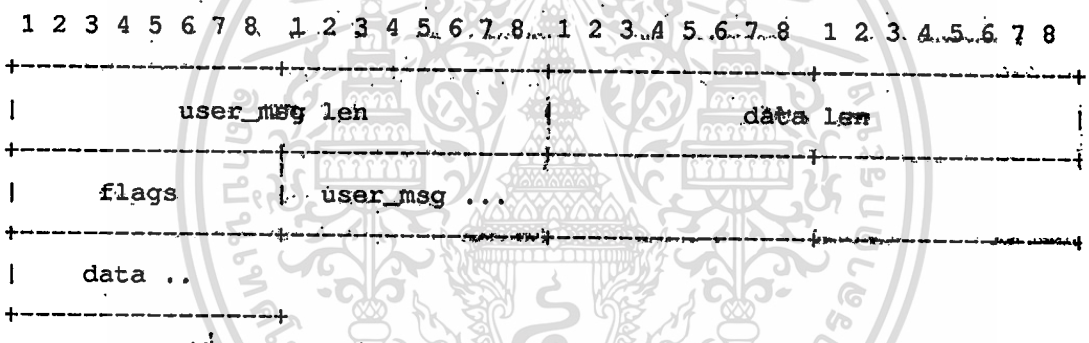
9. user (user len bytes) คือ ชื่อผู้ใช้

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

CONTINUE packet body ประกอบไปด้วย



รูปที่ 2.5 แสดงรูปแบบของ AUTHEN CONTINUE packet body

1. user_msg len (2 bytes) คือ จำนวนตัวอักษรของข้อมูลของผู้ใช้

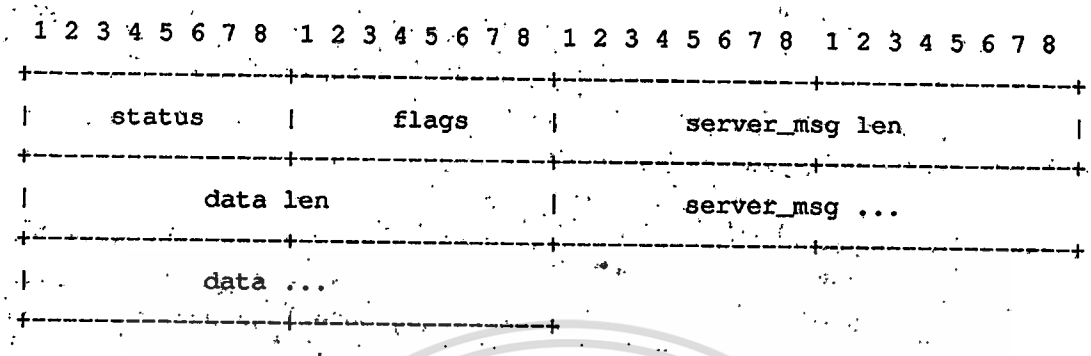
2. data len (2 bytes) คือ จำนวนตัวอักษรของข้อมูลของผู้ใช้

3. flags (1 byte) : 0x01 คือ ยกเลิก

4. user_msg (user_msg len bytes) คือ ข้อมูลของผู้ใช้

5. data (data len bytes) คือ ข้อมูลของเครื่องผู้ใช้

REPLY packet body ประกอบไปด้วย



รูปที่ 2.6 แสดง AUTHEN REPLY packet body

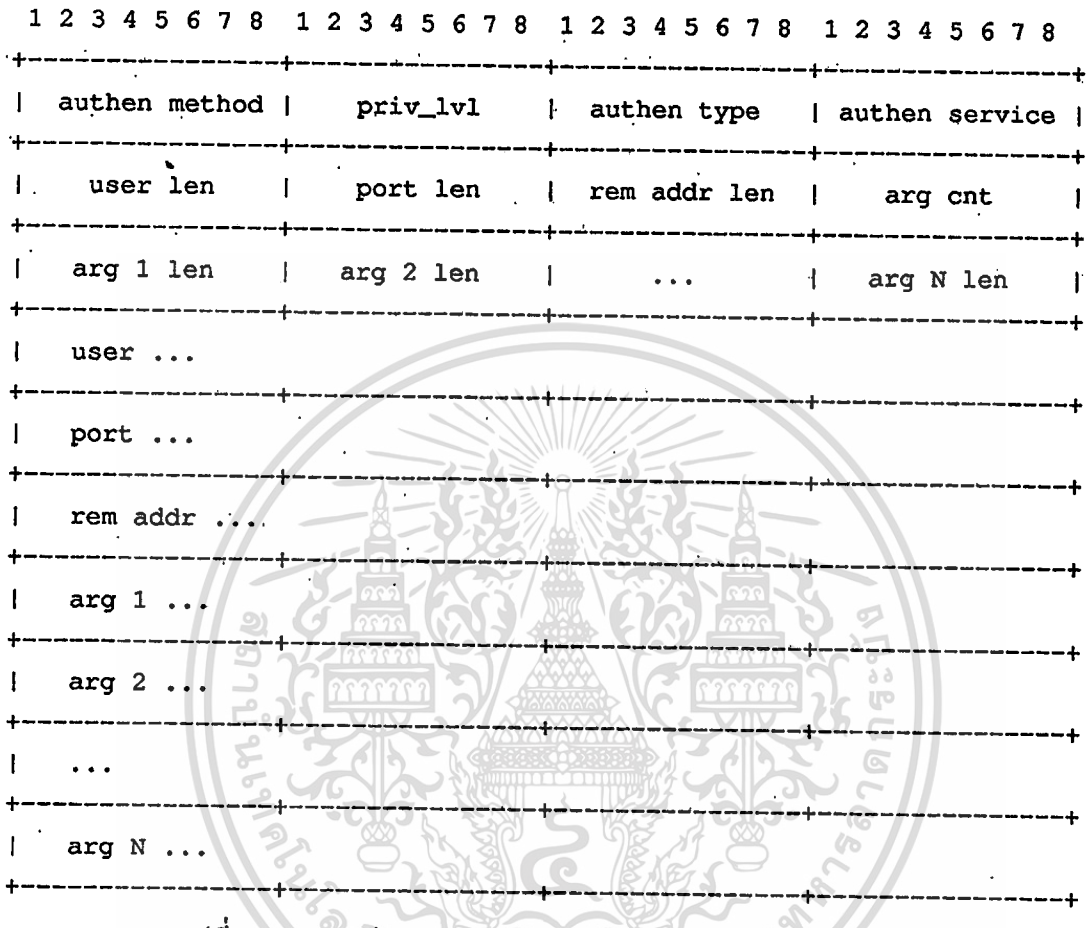
1. status (1 byte) คือ สถานะของการตรวจสอบสิทธิในการเข้าถึง
   : 0x01 คือ PASS (ผ่านการ Authentication)
   : 0x02 คือ FAIL (ไม่ผ่านการ Authentication)
   : 0x03 คือ GETDATA (รับข้อมูลเพิ่ม)
   : 0x04 คือ GETUSER (รับชื่อผู้ใช้)
   : 0x05 คือ GETPASS (รับรหัสผ่าน)
2. flags (1 byte) : 0x01 คือ คือจะไม่แสดงสิ่งที่ผู้ใช้พิมพ์ให้เป็น
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

2.2.5.2 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

REQUEST packet body ประกอบไปด้วย



รูปที่ 2.7 แสดงรูปแบบของ AUTHOR REQUEST packet body

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

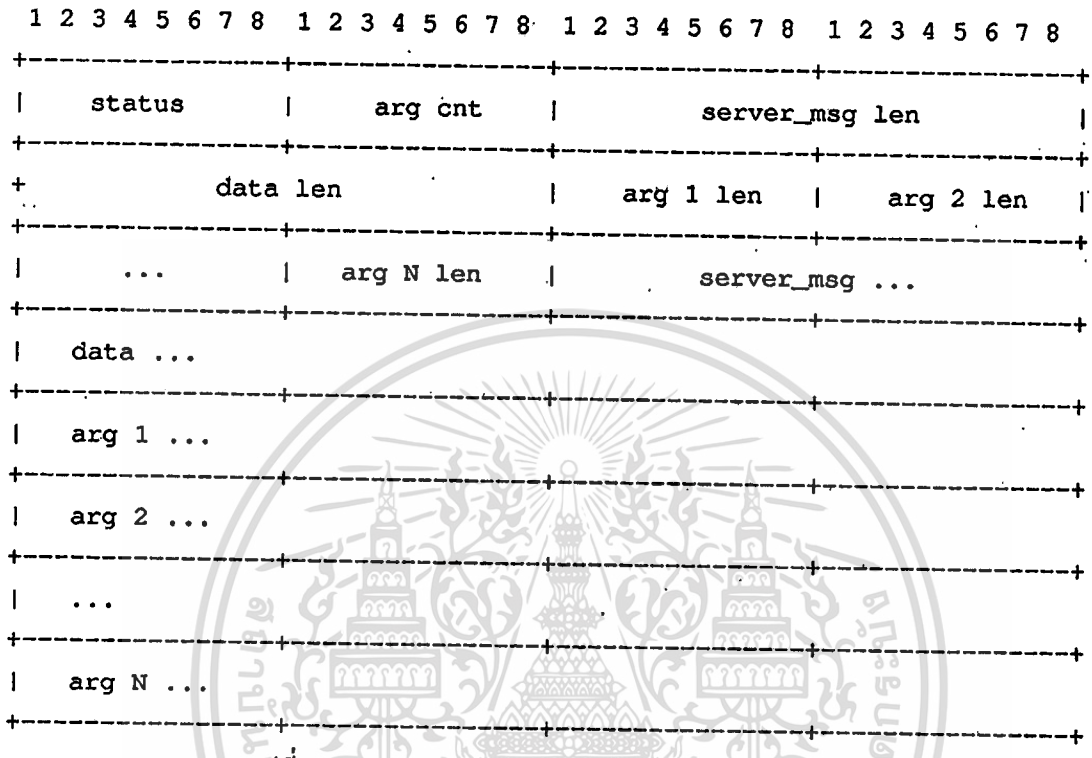
: routing คือ กำหนดข้อมูลการหาเส้นทางการส่งข้อมูล

: route คือ กำหนดเส้นทางที่ใช้ในการส่งข้อมูล

: idletime คือ idle-timeout สำหรับ connection (นาที)

