รายงานสหกิจศึกษาฉบับสมบูรณ์

ระบบควบคุมการเข้าใช้งานเครือข่ายภายในองค์กร
Network Access Control System for SMB

วีรศักดิ์ สุวรรณพงษ์
WEERASAK SUWANNAPONG

ภาควิชาวิศวกรรมคอมพิวเตอร์ สาขาวิชาวิศวกรรมสารสนเทศ
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2560

รายงานสหกิจศึกษาฉบับสมบูรณ์

ระบบควบคุมการเข้าใช้งานเครือข่ายภายในองค์กร

Network Access Control System for SMB

วีรศักดิ์ สุวรรณพงษ์

WEERASAK SUWANNAPONG

ภาควิชาวิศวกรรมคอมพิวเตอร์ สาขาวิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2560

ชื่อโครงงานสหกิจศึกษา	ระบบควบคุมการเข้าใช้งานเครือข่ายภายในองค์กร
ชื่อ-สกุลนักศึกษา	นายวีรศักดิ์ สุวรรณพงษ์
คณะ	วิศวกรรมศาสตร์บัณฑิต **ภาควิชา** วิศวกรรมสารสนเทศ
ชื่อ-สกุล อาจารย์นิเทศน์	ผศ.มยุรี เลิศเวชกุล
ชื่อ-สกุล ผู้นิเทศน์งาน	คุณนฤดล รุ่งวีรกุลอนันต์
ชื่อสถานประกอบการ	บริษัท ไดเมนชั่นดาต้า (ประเทศไทย) จำกัด

บทคัดย่อ

บริษัท ไดเมนชั่นดาต้า (ประเทศไทย) จำกัดเป็นบริษัทที่ให้บริการโซลูชั่นทางด้านไอที มีความต้องการที่จะใช้งานซอฟต์แวร์โอเพนซอร์สเพื่อเพิ่มความปลอดภัยให้กับระบบเครือข่าย ในการตรวจสอบผู้ที่เข้าใช้งานระบบ หรือผู้ที่มีสิทธิในการจัดการระบบ สามารถกำหนดขอบเขตการทำงานของแต่ละบุคคลที่เข้ามาใช้งาน ทั้งนี้การดำเนินโครงงานนี้จำเป็นต้องใช้ความรู้ทางด้านความปลอดภัยของเครือข่าย การออกแบบ การติดตั้ง การตั้งค่าอุปกรณ์เครื่อข่าย มีการวิเคราะห์ปัญหาที่เกิดขึ้น เพื่อเสนอแนวทางการแก้ไขปัญหาให้กับลูกค้า และมีการติดตามงานเพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพสูงที่สุด และเป็นที่พึงพอใจของลูกค้า

Co-operative Title	Network Access Control System for SMB
Student Intern Name	Weerasak Suwannapong
Faculty	Engineering **Department** Information Engineering
Advisor Name	Asst.Prof. Mayuree Lertwatechakul
Mentor Name	Narudol Rungveerakulanan
Company	Dimension Data (Thailand) Limited

ABSTRACT

Dimension Data (Thailand) Limited is a company whose main business is to provide IT business solutions. Recently, there are needs to use the network access control system for implementing the customers' network security. It is required to have knowledge in network security as well as how to design, install and configure networking equipment. The problem analysis is also needed before a design phase as to deliver the most security and efficient network solution to the customer.

กิตติกรรมประกาศ

ข้าพเจ้าได้รับผิดชอบและปฏิบัติหน้าที่ในบริษัท ไดเมนชั่นดาต้า จำกัด ระหว่างวันที่ 7 สิงหาคม ถึงวันที่ 24 พฤศจิกายน พ.ศ.2560 ในโครงการวิชาสหกิจศึกษาที่ทางคณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และบริษัทฯร่วมมือกันจัดตั้งขึ้นในหัวข้อโครงการ การพัฒนาระบบยืนยันตัวตนและกำหนดสิทธิ์การเข้าใช้งานเครือข่ายภายในองค์กร ซึ่งข้าพเจ้าได้รับความรู้ ความเข้าใจและประสบการณ์ในการทำงานที่เป็นประโยชน์อย่างมาก อีกทั้งการดูแลและการช่วยเหลือต่าง ๆ ตลอดเวลาการทำงาน โดยการปฏิบัติงานสหกิจศึกษาในครั้งนี้สำเร็จลุล่วงได้ เพราะมีการชี้แนะและได้รับความร่วมมือจากบุคคลต่าง ๆ ดังต่อไปนี้

พนักงานแผนก Managed Service

- คุณนฤดล รุ่งวีรกุลอนันต์
- คุณจุไรรัตน์ สุภาวัฒนา
- คุณสัมพันธ์ ศรจรัสสุวรรณ
- คุณภาคภูมิ พรประทานเวช
- คุณชโยทิศ พันธ์ธนพฤกษ์
- คุณอัครกิตติ วงศ์สิงห์
- คุณธีร์วราภัทร์ ศรอนันต์กุล
- คุณวาสนา สุขเกษม
- คุณสิรวิชญ์ อมรกิตติสาร