: autocmd คือ การกำหนดคำสั่งที่จะทำงานโดยอัตโนมัติ

RESPONSE packet body ประกอบไปด้วย



รูปที่ 2.8 แสดง AUTHOR RESPONSE packet body

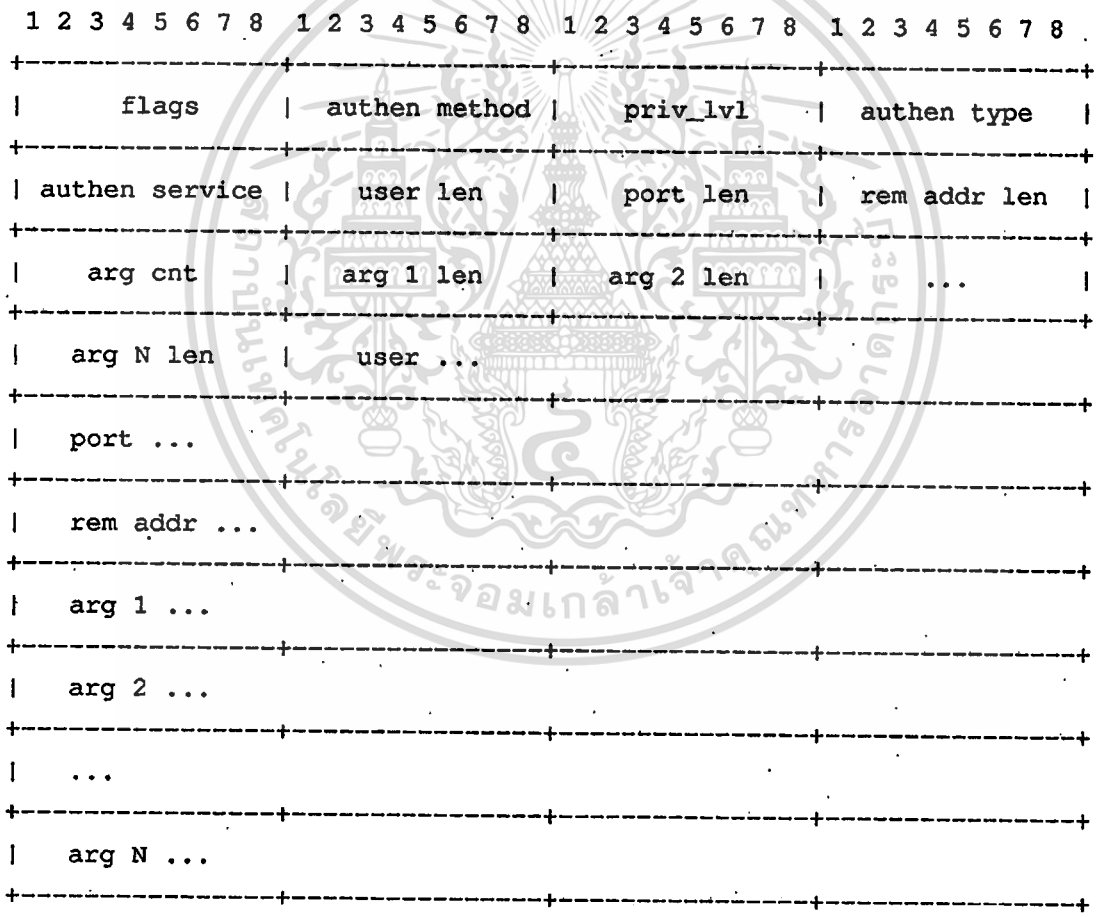
1. status (1 byte) คือสถานะของการ Authorization
   : 0x01 คือ PASS_ADD (อนุญาตให้ใช้ได้โดยเพิ่ม arg)
   : 0x02 คือ PASS_REPL (อนุญาตให้ใช้ได้โดยแทน arg)
   : 0x03 คือ ไม่อนุญาตให้ใช้งาน
2. arg cnt (1 byte) คือ จำนวน argument
3. server_msg len (2 bytes) คือ ความยาวข้อความของ Server
4. data len (2 bytes) 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

2.2.5.3 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

REQUEST packet body ประกอบไปด้วย



รูปที่ 2.9 แสดงรูปแบบของ ACCT REQUEST packet body

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 วิธีการตรวจสอบสิทธิในการเข้าถึง รายละเอียดเหมือนการตรวจสอบสิทธิในการเข้าถึง

3. priv_lvl (1 byte) คือ ระดับของสิทธิของผู้ใช้ (privilege) รายละเอียดเหมือนการตรวจสอบสิทธิในการเข้าถึง

4. authen type (1 byte) คือ ชนิดของการตรวจสอบสิทธิในการเข้าถึง รายละเอียดเหมือนการตรวจสอบสิทธิในการเข้าถึง

5. authen service (1 byte) คือ บริการของการตรวจสอบสิทธิในการเข้าถึง รายละเอียดเหมือนการตรวจสอบสิทธิในการเข้าถึง

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

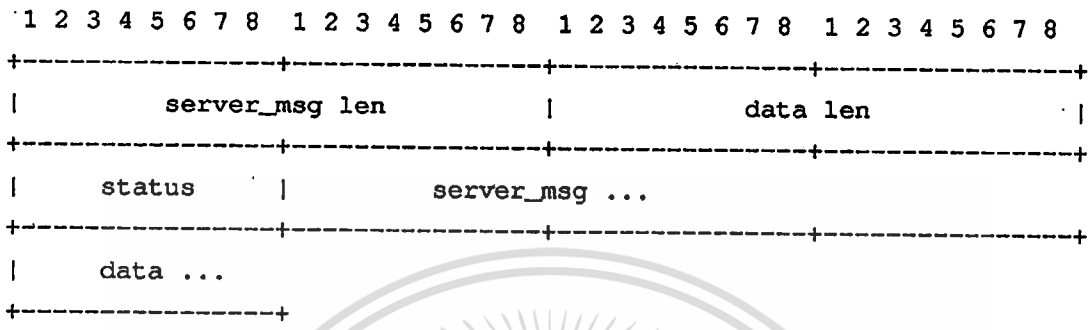
: start_time คือ เวลาเริ่มเป็นจำนวนวินาทีนับจาก 12:00 AM Jan 1, 1970

: timezone คือ เขตเวลา

: service คือ บริการที่ใช้

: elapsed_time คือ จำนวนวินาทีที่ใช้

REPLY packet body ประกอบไปด้วย



รูปที่ 2.10 แสดง ACCT REPLY packet body

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

2.2.6 การทำงาน

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 พิจารณา username, 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

2.3 เปรียบเทียบ TACACS+ protocol กับ RADIUS protocol

2.3.1 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

2.3.2 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

2.3.3 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 อื่นๆได้ เช่น 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

2.3.4 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

2.3.5 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

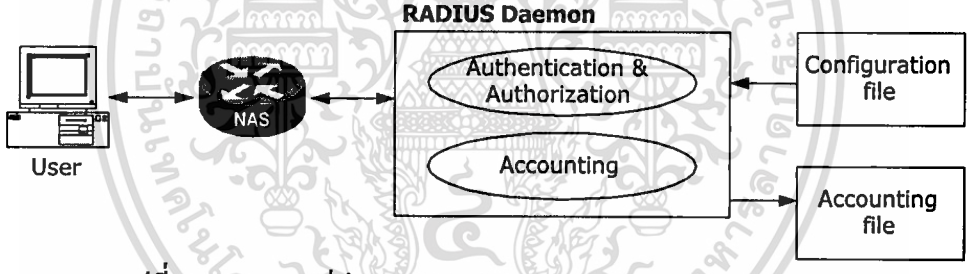
บทที่ 3

ผลการศึกษาระบบงานเดิม

3.1 ระบบ RADIUS Daemon

3.1.1 องค์ประกอบ

- RADIUS Daemon
- NAS (Network Access Server)
- ผู้ใช้บริการ
- Configuration File
- Accounting File



รูปที่ 3.1 แสดงองค์ประกอบของระบบ RADIUS Daemon

3.1.2 การทำงานของระบบ

3.1.2.1 RADIUS Daemon

- ติดต่อระหว่าง NAS โดยใช้ RADIUS protocol และ Configuration & Accounting files
- รับข้อมูลของผู้ใช้ในระบบที่ส่งมาจาก NAS และทำการตรวจสอบตรงกับข้อมูลใน Configuration file ว่าตรงกันหรือเปล่า
- ส่งผลการตรวจสอบที่ได้ กลับไปที่ NAS
- รับข้อมูล Accounting ที่ส่งมาจาก NAS และทำการเก็บข้อมูลนั้นไว้ใน Accounting file

3.1.2.2 NAS (Network Access Server)

- ติดต่อระหว่างผู้ใช้บริการ และ RADIUS Daemon
- รับข้อมูลจากผู้ใช้บริการ แล้วส่งต่อให้ RADIUS Daemon เพื่อ Authentication & Authorization
- นำผลการ Authentication & Authorization ที่ได้จาก NAS มาปฏิบัติ เช่นอนุญาตให้ใช้ Shell ได้ หรือ ไม่อนุญาตให้ใช้
- ส่งข้อมูล Accounting ให้กับ RADIUS Daemon เพื่อบันทึกไว้

3.1.2.3 ผู้ใช้บริการ

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

3.1.2.4 Configuration file

- ติดต่อกับ RADIUS Daemon
- เก็บข้อมูล Configuration ของ RADIUS Daemon ประกอบด้วย ข้อมูลที่ใช้ในการ Authentication, Authorization, Accounting, shared secret key ที่ใช้ encrypt user's password ระหว่างการส่งข้อมูลระหว่าง NAS กับ RADIUS Daemon

3.1.2.5 Accounting file

- ติดต่อกับ RADIUS Daemon
- เก็บข้อมูล Accounting ประกอบไปด้วย ข้อมูลผู้ใช้บริการ, บริการที่ใช้, ชื่อ NAS, เวลาที่เริ่ม และหยุดใช้งาน และอื่นๆ เพื่อใช้ในการทำ billing หรือตรวจสอบภายหลัง

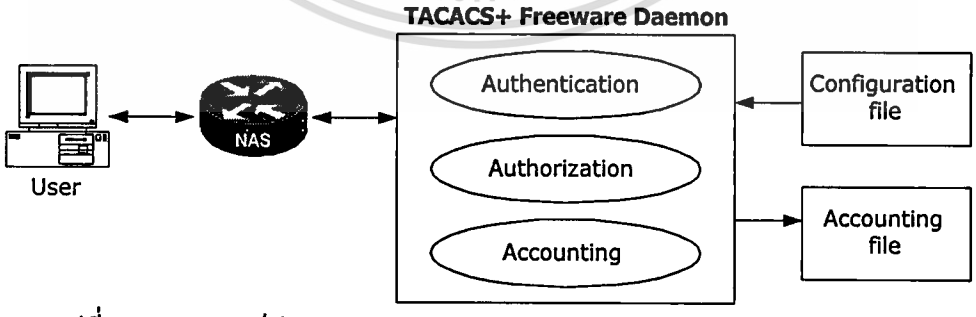
3.1.3 สรุปผลการศึกษา

- ใช้ RADIUS protocol ในการ authentication, authorization และ accounting
- Authentication และ Authorization รวมกัน
- AAA packet มีความปลอดภัยน้อย เพราะ encrypt ข้อมูลเฉพาะ password ข้อมูลอื่นๆสามารถถูกดักจับและอ่านได้
- Input หรือรับ Configuration ผ่าน config file
- Output หรือออกรายงาน ผ่าน log file
- ติดต่อกับผู้ใช้ด้วย command line
- ไม่สามารถควบคุมการใช้คำสั่งใน router ได้
- Statistic เก็บไว้ใน log file ยากต่อการค้นหา

3.2 ระบบ TACACS+ Freeware Daemon

3.2.1 องค์ประกอบ

- TACACS+ Freeware Daemon
- NAS (Network Access Server)
- ผู้ใช้
- Configuration File
- Accounting File



รูปที่ 3.2 แสดงองค์ประกอบของระบบ TACACS+ Freeware Daemon

3.2.2 การทำงานของระบบ

3.2.2.1 TACACS+ Free Daemon

- ติดต่อระหว่าง NAS โดยใช้ TACACS+ protocol และ Configuration & Accounting files
- รับข้อมูลของผู้ใช้ในระบบที่ส่งมาจาก NAS และทำการตรวจสอบตรงกับข้อมูลใน Configuration file ว่าตรงกันหรือเปล่า
- ส่งผลการตรวจสอบที่ได้ กลับไปที่ NAS
- รับข้อมูล Accounting ที่ส่งมาจาก NAS และทำการเก็บข้อมูลนั้นไว้ใน Accounting file

3.2.2.2 NAS (Network Access Server)

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

3.2.2.3 ผู้ใช้บริการ

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

3.2.2.4 Configuration file

- ติดต่อกับ RADIUS Daemon
- เก็บข้อมูล Configuration ของ TACACS+ Freeware Daemon ประกอบด้วย ข้อมูลที่ใช้ในการ Authentication, Authorization,

Accounting, shared secret key ที่ใช้ encrypt user's password ระหว่างการส่งข้อมูลระหว่าง NAS กับ RADIUS

3.2.2.5 Accounting file

- ติดต่อกับ RADIUS Daemon
- เก็บข้อมูล Accounting ประกอบไปด้วย ข้อมูลผู้ใช้บริการ, บริการที่ใช้, ชื่อ NAS, เวลาที่เริ่ม และหยุดใช้งาน และอื่นๆ เพื่อใช้ในการทำ billing หรือตรวจสอบภายหลัง

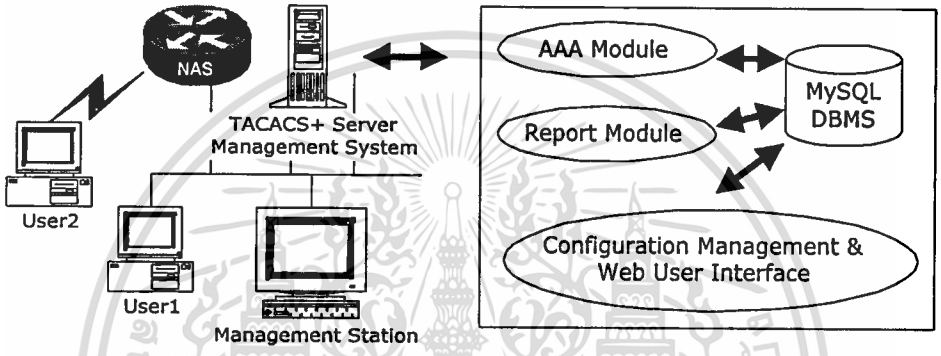
3.2.3 สรุปผลการศึกษา

- พัฒนาโดย Cisco System ให้ load ฟรี แต่ไม่มีการรับประกัน และสนับสนุนอย่างเป็นทางการ
- ใช้ TACACS+ protocol ในการ authentication, authorization และ accounting
- AAA packet มีความปลอดภัยมากขึ้นเนื่องจากถูก encrypt ทุก packet
- Input หรือรับ Configuration ผ่าน config file
- Output หรือออกรายงาน ผ่าน log file
- ติดต่อกับผู้ใช้ด้วย command line
- สามารถควบคุมการใช้คำสั่งใน router ได้
- Statistic เก็บไว้ใน log file ยากต่อการค้นหา

บทที่ 4

ระบบควบคุม TACACS+ Server ผ่าน Web

4.1 องค์ประกอบของระบบ



รูปที่ 4.1 แสดงองค์ประกอบของระบบควบคุม TACACS+ Server ผ่าน Web

องค์ประกอบของระบบควบคุม TACACS+ Server ผ่าน Web ประกอบไปด้วย

- TACACS+ Server Management System
- 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 เพื่อเก็บข้อมูลต่างๆ เช่น ข้อมูลผู้ใช้ ข้อมูลบริการที่ใช้เวลาที่ใช้งาน เป็นต้น
- **Configuration Management & Web User Interface** ทำหน้าที่ติดต่อกับผู้บริหารระบบเครือข่ายเพื่อ เพิ่ม, แก้ไข และลบ รายละเอียดทั้งหมดเกี่ยวกับผู้ใช้

- **Report Module** ทำหน้าที่แสดงรายงานต่างๆ เช่นรายชื่อผู้ใช้งานในระบบในปัจจุบัน รายงานจำนวนชั่วโมง ต่อเดือน หรือ สัปดาห์ เรียงตามบริการที่ใช้ และตามรายชื่อผู้ใช้บริการ
- **Database Module** ติดต่อกับทั้ง 3 Module เพื่อสนับสนุนข้อมูลต่างๆ ดังนี้ ข้อมูลเกี่ยวกับผู้ใช้ ข้อมูลเกี่ยวกับ NAS, ข้อมูลเกี่ยวกับบัญชี เป็นต้น

4.1.2 ผู้ใช้บริการ (USER1 & USER2)

- ติดต่อกับ NAS เพื่อขอใช้บริการเครือข่ายเช่น Shell, PPP, SLIP และอื่นๆ
- 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 เช่น อนุญาตให้ใช้ 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 เพื่อเรียกดูรายงานต่างๆ ของระบบ

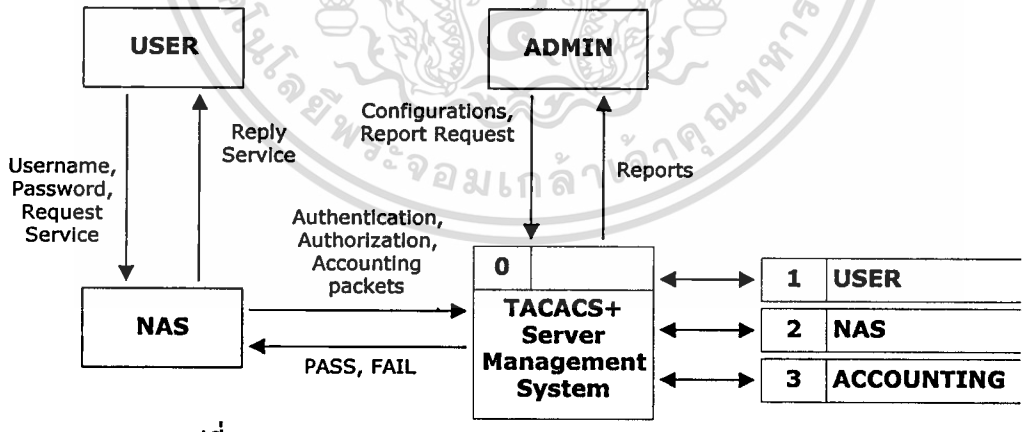
4.2 การออกแบบระบบ

4.2.1 ความต้องการของระบบ

- เก็บข้อมูลของผู้ใช้บริการได้อย่างมีประสิทธิภาพ
- ระบบสามารถควบคุม Enable Password ของ NAS ทุกตัวในระบบได้
- ระบบรองรับบริการที่อนุญาตให้ผู้ใช้สามารถใช้ได้มีดังนี้ Shell หรือ PPP
- ผู้ใช้บริการมี password เพียงค่าเดียวใช้กับทุกบริการ เช่น Shell หรือ PPP
- ระบบสามารถควบคุมการใช้งานคำสั่งต่างๆ ของผู้ใช้ได้ สำหรับ NAS ทุกตัว
- ระบบติดต่อผู้บริหารระบบเครือข่ายผ่าน Web Browser
- ระบบสามารถสืบค้นข้อมูลการใช้งานของผู้ใช้ย้อยหลังได้
- ระบบสามารถแสดงรายชื่อผู้ใช้ในปัจจุบันได้
- ระบบสามารถกำหนดข้อจำกัดของผู้ใช้แต่ละคนได้ ได้แก่วันและเวลาที่อนุญาตให้ใช้งาน NAS ที่อนุญาตหรือไม่อนุญาต

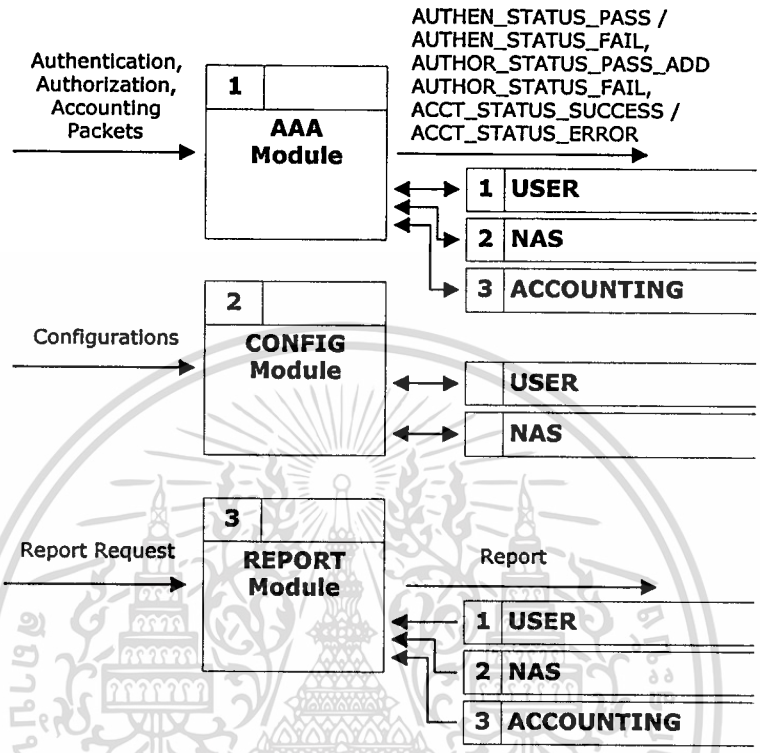
4.2.2 Process Modeling

4.2.2.1 Data Flow Diagram (Context Diagram)



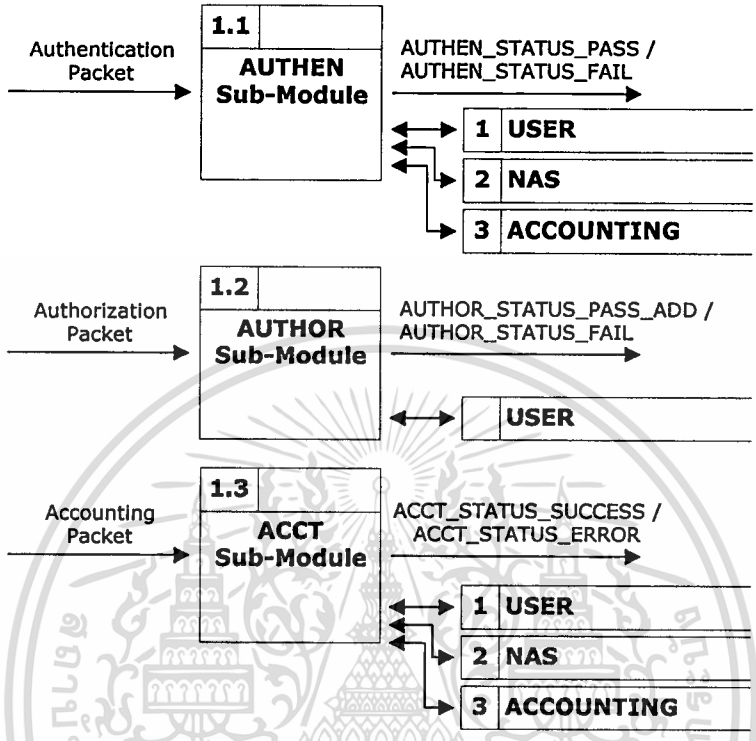
รูปที่ 4.2 แสดง Data Flow Diagram (Context Diagram)