พนักงานแผนกทรัพยากรบุคคล

- คุณอรียา จารุภูมิ

และข้าพเจ้าขอขอบคุณอาจารย์ที่ปรึกษา ผศ.มยุรี เลิศเวชกุล ที่คอยให้คำแนะนำ คำปรึกษาและคอยรับฟังและช่วยเหลือปัญหาต่าง ๆ ในการทำโครงการครั้งนี้ และท้ายที่สุดข้าพเจ้าขอขอบคุณครอบครัวที่คอยให้กำลังใจที่ดีแก่ข้าพเจ้าเสมอมาทำให้ปริญญานิพนธ์ฉบับนี้ให้สำเร็จลุล่วงไปได้ด้วยดี

วีรศักดิ์ สุวรรณพงษ์

สารบัญ

หน้า

สารบัญรูปภาพ

สารบัญตาราง

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญ

เนื่องจาก บริษัท ไดเมนชั่นดาต้า (ประเทศไทย) จำกัด ได้จัดโครงการสหกิจศึกษาระหว่างบริษัท ไดเมนชั่นดาต้า (ประเทศไทย) จำกัด กับ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยในส่วนงานของแผนกติดตั้งนั้น ได้มีการติดตั้งระบบการยืนยันตัวตนและกำหนดสิทธิการเข้าจัดการระบบเครือข่ายภายในองค์กรให้กับบริษัทแห่งหนึ่ง จึงได้มีการมอบหมายงานให้นักศึกษาทำการศึกษาและหาความรู้เกี่ยวเทคโนโลยีการยืนยันตัวตนและกำหนดสิทธิการเข้าจัดการระบบเครือข่ายภายในองค์กร ซึ่งเป็นผลิตภัณฑ์ซอฟแวร์ชนิดหนึ่ง รวมถึงวิธีการติดตั้งและการออกแบบ เพื่อให้นักศึกษามีความรู้และสามารถออกแบบและติดตั้งระบบให้กับลูกค้าได้ ตามความต้องการที่ได้รับมาจากลูกค้า

1.2 วัตถุประสงค์ของการปฏิบัติงาน

เนื่องจากบริษัท ไดเมนชั่นดาต้า (ประเทศไทย) จำกัด เป็นบริษัทที่ให้บริการโซลูชั่นทางด้านไอทีแก่ธุรกิจต่างๆ มีความต้องการที่จะขยายขอบเขตของผลิตภัณฑ์ที่จะให้บริการแก่ลูกค้าเพื่อให้ลูกค้านั้นได้มีตัวเลือกมากยิ่งขึ้นในการใช้บริการของไดเมนชั่นดาต้าและเพื่อประสิทธิภาพของระบบเครือข่ายของลูกค้านั้น จำเป็นต้องมีการศึกษาในตัวผลิตภัณฑ์และทำการทดสอบการทำงานในระดับเบื้องต้นก่อนที่จะนำไปติดตั้งหรือให้บริการกับลูกค้า

1.3 วิธีการดำเนินงาน

- ศึกษาระบบและเทคโนโลยีของ Software รวมถึงคุณสมบัติการทำงานต่างๆตามความต้องการ (Requirement)
- วิเคราะห์ ระบบเครือข่ายของลูกค้าที่จะต้องการนำ Software ไปติดตั้ง
- ออกแบบและแก้ไขระบบเครือข่ายเพื่อให้ได้ตรงตาม Requirement
- ทดสอบระบบ
- วิเคราะห์ปัญหาที่เกิดขึ้น
- เสนอแนะแนวทางการเพิ่มประสิทธิภาพ
- สรุปผล

1.4 ขอบเขตของงาน

- เรียนรู้การทำงานและศึกษาโครงสร้างระบบความปลอดภัยของเครือข่ายที่จะนำ Software ไปติดตั้ง
- กำหนดรูปแบบการยืนยันตัวตนในการเข้าใช้งานระบบ
- กำหนดสิทธิของแต่ละบุคคลากรที่ทำหน้าที่ดูแลเครือข่าย
- จัดการชุดคำสั่งในการใช้งาน
- เสนอแนะแนวทางการเพิ่มประสิทธิภาพให้กับระบบเครือข่าย

1.5 ประโยชน์ที่คาดว่าจะได้รับ

- นักศึกษาได้รับความรู้และเข้าใจในเรื่องของ Network Security และการ Design ตาม Requirement ที่ได้รับ
- ระบบเครือข่ายที่ได้รับการติดตั้ง จะมีประสิทธิภาพในการทำงานและการจัดการทรัพยากรมากยิ่งขึ้น
- บริษัทฯได้รับแนวทางในการติดตั้งอุปกรณ์และ Software ตามการออกแบบและความต้องการ

บทที่ 2

ทบทวนวรรณกรรม

2.1 Network Access Control

Network Access control (NAC) เป็นระบบการควมคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย เพื่อป้องกันภัยที่อาจจะเกิดขึ้นภายในระบบเครื่อข่าย เช่น ป้องกันผู้ใช้งานที่ไม่ได้รับอนุญาตมาใช้งานเครือข่ายและทรัพยากรในเครือข่าย ควบคุมผู้ใช้งานที่ได้รับอนุญาตให้ใช้งานได้เครือข่ายได้ตามหน้าที่ที่รับผิดชอบเท่านั้น ตรวจสอบความพร้อมของเครือคอมพิวเตอร์ก่อนอนุญาตให้เข้าใช้งาน เช่น ตรวจสอบ Antivirus หรือ Firewall เป็นต้น โดยตัวอุปกรณ์ NAC เองนั้นจะต้องแยกแยะและรู้จักอุปกร์อื่นๆในระบบให้หมดก่อนว่าเป็นอุปกรณ์ชนิดใดบ้าง เช่น PC, Server, Printer, IP Phone, Switch, Router หรือ Access Point แล้วจึงค่อยกำหนดสิทธิ์ต่างๆ ตามนโยบายความปลอดภัยของบริษัท เช่น การยืนยันตัวตน สิทธิ์การเข้าถึง Server และ สิทธิ์การใช้งาน Protocol ต่างๆ หรือแม่แต่การบังคับลง Software หรือ Patch ต่างๆ ดังนั้นในภาพรวมแล้ว หน้าที่ของ Network Access Control จะถูกจำแนกได้ดังนี้

2.1.1 Automatic Discovery and Classification

ทันทีที่ติดตั้งอุปกรณ์ NAC เข้าไปในระบบเครือข่าย อุปกรณ์ NAC จะค้นหาอุปกรณ์อื่นๆในระบบมาแสดงเป็นภาพรวม และจากนั้นค่อยทำการจำแนก เพื่อแบ่งประเภทอุปกรณ์ออกจากกันว่าเป็น PC ที่ติดตั้ง OS ชนิดใด หรือเป็นอุปกรณ์ Network ในบางกรณีเราอาจติดตั้งระบบ NAC เข้าไปเพื่อวัตถุประสงค์ทางด้าน Discovery เป็นหลักเนื่องจากความหลากหลายของอุปกรณ์ Network ในระบบ ซึ่งเป็น Solution ที่ทำให้ผู้ดูแลระบบเห็นภาพรวมของระบบเครือข่าย

2.1.2 Identity-based Policy Enforcement

กำหนดนโยบายความปลอดภัยต่างๆ ในรูปแบบ Identity-based โดยนำข้อมูลจากการค้นหาและจำแนกในข้อที่แล้ว มาบังคับใช้ต่อว่าอุปกรณ์ประเภทไหนจะมีสิทธิ์เข้าถึงระบบเครือข่ายมากน้อยแค่ไหน และอุปกรณ์ประเภทไหนจะต้องทำการยืนยันตัวตนด้วยวิธีการแบบใดบ้าง ไม่ว่าจะเป็น Mac Authentication, 802.1X หรือ Web Authentication ก็ตาม และจะยืนยันกับฐานข้อมูลใด เช่น Microsoft AD, LDAP, RADIUS, Novell หรือ Local Databaseในบางองค์กร อาจมีการกำหนดนโยบายแยกตามผู้ใช้งานตามแผนก โดยมีการดึงข้อมูลจาก AD หรือ LDAP มาช่วยจำแนก หรือให้อุปกรณ์ NAC จำแนกให้เองก็ได้ โดยเฉพาะอย่างยิ่งภายในองค์กรที่พนักงานมีการย้ายสถานที่ทำงานบ่อยๆ จนไม่สามารถจะ Fix IP หรือ VLAN ให้ผู้ใช้งานแต่ละคนได้ เพื่อให้ผู้ใช้งานแต่ละแผนกมีสิทธิ์ในการเข้าถึงข้อมูลที่แตกต่างกัน

2.1.3 Network-based Policy Enforcement

กำหนดสิทธิ์ในการเข้าถึงระบบเครือข่ายของผู้ใช้งานแบบรายบุคคลได้ คล้ายกับการตั้ง Firewall ไว้ด้านหน้าเครื่อง PC หรือ Notebook ในส่วนที่ผู้ดูแลระบบต้องเรียนรู้คือ วิธีที่ใช้ในการควบคุมสิทธิ์ชอง NAC แต่ละยี่ห้อ ซึ่งแต่ละยี่ห้อเองก็จะมีวิธีการในการบังคับต่างกันไป เช่น Switch Control, Firewall Control, 802.1x เป็นต้น

2.1.4 Application-based Policy Enforcement

กำหนดสิทธิ์การใช้งานในระดับ Application ของผู้ใช้งานระบบ โดยการติดตั้ง Agent Software เพื่อให้อุปกรณ์ได้มีการติดตั้งและใช้งาน Software ที่จำเป็นต่างๆ เช่น Antivirus, PC Management และให้หยุดใช้งานโปรแกรมที่ผิดนโยบายขององค์กร เช่น Bit torrent เป็นต้น