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

Process 1 : AAA Module

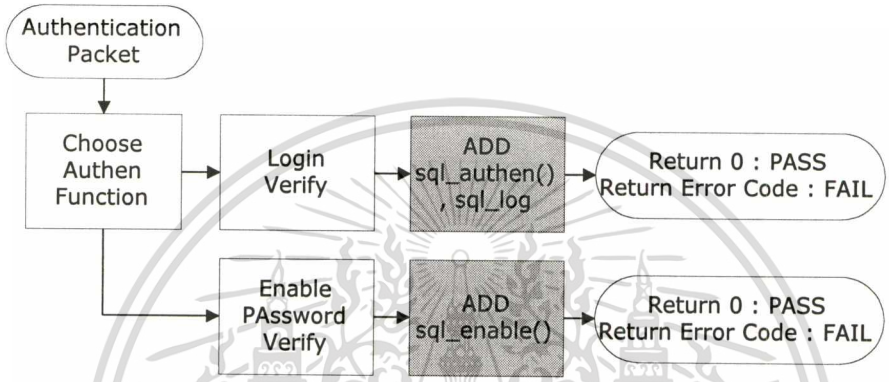
รับข้อมูลจาก NAS และทำการตรวจสอบกับฐานข้อมูล จากนั้นส่งผลที่ได้กลับไปให้ NAS

Process 1.1 : Authentication Sub-Module

- กรณี LOGIN รับข้อมูล 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 , 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())



รูปที่ 4.5 แสดง Authentication Sub-Module

Process 1.2 : Authorization Sub-Module

- รับข้อมูล Authorization packet มาทำการตรวจสอบ SERVICE, CMD, CMD-ARG ว่าอนุญาตให้ใช้งานได้หรือไม่

sql_user_exists() ตรวจสอบว่ามีรายชื่อผู้ใช้อยู่ในฐานข้อมูลหรือไม่

sql_get_svc_ppp() ตรวจสอบว่าอนุญาตให้ผู้ใช้สามารถใช้บริการ PPP ได้หรือไม่

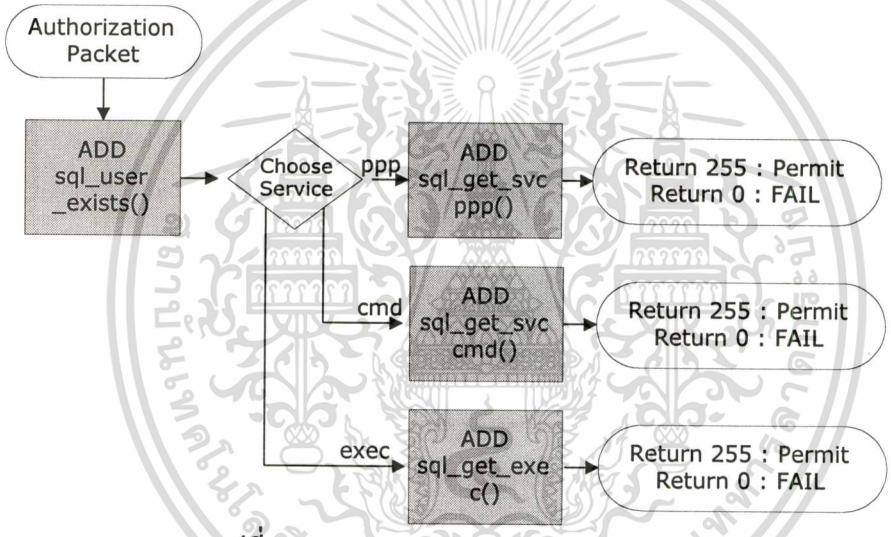
sql_get_svc_exec() ตรวจสอบว่าอนุญาตให้ผู้ใช้สามารถใช้บริการ EXEC ได้หรือไม่

sql_get_svc_cmd() ตรวจสอบว่าอนุญาตให้ผู้ใช้สามารถใช้คำสั่งนั้นๆ ได้หรือไม่

โดยจะทำการตรวจสอบว่า Command permit = "*" หรือไม่ ถ้าใช่จากนั้นทำการตรวจสอบ Command deny ต่อไป

หรือจะทำการทดสอบ Command Argument permit = "*" หรือไม่ ถ้าใช่จะทำการตรวจสอบ Command deny ต่อไป

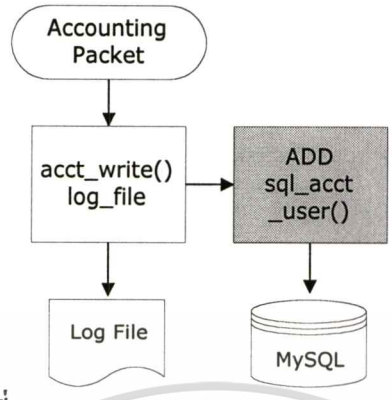
หรือถ้าไม่ได้กำหนดไว้ ให้ตรวจสอบ Command deny เลย



รูปที่ 4.6 แสดง Authorization Sub-Module

Process 1.3 : Accounting Sub-Module

- 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 และอื่นๆ ในฐานข้อมูล ACCT-CMD



รูปที่ 4.7 แสดง Accounting Sub-Module

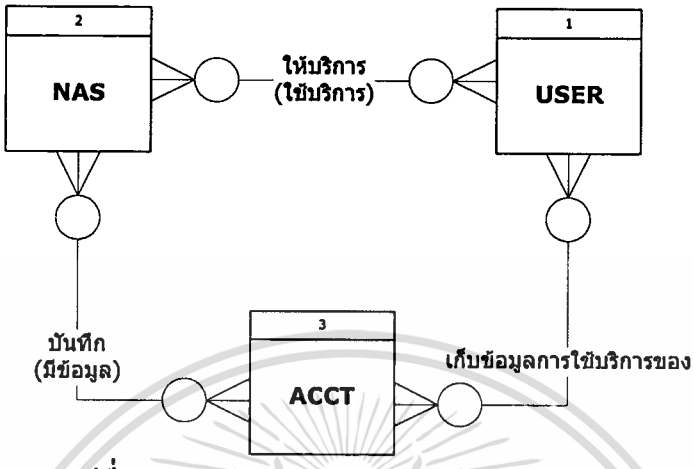
Process 2 : Configuration Module

- เพิ่ม / แก้ไข / ลบ ข้อมูลผู้ใช้ และ ข้อจำกัดเกี่ยวกับ NAS, คำสั่งต่างๆ (CMD) โดย user.php3, user-submit.php3
- เพิ่ม / แก้ไข / ลบ ข้อมูล NAS โดย nas.php3, nas-submit.php3

Process 3: Report Module โดย report.php3, report-submit.php3

- จัดทำรายงานรายชื่อผู้ใช้ในปัจจุบัน (Current User Login Report)
- จัดทำรายงานการใช้งานของผู้ใช้ เป็นรายวันหรือรายเดือน (Usage Report)
- จัดทำรายงาน LOGIN FAIL
- จัดทำรายงานปริมาณการใช้งานของ NAS (Utilization Report)
- จัดทำรายงานการใช้คำสั่งต่างๆ (Command Privilege Report)

4.2.2 Data Modeling



รูปที่ 4.8 แสดง Entity Relationship Diagram

เมื่อทำการวิเคราะห์ข้อมูลแล้ว พิจารณาแยกตารางจากหลักการ ตารางแต่ละตารางจะต้องมีเพียง 1 ความหมาย ทำให้สามารถแบ่งตารางได้ดังนี้

- ตาราง USER เก็บข้อมูลของผู้ใช้ ได้แก่ รหัสผู้ใช้ ชื่อผู้ใช้ Password ข้อจำกัดด้านเวลา (เก็บเป็นรายชั่วโมงในสัปดาห์ 24x7 Y/N) บริการต่างๆ ความสามารถในการแก้ไขข้อมูลระบบ
- ตาราง NAS เก็บข้อมูลของ NAS ได้แก่ รหัส NAS ชื่อ NAS Enable Password และ IP Address ของ NAS
- ตาราง NAS_PERMIT เก็บข้อมูลว่าอนุญาติให้ผู้ใช้ใช้บริการที่ NAS ใดบ้าง
- ตาราง NAS_DENY เก็บข้อมูลว่าไม่อนุญาติให้ผู้ใช้ใช้บริการที่ NAS ใดบ้าง
- ตาราง CMD_PERMIT เก็บข้อมูลว่าอนุญาติให้ผู้ใช้ใช้คำสั่งใดบ้าง
- ตาราง CMD_DENY เก็บข้อมูลว่าไม่อนุญาติให้ผู้ใช้ใช้คำสั่งใดบ้าง
- ตาราง CURRENT เก็บรายชื่อผู้ใช้งาน ณ ปัจจุบัน
- ตาราง UTILIZATION เก็บจำนวนผู้ใช้งานใน NAS ใดๆ ณ วันเวลานั้นๆ เพื่อนำไปทำรายงานจำนวนผู้ใช้งานในระบบ

- 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)
- ตาราง ACCT-CMD เก็บข้อมูลการใช้งานของผู้ใช้เกี่ยวกับคำสั่งต่างๆ ได้แก่วันที่เวลา NAS ที่ใช้งาน Terminal No. IP Address ของผู้ใช้เอง Task ID เวลาเริ่มใช้งาน Time Zone บริการที่ใช้งาน และคำสั่งที่ใช้งาน

4.2.3 Data Dictionary

ตารางที่ 4.1 แสดง Data Dictionary ของ TABLE USER

Attribute	Data Type	Description
USER_ID (PK)	INT(3)	รหัสผู้ใช้
USER_NAME	CHAR(32)	ชื่อผู้ใช้
USER_FULLNAME	CHAR(80)	ชื่อผู้ใช้เต็ม
PASSWORD	CHAR(13)	Password
TIME_RESTRICTION	CHAR(168)	ข้อจำกัดเรื่องวันเวลา
EXPIRE_DATE	DATE	วันหมดอายุ
SERVICE_EXEC	CHAR(1)	บริการ EXEC
SERVICE_PPP	CHAR(1)	บริการ PPP
ADMINISTRATOR	CHAR(1)	เป็นผู้ควบคุมระบบหรือไม่

ตารางที่ 4.2 แสดง Data Dictionary ของ TABLE NAS

Attribute	Data Type	Description
NAS_ID(PK)	INT(3)	รหัส NAS
NAS_NAME	CHAR(32)	ชื่อ NAS
NAS_ADDRESS	CHAR(15)	IP Address ของ NAS
NAS_FULLNAME	CHAR(80)	ชื่อเต็ม NAS
ENABLE_PASSWORD	CHAR(13)	ENABLE PASSWORD

ตารางที่ 4.3 แสดง Data Dictionary ของ TABLE NAS_PERMIT

Attribute	Data Type	Description
USER_ID (PK)	INT(3)	รหัสผู้ใช้
NAS_ID (PK)	INT(3)	รหัส NAS

ตารางที่ 4.4 แสดง Data Dictionary ของ TABLE NAS_DENY

Attribute	Data Type	Description
USER_ID (PK)	INT(3)	รหัสผู้ใช้
NAS_ID (PK)	INT(3)	รหัส NAS

ตารางที่ 4.5 แสดง Data Dictionary ของ TABLE CMD_PERMIT

Attribute	Data Type	Description
USER_ID (PK)	INT(3)	รหัสผู้ใช้
CMD (PK)	CHAR(255)	คำสั่ง
CMD_ARG	CHAR(255)	Argument ของคำสั่ง

ตารางที่ 4.6 แสดง Data Dictionary ของ TABLE CMD_DENY

Attribute	Data Type	Description
USER_ID (PK)	INT(3)	รหัสผู้ใช้
CMD (PK)	CHAR(255)	คำสั่ง
CMD_ARG	CHAR(255)	Argument ของคำสั่ง

ตารางที่ 4.7 แสดง Data Dictionary ของ TABLE CURRENT

Attribute	Data Type	Description
DATE (PK)	DATE	วันที่
TIME (PK)	TIME	เวลา
USER_ID (PK)	INT(3)	รหัสผู้ใช้
NAS_ID (PK)	INT(3)	รหัส NAS

ตารางที่ 4.8 แสดง Data Dictionary ของ TABLE UTILIZATION

Attribute	Data Type	Description
DATE (PK)	DATE	วันที่
TIME (PK)	TIME	เวลา
NAS_ID	INT(3)	รหัส NAS
NO_OF_USER	INT(3)	จำนวนผู้ใช้บริการ

ตารางที่ 4.9 แสดง Data Dictionary ของ TABLE LOGIN_FAIL

Attribute	Data Type	Description
DATE (PK)	DATE	วันที่
TIME (PK)	TIME	เวลา
USER_ID (PK)	INT(3)	รหัสผู้ใช้
NAS_ID (PK)	INT(3)	รหัส NAS
REASON	CHAR(20)	เหตุผล

ตารางที่ 4.10 แสดง Data Dictionary ของ TABLE ACCT_USER

Attribute	Data Type	Description
ACCT_ID (PK)	INT(4)	รหัส ACCT
DATE	DATE	วันที่
TIME	TIME	เวลา
NAS_ID	INT(3)	รหัส NAS
USER_ID	INT(3)	รหัสผู้ใช้

TERMINAL_NO	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

ตารางที่ 4.11 แสดง Data Dictionary ของ TABLE ACCT_CMD

Attribute	**Data Type**	**Description**
ACCT_ID (PK)	INT(4)	รหัส ACCT
DATE	DATE	วันที่
TIME	TIME	เวลา
NAS_ID	INT(3)	รหัส NAS
USER_ID	INT(3)	รหัสผู้ใช้
TERMINAL_NO	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_LEVEL	INT(1)	ระดับความสามารถ
CMD	CHAR(255)	คำสั่ง
CMD_ARG	CHAR(255)	Argument ของคำสั่ง

บทที่ 5

NAS Configuration

ในโครงการพัฒนาระบบงานนี้ใช้ผลิตภัณฑ์ NAS ของ Cisco Systems, Inc. รุ่น Cisco 4500 Software IOS Version 11.2

5.1 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 10.0.87.19
- กำหนด shared secret key ใช้ encrypt ข้อมูลระหว่าง NAS – TACACS+ Server ใช้คำสั่งดังนี้

  NAS(config)#tacacs-server key yourkey

5.2 Authentication

- วิธี Authentication มีดังนี้
  - enable ใช้ enable password
  - line ใช้ line password
  - local ใช้ local username database
  - none ไม่ต้อง Authentication
  - tacacs+ ใช้ TACACS+ Authentication

- กำหนดให้ login จาก vty port ต้อง authentication ด้วยวิธี tacacs+ และเมื่อไม่สามารถติดต่อ TACACS+ Server ได้ให้ใช้วิธี local data ใช้คำสั่งดังนี้

```
NAS(config)#aaa authentication login vty-login tacacs+ local
NAS(config)#line vty 0 4
NAS(config-line)#login authentication vty-login
```

- กำหนดให้ login จาก async ppp port ต้อง authentication ด้วยวิธี tacacs+ และเมื่อไม่สามารถติดต่อ TACACS+ Server ได้ให้ใช้วิธี local data ใช้คำสั่งดังนี้

```
NAS(config)#aaa authentication ppp ppp-login tacacs+ local
NAS(config)#interface async 1
NAS(config-line)#login authentication ppp-login
```

- กำหนดให้ เมื่อต้องการ enable privilege ต้อง authentication ด้วยวิธี tacacs+ และเมื่อไม่สามารถติดต่อ TACACS+ Server ได้ให้ใช้วิธี local enable ใช้คำสั่งดังนี้

```
NAS(config)#aaa authentication enable default tacacs+ enable none
```

5.3 Authorization

- Keyword บริการต่างๆ

Network	บริการ SLIP, PPP, PPP NCPs, และ ARA
Connection	บริการ outbound telnet และ rlogin
Exec	บริการ shell
Command level	การใช้คำสั่งต่างๆ ใน privilege level นั้นๆ

- วิธี Authorization มีดังนี้

tacacs+	ใช้ TACACS+ Authentication
if-autenticated	อนุญาตให้ผู้ใช้ที่ผ่าน authentication แล้ว
none	ไม่ต้อง Authorization
local	ใช้ local database สำหรับ authorization

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

  NAS(config)#aaa authorization exec tacacs+ none

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

  NAS(config)#aaa authorization connection tacacs+ none

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

  NAS(config)#aaa authorization network tacacs+ none

- กำหนดให้ผู้ใช้ที่ต้องการใช้คำสั่งที่มี privilege 15 ต้อง authorzentication ด้วยวิธี tacacs+ และเมื่อไม่สามารถติดต่อ TACACS+ Server ได้ ไม่ต้อง authorization ใช้คำสั่งดังนี้

  NAS(config)#aaa authorization command 15 tacacs+ none

5.4 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 start-stop tacacs+

- กำหนดให้มีการส่ง Account packet กรณีที่เริ่มและเลิกใช้บริการ Network (PPP) ใช้คำสั่งดังนี้

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

- กำหนดให้มีการส่ง Account packet กรณีที่ใช้ใช้คำสั่งในระดับ privilege 15 (สูงสุด) ใช้คำสั่งดังนี้

  NAS(config)#aaa accounting command 15 stop-only tacacs+

5.5 สรุป Configuration

```
!
user local-username password local-password
!
aaa new-model
aaa authentication login vty-login tacacs+ local
aaa authentication ppp ppp-login tacacs+ local
aaa authentication enable default tacacs+ enable none
aaa authorization exec tacacs+ none
aaa authorization connection tacacs+ none
aaa authorization network tacacs+ none
aaa authorization command 15 tacacs+ none
aaa accounting exec start-stop tacacs+
aaa accounting network start-stop tacacs+
aaa accounting  command 15 stop-only tacacs+
!
```

```
interface Async 1
  login authentication ppp-login
!
tacacs-server host 10.0.87.19
tacacs-server key yourkey
!
line vty 0 4
login authentication vty-login
!
```

บทที่ 6

Web User Interface

Web User Interface ของ TACACS+ Server Management System via Web แบ่งออกเป็น 4 ส่วนหลักๆ ได้แก่

- Administrator Login
- User Information
- NAS Configuration
- Report

6.1 Administrator Login

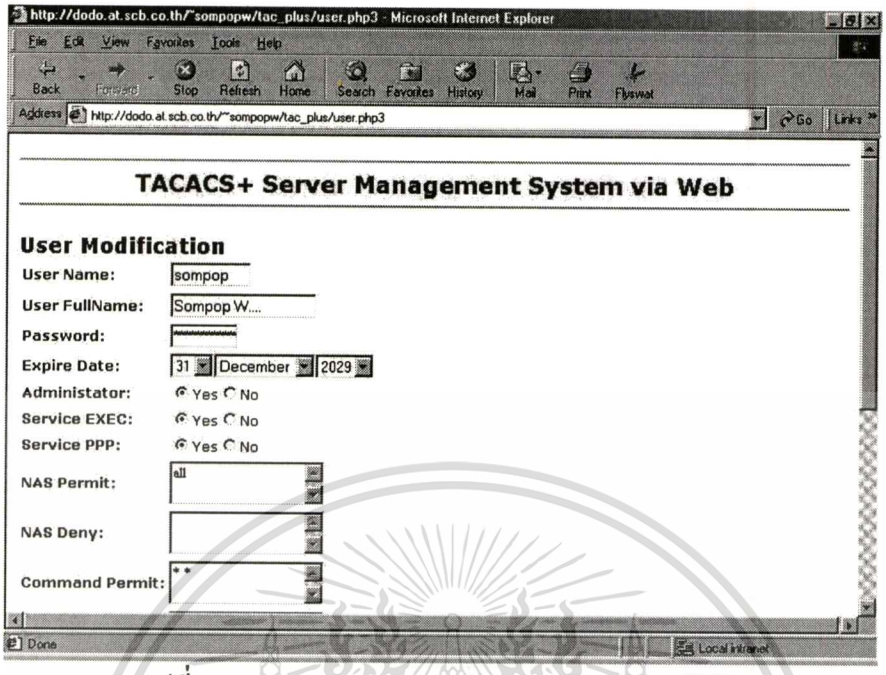
เป็นการตรวจสอบสิทธิในการแก้ไขข้อมูล ในฐานข้อมูล USER

6.2 User Information

ส่วน User Information มี 3 หน้าที่คือ Add, Update, Delete

ข้อมูลเกี่ยวกับ User ที่สามารถแก้ไขได้มีดังนี้

- User ID รหัสผู้ใช้
- User Name ชื่อผู้ใช้
- User Full Name ชื่อเต็มผู้ใช้
- Password รหัสลับ
- Expire Date วันหมดอายุ
- Administrator ความสามารถในการแก้ไขข้อมูล
- NAS Permit NAS ที่อนุญาตให้ใช้ได้
- NAS Deny NAS ที่ไม่อนุญาตให้ใช้
- Time Restriction วันเวลาที่อนุญาตให้ใช้ได้ ในรอบสัปดาห์
- Command Permit คำสั่งที่อนุญาตให้ใช้ได้
- Command Deny คำสั่งที่ไม่อนุญาตให้ใช้ได้