2.1.5 IPS-based Policy Enforcement

ตรวจจับการโจมดีระบบเครือข่ายจากผู้ใช้งานแต่ละคนได้ ไม่ว่าจะเป็นการโจมตีโดยตั้งใจ หรือการโจมตีที่ไม่รู้ตัวอันเกิดจากไวรัส แล้วนำข้อมูลไปใช้เพื่อทำการกำหนดสิทธิ์ที่แน่นหนามากยิ่งขึ้น เช่น การห้ามใช้ Protocol หรือการห้ามเข้าถึง Server

2.1.6 Real Time Monitoring and Reporting

สามารถ Monitor ระบบได้อย่าง Real-Time เพื่อให้ผู้ดูแลระบบสามารถติดตามและแก้ไขปัญหาได้ทันท่วงที รวมถึงสรุปเหตุการณ์ต่างๆที่เกิดขึ้นเพื่อนำไปวิเคราะห์ข้อมูลต่อไป

2.2 NAC Architecture

สามารถแบ่งออกได้เป็น 2 ประเภท ได้แก่

2.2.1 Inline NAC

เป็น NAC ที่ติดตั้งขวางเส้นทางการส่งข้อมูลของเครือข่าย เช่นเดียวกับ Firewall ทำให้พบปัญหาที่จะทำให้ระบบเครือข่ายทำงานช้าลง หรือหากอุปกรณ์ NAC มีปัญหาจะส่งผลกระทบทำให้ Network หยุดทำงาน เว้นแต่จะทำการติดตั้งแบบ Redundancy ซึ่งก็มีค่าใช้จ่ายสูงตามมา

2.2.2 Out-of-Band NAC

เป็น NAC ที่มีการติดตั้งในรูปแบบที่ไม่ขวางเส้นทางการส่งข้อมูลของระบบเครือข่าย เพื่อให้ระบบทำงานด้วยความเร็วปกติในขณะทำการควบคุมสิทธิ์การเข้าใช้งานระบบ โดย Out-of-Band NAC ถูกสร้างขึ้นมาหลากหลายเทคโนโลยี โดยแบ่งเป็นวิธีต่างๆได้ดังนี้

- Virtual Firewall สามารถควบคุมสิทธิ์การของผู้ใช้งานแต่ละคน โดยการสร้าง Firewall เสมือนขึ้นมา โดยไม่จำเป็นต้องแก้ไขค่า Configuration ของอุปกรณ์เครือข่ายใดๆ

- 802.1X เป็นหนึ่งในมาตรฐานที่มีใน NAC ทุกยี่ห้อ โดยการตั้งค่านั้นต้อง 802.1X ต้องทำการ Config ทุก Port ของ Switch ที่มีอุปกรณ์ที่ต้องการควบคุมเชื่อมต่ออยู่ แล้วกำหนดให้ NAC ทำหน้าที่เป็น RADIUS Proxy เพื่อคอยรับข้อมูลการยืนยันตัวต้นและกำหนด VLAN ของแต่ละคน
- Stateful DHCP ป็นการติดตั้ง Agent บน DHCP Server เพื่อให้ทำการตรวจจับเมื่อมีการร้องขอ DHCP ว่าเป็นเครื่องที่อยู่ในระบบหรือไม่ ถ้าใช่ก็ให้ทำการแจก IP Gateway หลักไป แต่ถ้าไม่ใช่ก็ให้ทำการแจก IP Gateway สำหรับ Guest เพื่อให้ผ่านกระบวนการทางด้านความปลอดภัยต่อไป
- Switch Control / Firewall Control เป็นการใช้ SNMP เพื่อให้ NAC สามารถทำการแก้ไขค่า ACL ของ Switch หรือ Firewall ได้ เพื่อให้ Switch และ Firewall เป็นตัวช่วยในการกำหนดสิทธิ์สำหรับผู้ใช้งานแต่ละคน