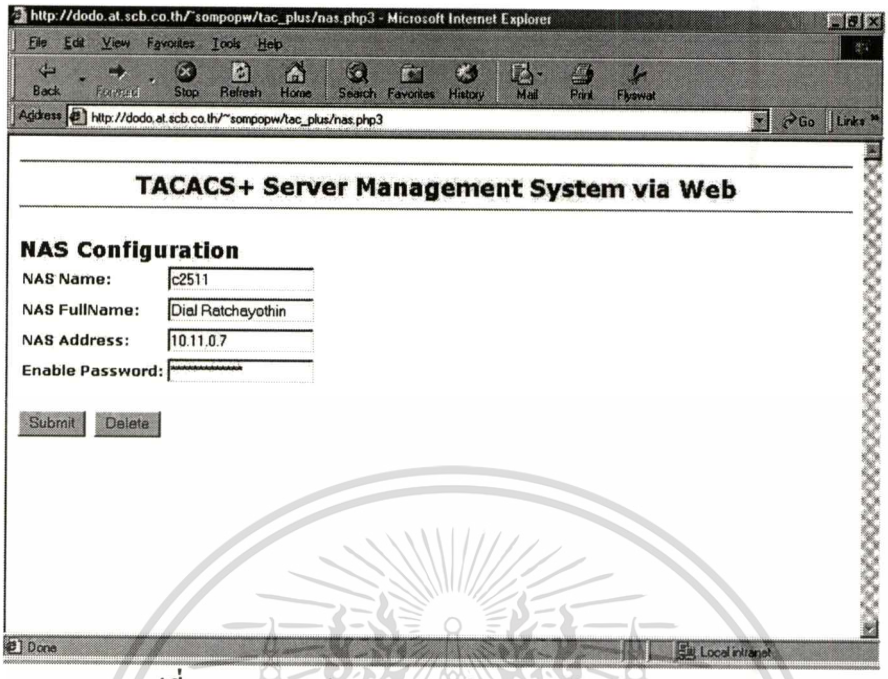
รูปที่ 6.1 แสดงรูปแบบ Form ในการแก้ไขข้อมูลผู้ใช้

6.2 NAS Configuration

ส่วน NAS Configuration มี 3 หน้าที่คือ Add, Update, Delete

ข้อมูลเกี่ยวกับ NAS ที่สามารถแก้ไขได้มีดังนี้

- NAS ID รหัส NAS
- NAS Name ชื่อ NAS
- NAS Full Name ชื่อเต็ม NAS
- NAS Address IP Address ของ NAS
- Enable Password Enable privilege password

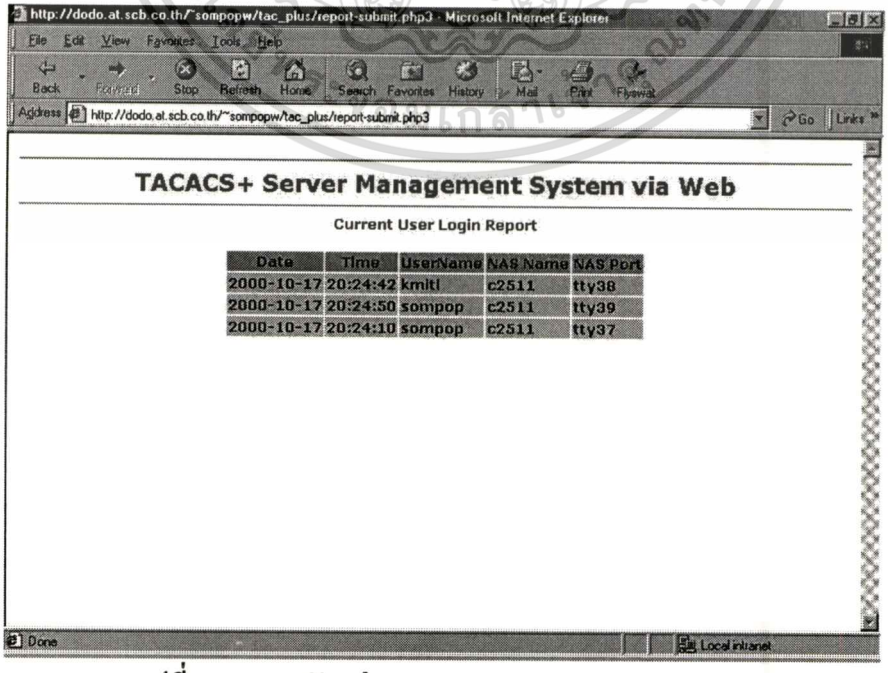


รูปที่ 6.2 แสดงรูปแบบ Form ในการแก้ไขข้อมูล NAS

6.3 Report

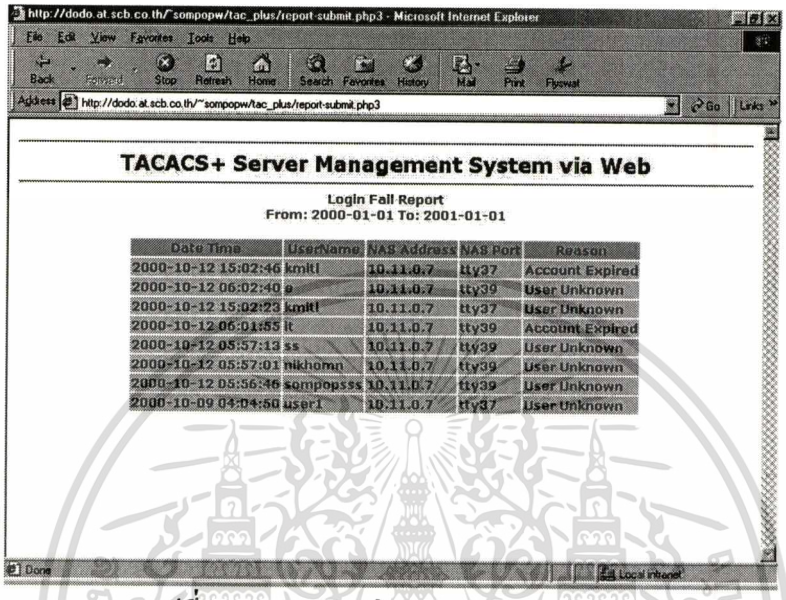
มี 5 Report ดังนี้

- Current User Login แสดงรายชื่อผู้ใช้งานในระบบ ณ เวลาปัจจุบัน โดยจะต้องเลือก NAS ที่ต้องการก่อน



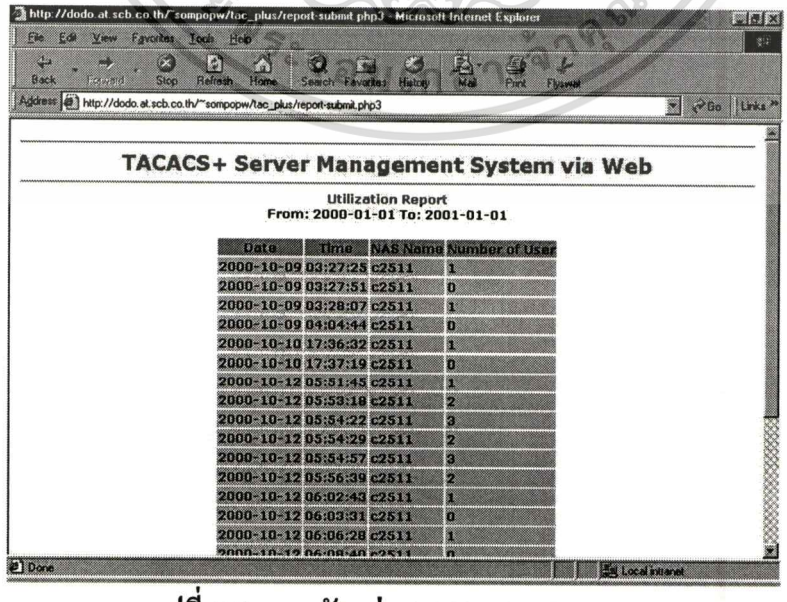
รูปที่ 6.3 แสดงตัวอย่าง Current User Login Report

- Login Fail แสดงรายชื่อผู้ใช้งานที่มีการ login fail โดยสามารถเลือก ช่วงเวลาที่ต้องการจะดู, เหตุผล หรือ ผู้ใช้คนใดคนหนึ่งได้



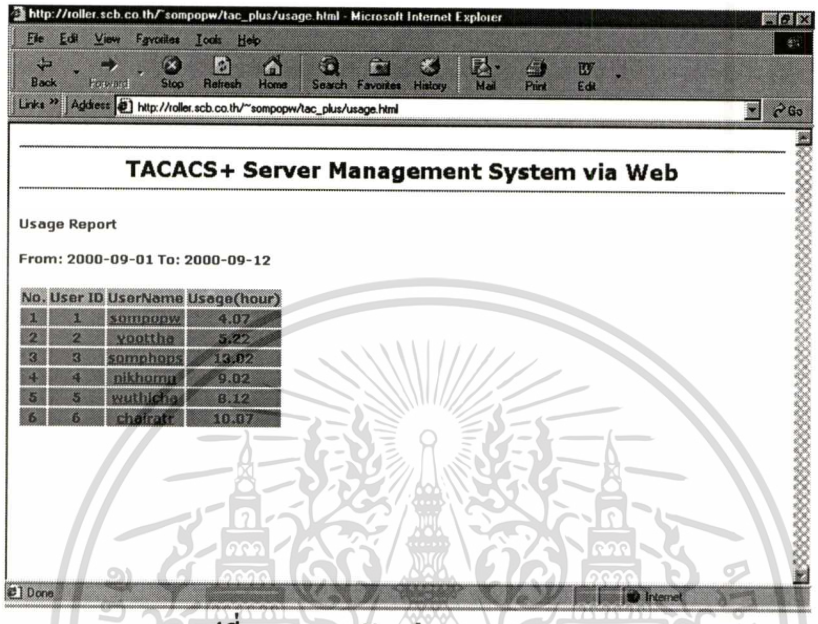
รูปที่ 6.4 แสดงตัวอย่าง Login Fail Report

- Utilization แสดงจำนวนผู้ใช้งาน โดยสามารถเลือก ช่วงเวลาที่ต้องการจะดู และ NAS ที่ต้องการดู

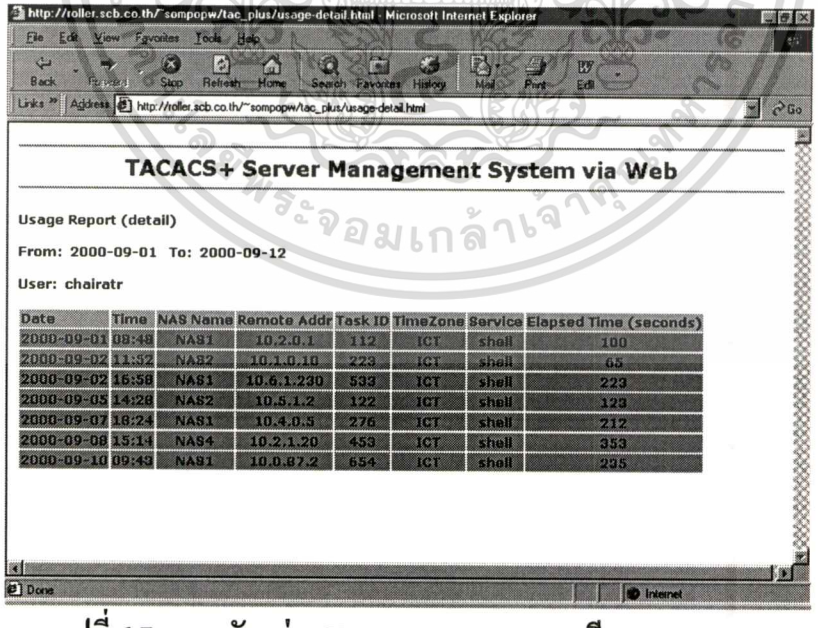


รูปที่ 6.5 แสดงตัวอย่าง Utilization Report

- Usage แสดงรายชื่อผู้ใช้งาน และจำนวนชั่วโมงที่ใช้งาน โดยสามารถเลือกช่วงเวลาที่ต้องการจะดู และสามารถเลือกดูรายละเอียดเป็นรายบุคคลได้