2.3 Network Access Server

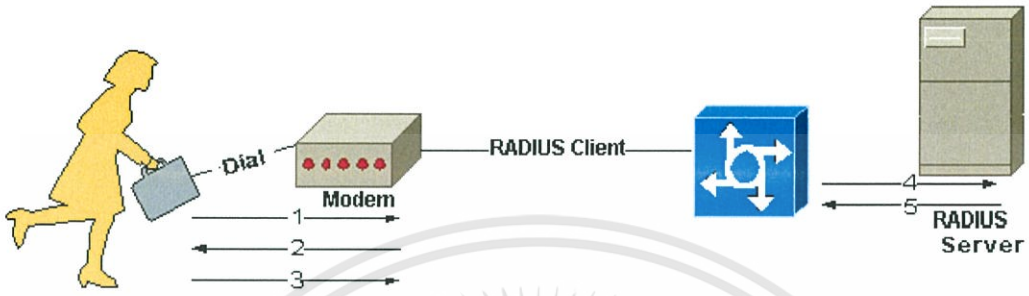
Network Access Server (NAS) เป็นระบบที่ให้บริการการเชื่อมต่อเข้าสู่เครือข่าย ในบอกกรณีอาจเรียกได้ว่าเป็น Gateway ระหว่าง User และระบบเครือข่าย เมื่อ User ต้องการที่จะเข้าสู่ระบบเครือข่าย NAS จะทำหน้าที่ส่งผ่านข้อมูลการยืนยันตัวตนระหว่าง User กับ Radius Server กระบวนการนี้เรียกว่า Authentication Session และในขณะที่สิ้นสุดกระบวนการ Radius Server จะทำการสั่งให้ NAS ปฏิเสธ User และละทิ้งการเชื่อมต่อเข้าระบบเครือข่าย หรือ ทำการยอมรับ User ในการเข้าสู่ระบบเครือข่าย และเมื่อ User ทำการเชื่อต่อเข้าสู่ระบบเครือข่ายเรียบร้อยแล้ว ข้อกำหนดด้านความปลอดภัยที่ได้ถูกกำหนดไว้ จะมีการบังคับใช้ได้โดย NAS ที่ทำหน้าที่เปรียบเสมือน Gateway Router และ Firewall สำหรับ User นั้น

2.4 RADIUS

RADIUS (Remote Authentication Dial-In User Service) เ ป็ น Networking Protocol ที่ให้บริการศูนย์กลางการ Authentication, Authorization, Accounting หรือที่เรียกว่า AAA (Triple A) ทำหน้าที่จัดการ User ที่เชื่อมต่อและเข้าใช้บริการระบบเครือข่าย RADIUS นั้นได้พัฒนาขึ้นโดย Livingston Enterprises Inc. ในปี คริสต์ศักราช 1991 และหลังจากนั้นได้นำเข้าสู่ Internet Engineering Task Force (IETF) standards

RADIUS เป็น Client/Server Protocol ที่ทำงานบน Layer ที่ 7 หรือ Application Layer ของระบบ OSI Model และใช้ได้ทั้ง Protocol TCP และ UDP ในการสื่อสาร โดยปกติแล้ว RADIUS client มักจะเป็น NAS และ RADIUS server จะเป็นกระบวนการที่ทำงานอยู่ UNIX หรือ Window NT โดย RADIUS client นั้นจะทำการส่งข้อมูลของ User ไปยัง RADIUS server ที่กำหนดและ

ทำการตอบสนองตามข้อมูลที่ตอบกลับมา โดย RADIUS sever จะรับคำขอเพื่อเชื่อมต่อจาก User จากนั้นจะทำการยืนยันตัวตนให้กับ User และทำการส่งค่า Configuration ที่จำเป็นสำหรับ RADIUS client เพื่อให้บริการกับ User



รูป 2.1 การติดต่อระหว่าง User และ RADIUS client/server

1. User เริ่มกระบวนการ Point-to-Point Authentication ไปยัง NAS
2. NAS จะแจ้งเตือนเพื่อทำการรับข้อมูล User และ Password (ถ้าใช้ Protocol แบบ Password Authentication Protocol [PAP]) หรือ แบบ Challenge
3. User ทำการตอบกลับ
4. RADIUS client ส่ง Username และ Password ที่ทำการเข้ารหัสแล้วไปยัง RADIUS server
5. RADIUS server ทำการตอบกลับด้วย การยอมรับ หรือปฏิเสธ
6. RADIUS client จะกระทำตาม service และ service parameters

ข้อดีของ RADIUS

- สามารถตรวจสอบได้ว่ามีเข้าใช้งานเครือข่ายบ้าง
- ตรวจสอบ User ที่เข้ามาใช้งานเครือข่ายได้แบบ Real-Time
- มีการเก็บประวัติการเข้าใช้งานสามารถมาเลือกดูในภายหลังได้

2.5 TACACS+

Terminal Access Controller Access-Control System เป็น protocol ของ cisco ที่ใช้งานในรูปแบบของ Access control ของอุปกรณ์เน็ตเวิร์คเฉพาะ cisco เท่านั้น เป็นการพัฒนาเพิ่มขึ้นมาจาก RADIUS โดนเพิ่มความสามารถของ AAA ให้มีความเหมาะสมมากยิ่งขึ้น โดย TACACS+ จะใช้งาน TCP Port 49 และมีความน่าเชื่อถือในการเชื่อมต่อสูง เพราะต้องการความถูกต้องและความสมบูรณ์ของข้อมูล

2.6 MAC Authentication

เป็นการยืนยันตัวตนรูปแบบหนึ่ง ที่เป็นความนิยมเป็นอย่างสูง ซึ่งเป็นการยืนยันตัวตนที่สะดวกต่อการใช้งานเป็นอย่างมากเนื่องจากไม่ต้องใส่ Username และ Password ทุกครั้งที่เชื่อมต่อกับระบบ แต่ว่าอาจจะมีช่องโหว่ที่เป็นความเสี่ยงในการใช้งานอยู่บ้าง MAC Authentication จึงเหมาะกับระบบเครือข่ายขนาดเล็กที่มีการยืนยันตัวตนแบบง่ายๆ ไม่มีการเพิ่มอุปกรณ์เข้ามาในระบบมาก และระบบมีความนิ่งในระดับหนึ่งแล้ว หรือเป็นการใช้เพื่อเป็นการชั่วคราวสำหรับการเปลี่ยนไปใช้ระบบใหม่ที่ใหญ่และจัดการง่ายยิ่งขึ้นกว่าเดิม

2.7 มาตรฐาน 802.1X

มาตรฐาน 802.1X หรือที่เรียกกันอีกอย่างหนึ่งว่า dot1X(ดอทวันเอ็กซ์) เป็นมาตรฐานที่มีอยู่บนทั้งอุปกรณ์ Switch และ Wireless Access Point เพื่อใช้ในการยืนยันตัวตนก่อนเข้าใช้งานได้ตั้งแต่เริ่มต้นเชื่อมต่อกับระบบเครือข่ายโดยทันที โดยเมื่อมีผู้ที่ต้องการเข้าใช้เครือข่าย จะต้องมีการแสดงหลักฐานสำหรับประกอบการตรวจสอบ (credential) ต่ออุปกรณ์แม่ข่าย จะนั้นจะมีการส่งผ่านหลักฐานเหล่านั้นไปยัง RADIUS server โดยการแลกเปลี่ยนข้อมูลกันระหว่าง RADIUS server และอุปกรณ์แม่ข่ายจะเป็นไปตาม Protocol EAP (Extensible Authentication Protocol) โดยในปัจจุบันมีการใช้ Protocol ดังกล่าว 4 รูปแบบหลักๆ คือ

- EAP-MD5
- LEAP
- EAP-TLS
- EAP-TTLS

2.8 AAA (triple A)

AAA ทำให้ไฟร์วอลสามารถระบุได้ว่ายูสเซอร์ที่เข้ามาใช้งานนั้นเป็นใคร (Authentication), ยูสเซอร์นั้นสามารถทำอะไรหรือเข้าถึงข้อมูลได้มากแค่ไหน (Authorization) และยูสเซอร์นั้นทำอะไรไปบ้างในการเข้ามาใช้งานเครือข่าย (Accounting)

2.6.1 Authentication

การทำ Authentication หรือในภาษาไทยคือการยืนยันตัวตนนั้นจะควบคุมการเข้าถึงต่างๆโดยจะต้องมีการยืนยันโดยทั่วไปแล้วนั้นจะเป็น username และ password โดยสามารถให้เซอร์วิสดังต่อไปนี้มีการยืนยันตัวตนก่อนที่จะเข้าใช้งานได้เช่น Telnet , SSH , Serial console , VPN และ Network access

2.6.2 Authorization

Authorization หรือการระบุสิทธิ์ในการเข้าถึงจะเป็นการควบคุมแต่ละยูสเซอร์หลังจากได้ทำการยืนยันตัวตนแล้ว ทุกๆยูสเซอร์อาจมีสิทธิ์ในการเข้าใช้งานเน็ตเวิร์กเหมือนกันแต่สิทธิ์ในการเข้าถึงอาจไม่เท่ากันยกตัวอย่างเช่น ผู้ดูแลระบบเครือข่ายอาจมีสิทธิ์ในการปรับหรือหรือแก้ไขการตั้งค่าต่างๆของเครือข่ายแต่ยูสเซอร์ทั่วไปนั้นมีสิทธิ์แค่เข้าใช้งานเท่านั้นเป็นต้น

2.6.3 Accounting

เป็นการติดตามทราฟฟิกที่ผ่านตัวอุปกรณ์นั้นๆเช่นไฟร์วอลหรือเปรียบเสมือนการเก็บ log ของแต่ละยูสเซอร์ จำเป็นต้องมีการยืนยันตัวตนก่อนถึงจะสามารถเก็บทราฟฟิกที่ยูสเซอร์ใช้งานได้ เนื่องจากอาจเป็นการเก็บข้อมูลตามไอพีแอดเดรส จะเก็บข้อมูลเกี่ยวกับเซสชั่นที่มีการเปิดใช้งาน เซอร์วิสที่ใช้บริการ ระยะเวลาการใช้งานและปริมาณข้อมูลที่ใช้งาน