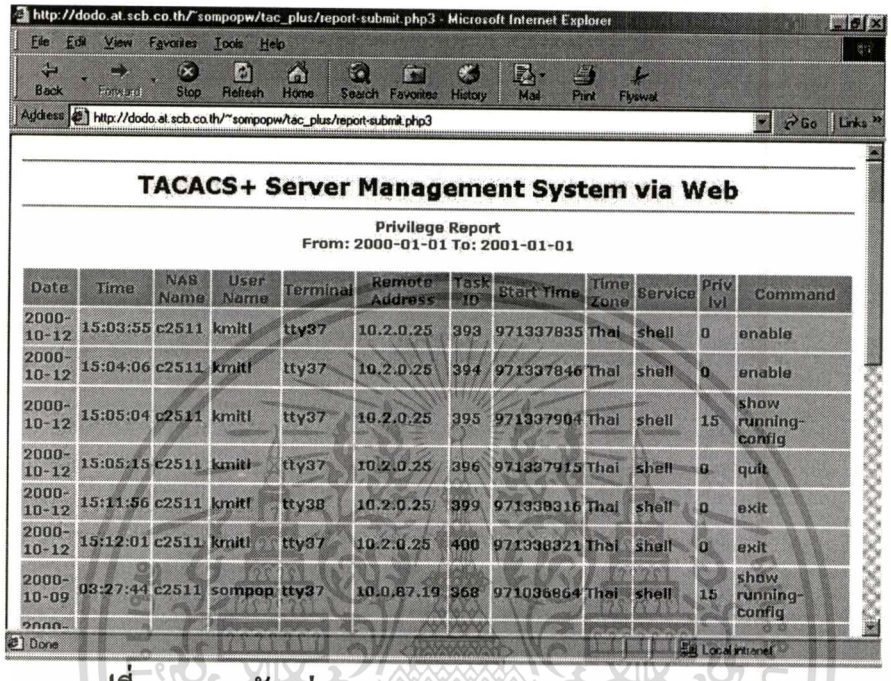


รูปที่ 6.6 แสดงตัวอย่าง Usage Report



รูปที่ 6.7 แสดงตัวอย่าง Usage Report แบบละเอียดรายบุคคล

- Command Privilege Level 15 แสดงรายชื่อผู้ใช้งาน วันเวลาและคำสั่งที่ใช้งาน โดยสามารถเลือก ช่วงเวลาที่ต้องการจะดู



รูปที่ 6.8 แสดงตัวอย่าง Command Privilege Level 15 Report

บทที่ 7
สรุปและข้อเสนอแนะ

7.1 สรุปผลการพัฒนาระบบ

จากการพัฒนาระบบควบคุม TACACS+ Server ผ่าน Web มีข้อดีดังนี้

- มีความง่ายในการใช้งาน นำ Web User Interface มาใช้ ผ่าน Web Browser
- มีความสามารถในการรองรับจำนวนผู้ใช้มากๆ ได้ เพราะข้อมูลต่างๆ เก็บอยู่ใน ฐานข้อมูล
- สามารถกำหนดนโยบายเกี่ยวกับความสามารถของผู้ใช้ได้มากขึ้นโดยเฉพาะอย่างยิ่งเรื่องคำสั่งที่อนุญาตให้ใช้ได้หรือไม่ เช่น อนุญาตให้ใช้คำสั่ง show configuration ไม่ให้ใช้คำสั่ง show running-config เป็นต้น
- สามารถกำหนด Account Expire ได้ เช่นหมดอายุตั้งแต่วันที่ 10 ธันวาคม 2543 ทำให้ผู้ใฝ้ไม่สามารถใช้งานได้หลังจากวันที่ดังกล่าว เป็นต้น
- สามารถกำหนดข้อจำกัดการใช้งานตามวันและเวลาได้ เช่นไม่อนุญาตให้ใช้งานวันเสาร์เวลา 13.00 น. และเวลา 20.00 น. เวลาอื่นอนุญาตให้ใช้งานได้ เป็นต้น
- สามารถกำหนดข้อจำกัดการใช้งานตาม NAS แต่ละตัวได้ เช่น อนุญาติให้ใช้งานที่ NAS – (c2511) ได้ ตัวอื่นไม่อนุญาต เป็นต้น
- การส่งข้อมูลผ่านเครือข่ายมีความปลอดภัยมากขึ้น เพราะมีการ encrypt ข้อมูลที่ส่งและรับทั้ง packet body ตามมาตรฐานของ TACACS+ Protocol

7.2 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

บรรณานุกรม

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

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

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

ภาคผนวก

การติดตั้งระบบ TACACS+ Server Management System

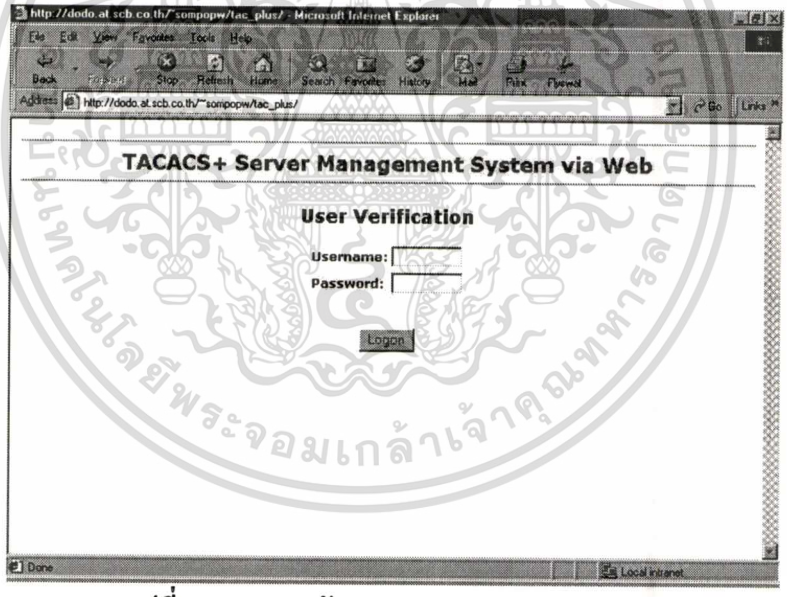
1. ติดตั้ง Solaris 2.7 x86
2. ติดตั้ง GNU gzip 1.2.4 i86pc Solaris 7
   - โดยใช้คำสั่ง pkgadd -d gzip-1.2.4-sol7-intel-local
3. ติดตั้ง GNU gcc 2.95.2 i86pc Solaris 7
   - unzip โดยใช้คำสั่ง gzip -d GNUgcc.2.95.2.i86pc.Solaris.7.pkg.tgz
   - untar โดยใช้คำสั่ง tar xpvf GNUgcc.2.95.2.i86pc.Solaris.7.pkg.tar
   - install โดยใช้คำสั่ง pkgadd -d .
4. ติดตั้ง GNU tar 1.13 i86pc Solaris 7
   - unzip โดยใช้คำสั่ง gzip -d GNUtar.1.13.i86pc.Solaris.7.pkg.tgz
   - untar โดยใช้คำสั่ง tar xpvf GNUtar.1.13.i86pc.Solaris.7.pkg.tar
   - install โดยใช้คำสั่ง pkgadd -d ./GNUtar
5. ติดตั้ง GNU make 3.78.1 i86pc Solaris 7
   - unzip โดยใช้คำสั่ง gzip -d GNUmake.3.78.1.i86pc.Solaris.7.pkg.tgz
   - untar โดยใช้คำสั่ง tar xpvf GNUmake.3.78.1.i86pc.Solaris.7.pkg.tar
   - - install โดยใช้คำสั่ง pkgadd -d ./GNUmake
6. ติดตั้ง Perl 5.005_02 i86pc Solaris 7
   - โดยใช้คำสั่ง pkgadd -d gzip-1.2.4-sol7-intel-local
7. ติดตั้ง mysql 3.22.32
   - unzip, configuration, make all
   - change root's password
   - create database tac_plus
   - create table: user, nas, nas_permit, nas_deny, cmd_permit, cmd_deny, login_fail, acct-user, acct-cmd, current, utilization
8. ติดตั้ง apache 1.3.12
   - unzip, configuration, make all

9. ติดตั้ง php 3.0.16
    - unzip, configuration (with option apache & mysql) , make all
10. ติดตั้ง aaa daemon (tac_plus 2.1)
    - untar โดยใช้คำสั่ง tar xpvf aaa_module.tar

การใช้งานระบบ

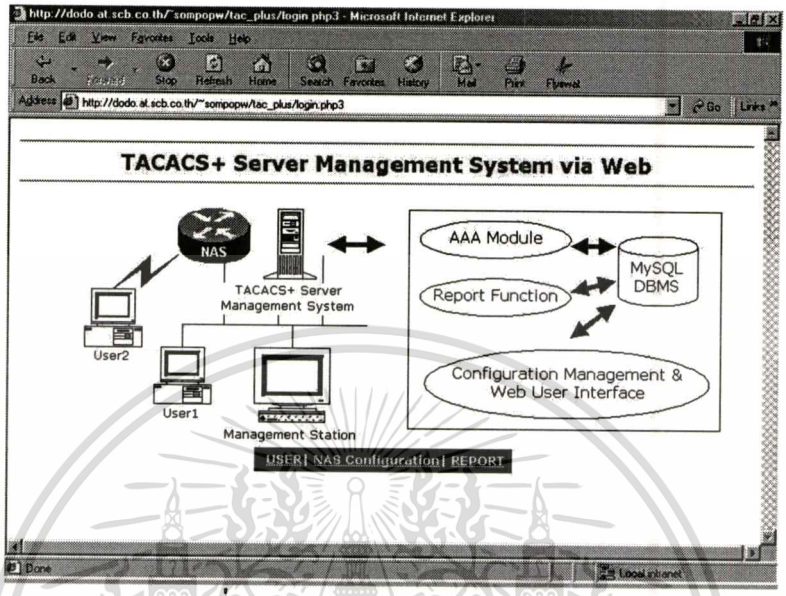
ขั้นตอนแรก start AAA Module ก่อน โดยใช้คำสั่ง $AAA_DIR/tac_plus –C key.conf

ขั้นตอนที่ 2 การ Login เข้าสู่การแก้ไขข้อมูลต่างๆ โดยกรอก User Name ที่เป็น Administrator และ Password ในหน้าจอต่อไปนี้