2.9 Virtual Machine

Virtual Machine คือระบบปฏิบัติการที่จะจำลองการทำงานของเครื่องคอมพิวเตอร์หรือซอฟท์แวร์ต่างๆลงบนเครื่องคอมพิวเตอร์อีกทีหนึ่ง เปรียบกับว่าเราสามารถแบ่งทรัพยากรของเครื่องคอมพิวเตอร์ 1 เครื่องออกเป็นหลายๆเครื่องได้นั่นเอง ประโยชน์จากการจำลองแบบนี้นั่นก็คือเราจะสามารถประหยัดงบประมาณหรือใช้ทรัพยากรของคอมพิวเตอร์ได้อย่างคุ้มค่าและสะดวกต่อการทดลองทางคอมพิวเตอร์ต่างๆ ยกตัวอย่างเช่น ต้องการที่จะจำลองระบบเครือข่ายขึ้นมา 1 ระบบ เมื่อใช้งาน Virtual Machine ก็ไม่มีความจำเป็นที่จะต้องใช้จำนวนคอมพิวเตอร์ตามจำนวนของอุปกรณ์หรือระบบนั้นๆ อาจใช้เพียง 1 เครื่องและทำการแบ่งทรัพยากรออกเป็นหลายๆส่วนเพื่อให้เพียงพอต่อทุกๆระบบปฏิบัติการนั่นเอง

รูป 2.2 ตัวอย่างหลักการทำงานของ Virtual Machine

บทที่ 3
ขั้นตอนการดำเนินงาน

วิธีการดำเนินสามารถแบ่งออกได้เป็น 3 ส่วนด้วยกันคือ

- จัดเตรียมเครื่องมือและอุปกรณ์ที่ใช้
- ศึกษาข้อมูลการใช้งานของอุปกรณ์และโปรแกรม
- การออกแบบ วิเคราะห์ และติดตั้งระบบ

3.1 จัดเตรียมเครื่องมือและอุปกรณ์ที่ใช้

3.1.1 Cisco Secure Access Control System 5.8

Cisco Secure Access Control System หรือ Cisco ACS เป็นซอฟท์แวร์ตัวหนึ่งของ Cisco ทำหน้าที่เป็น policy-based security server ที่ให้บริการตามรูปแบบมาตรฐานการยืนยันตัวตน, การยืนยันสิทธิ์, และการตรวจสอบการทำงาน (AAA service) ให้กับเครือข่าย Cisco ACS ยังอำนวยความสะดวกแก่ผู้ดูแลระบบสำหรับการจัดการอุปกรณ์เครือข่าย ไม่ว่าจะเป็นผลิตภัณฑ์ของ Cisco เอง หรือจะเป็นอุปกรณ์เครือข่ายของบริษัทอื่นๆ

รูป 3.1 ซอฟท์แวร์ Cisco Secure Access Control System

3.1.2 VMware Workstation

โปรแกรม VMware เป็นโปรแกรมซึ่งใช้ในการสร้าง Virtual Machine (VM) หรือเครื่องคอมพิวเตอร์เสมือน คือ เป็นการสร้างเครื่องคอมพิวเตอร์ขึ้นมาอีกเครื่อง(หรือหลายๆเครื่อง ถ้าแรมมากพอ)ภายในเครื่องของเราเอง ดังนั้นจึงทำให้เราสามารถทดลองใช้งาน OS หรือโปรแกรมอื่นๆที่เราสนใจโดยไม่ต้องทำการ format เครื่องหรือใช้ PC อีกเครื่องหนึ่งมาเพื่อทดสอบระบบที่เราสนใจและ virtual machine ที่กำลังมีการใช้งานอยู่บน VMware สามารถที่จะนำมาใช้งานภายนอกได้จริงในทันที (โดยใช้การ Bridge(Default) หรือ NATออกมาที่ Host ที่ได้ทำการ Run VMware อยู่) ดังนั้นประโยชน์อีกอย่างหนึ่งของ VMware คือสามารถทำการจำลองการทำงานของระบบ Network ได้โดยใช้คอมพิวเตอร์เพียงเครื่องเดียว

รูป 3.2 ซอฟท์แวร์ VMware

3.1.3 ซอฟท์แวร์ GNS3

GNS3 เป็นโปรแกรมจำลองระบบเน็ตเวิร์ค (Network Simulation) ย่อมาจาก Graphic Network Simulator 3 เป็นโปรแกรมที่เลียนแบบการทำงานของซอฟท์แวร์ระบบปฏิบัติการในตัวอุปกรณ์เน็ตเวิร์ค (IOS) โดยซอฟท์แวร์ GNS3 จำลองระบบปฏิบัติการได้ทั้ง Cisco และยี่ห้ออื่นๆ ซึ่งสามารถทำงานได้ใกล้เคียงอุปกรณ์จริงถึง 90%

รูป 3.3 ซอฟท์แวร์ GNS3

3.1.4 โน๊ตบุ๊คใช้สำหรับจำลองระบบเครือข่าย(Simulator) ก่อนที่จะนำไปติดตั้งจริง

รูป 3.4 คอมพิวเตอร์โน๊ตบุ๊ค

3.2 ศึกษาข้อมูลการใช้งานของอุปกรณ์และโปรแกรม

3.2.1 ศึกษาการใช้งานซอฟท์แวร์ VMware

การใช้งานนั้นมีหลากหลายรูปแบบให้เลือกใช้ตามความเหมาะสมของเครือข่ายที่เราต้องการที่จะจำลองขึ้นมา ซึ่งในโครงงานนี้ได้สนใจเพียงบางส่วนนั้นคือ