รูปที่ 8.1 แสดงหน้าจอ Administrator Login

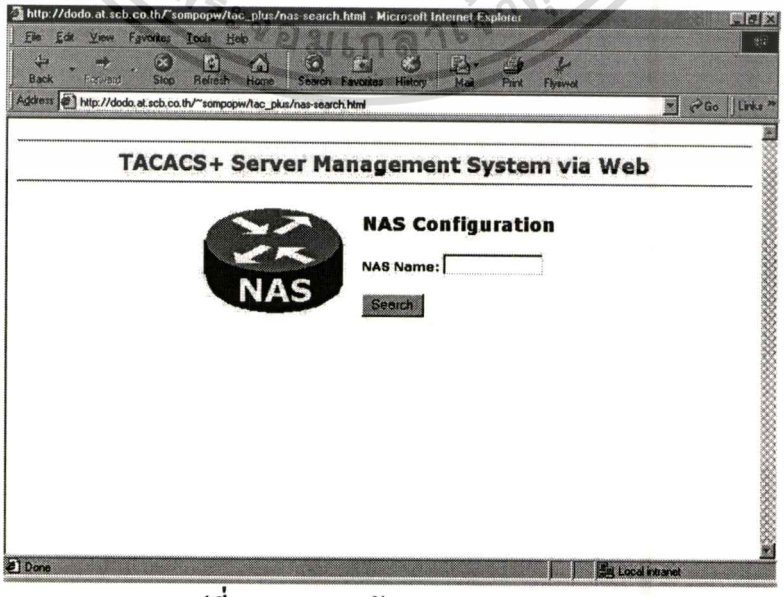
ขั้นตอนที่ 3 เลือกหัวข้อที่ต้องการแก้ไข



รูปที่ 8.2 แสดงหน้าจอ Main Menu

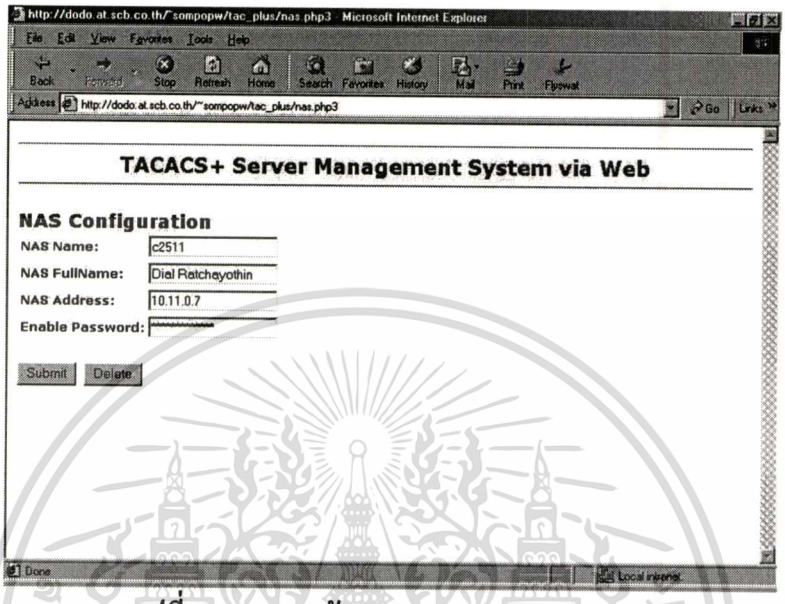
ขั้นตอนที่ 4 กรณีเลือกหัวข้อ NAS Configuration

ให้ใส่ NAS Name ที่ต้องการแก้ไข หรือถ้าไม่มีในระบบจะเป็นการเพิ่มโดยอัตโนมัติ



รูปที่ 8.2 แสดงหน้าจอ NAS Search

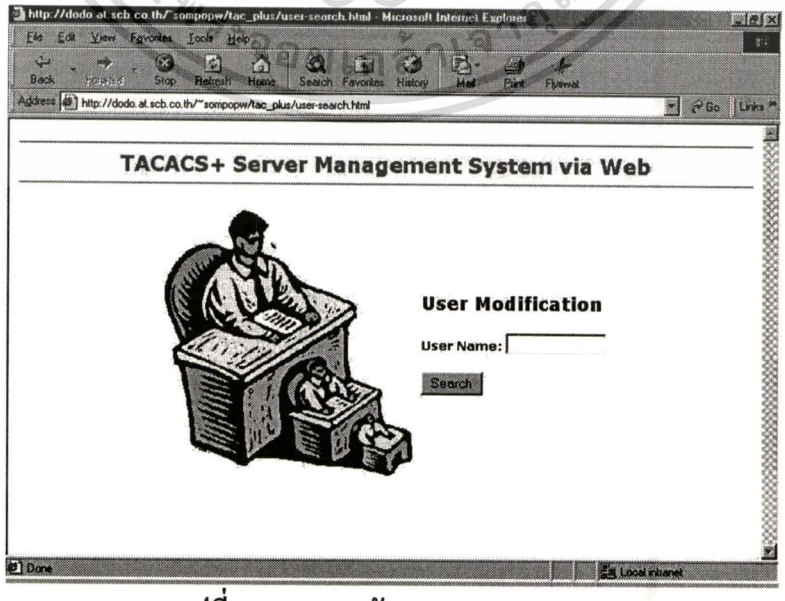
จากนั้นให้กรอกข้อมูล NAS Configuration ต่างๆ เมื่อเรียบร้อยแล้วให้กด Submit หรือ Delete เมื่อต้องการลบข้อมูล NAS นั้นๆ



รูปที่ 8.3 แสดงหน้าจอ NAS Configuration

ขั้นตอนที่ 5 กรณีเลือกหัวข้อ User

ให้ใส่ User Name ที่ต้องการแก้ไข หรือถ้าไม่มีในระบบจะเป็นการเพิ่มโดยอัตโนมัติ

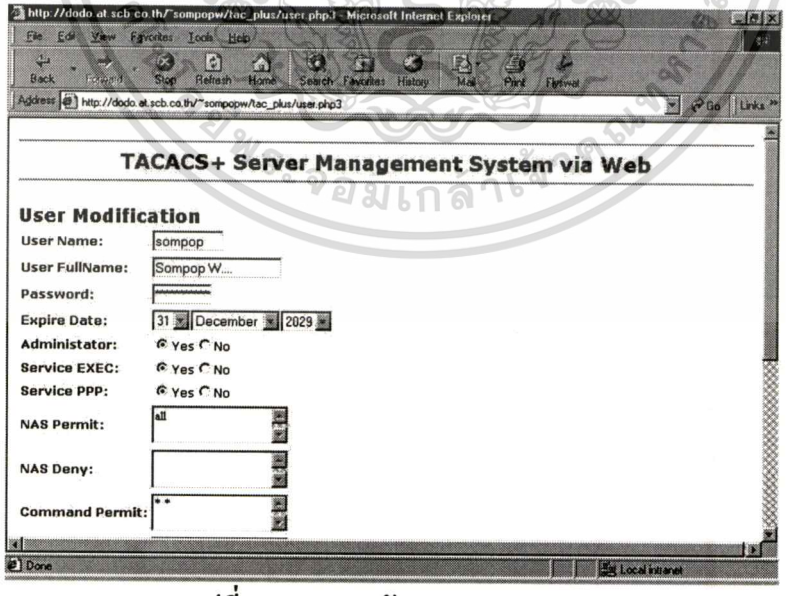


รูปที่ 8.4 แสดงหน้าจอ User Search

จากนั้นให้กรอกข้อมูล User ต่างๆ โดย

- User Name ไม่เกิน 32 ตัวอักษร และต้องไม่ซ้ำด้วย
- User Full Name ไม่เกิน 80 ตัวอักษร
- Password ไม่เกิน 8 ตัวอักษร
- Expire Date คือวันหมดอายุ
- Time Restriction คือข้อจำกัดตามวันและเวลา Check = Permit
- NAS Permit/Deny ให้กรอกเป็น IP Address ของ NAS นั้นๆ ทีละตัว คนละบรรทัด เมื่อต้องการอนุญาตหรือปฏิเสธทั้งหมด ให้ใช้ “all”
- Command Permit/Deny ให้กรอกเป็น Command และตามด้วย Command Argument เช่น show configuration คำสั่งที่กรอกลงไปจะต้องเป็นคำสั่งเต็มๆ ห้ามย่อ กรณีที่ต้องการอนุญาตหรือปฏิเสธทั้งหมด ให้ใช้ “*” เช่น “show *” หรือ “* *”

เมื่อเรียบร้อยแล้วให้กด Submit หรือ Delete เมื่อต้องการลบข้อมูล User นั้นๆ

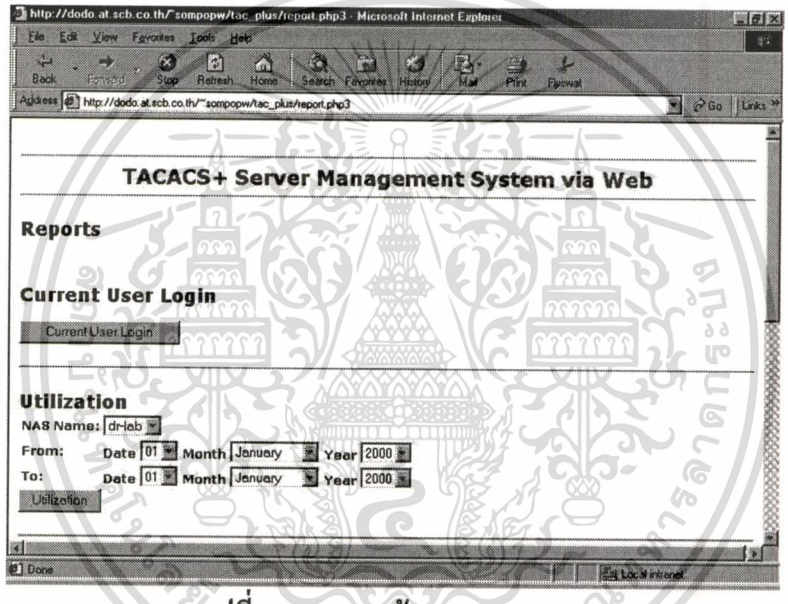


รูปที่ 8.5 แสดงหน้าจอ User Search

ขั้นตอนที่ 5 กรณีเลือกหัวข้อ Report

ให้เลือกช่วงวันที่ ที่ต้องการรายงาน และ NAS Name ตามหัวข้อ Report ต่างๆ

- Current User Login
- Utilization
- Login Fail
- Usage
- Command Privilege



รูปที่ 8.6 แสดงหน้าจอ Report

ประวัติผู้เขียน

ชื่อ-สกุล	นายสมภพ วชิรลาภไพฑูรย์
สถานที่เกิด	กรุงเทพมหานคร
ประวัติการศึกษา	วศ.บ (วิศวกรรมไฟฟ้า)
	มหาวิทยาลัยมหิดล
ประวัติการทำงาน	โครงการ Digital Network
	สำนักงานเทคโนโลยีประยุกต์
	ธนาคารไทยพาณิชย์ (มหาชน) จำกัด