- ศึกษาวิธีการติดตั้งโปรแกรม
- ศึกษาวิธีการเพิ่มเวอร์ชัวอินเตอร์เฟส (Virtual Interface)

- ศึกษาวิธีการจำลอง OS ต่างๆ
- ศึกษาวิธีการทำงานของเน็ตเวิร์กอินเตอร์เฟสเมื่อใช้ host-only
- ศึกษาวิธีการจัดการทรัพยาของ OS
- ศึกษาวิธีการเชื่อมต่อระหว่างเน็ตเวิร์คอินเตอร์เฟส
- ศึกษาวิธีเชื่อมต่อ OS ที่จำลองไว้ไปยังซอฟท์แวร์ตัวอื่นๆ รวมถึงการตั้งค่าเน็ตเวิร์คอินเตอร์เฟสของ OS นั้น

3.2.2 ศึกษาการใช้งานซอฟท์แวร์ GNS3

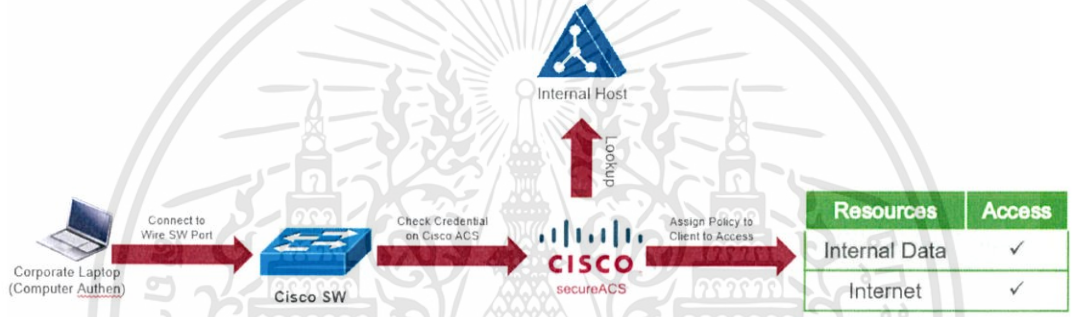
- ศึกษาวิธีการติดตั้งโปรแกรม
- ศึกษาวีธีการจำลองเครือข่าย
- ศึกษาวีธีการนำเข้าระบบปฏิบัติการของอุปกรณ์เน็ตเวิค
- ศึกษาวิธีการเชื่อมต่อของเน็ตเวิร์คอินเตอร์เฟส
- ศึกษาการตั้งค่าเพื่อการให้สามารถเชื่อมต่อระหว่าง VMware และ PC ได้
- ศึกษาการเชื่อมระหว่างเวอร์ชัวอินเตอร์เฟส (Virtual Interface)

3.2.3 ศึกษาการใช้งานซอฟท์แวร์ Cisco ACS 5.8

- ศึกษาการติดตั้งโปรแกรมบน VMware
- ศึกษาการตั้งค่าพื้นฐานของโปรแกรม
- ศึกษาการตั้งค่าเน็ตเวิร์คอินเตอร์เฟส
- ศึกษาการตั้งค่า TACACS+
- ศึกษาการตั้งค่า RADIUS
- ศึกษาการตั้งค่า Identity rule
- ศึกษาการตั้งค่า Command set
- ศึกษาการตั้งค่า User และ Password สำหรับ TACACS+
- ศึกษาการมอนิเตอร์ทราฟฟิกและทำรีพอร์ท

3.3 วิเคราะห์และออกแบบ

โครงงานเป็นการเพิ่มความปลอดภัยสำหรับเครือข่ายที่ได้มีการใช้งานอยู่ และต้องทำการติดตั้งระบบยืนยันตัวนี้เข้าไปตามความต้องการของลูกค้า ซึ่งในขั้นตอนนี้เป็นการวิเคราะห์ระบบเดิมของลูกค้าที่มีอยู่ เพื่อเก็บรวบรวมข้อมูลภาพรวมของระบบทั้งหมดอย่างเช่น มีอุปกรณ์ทั้งหมดจำนวนเท่าไหร่ มีจำนวนผู้ใช้งานปริมาณเท่าไหร่ เพื่อทำการจัดเตรียมอุปกรณ์ต่างๆ การเตรียมการตั้งค่า Configuration ต่างๆ แล้วจึงทำการนำเสนอการทำงานให้กับลูกค้า เพื่อเป็นการพัฒนาระบบให้ดียิ่งขึ้นและใช้เวลาในการติดตั้งให้น้อยที่สุด



รูป 3.5 โครงสร้างของเครือข่ายที่ออกแบบ

จากเครือข่ายที่ได้ออกแบบไว้ข้างต้นได้มีออกแบบ IP Address และ VLAN ที่ใช้ในการทดลองตามตารางดังต่อไปนี้

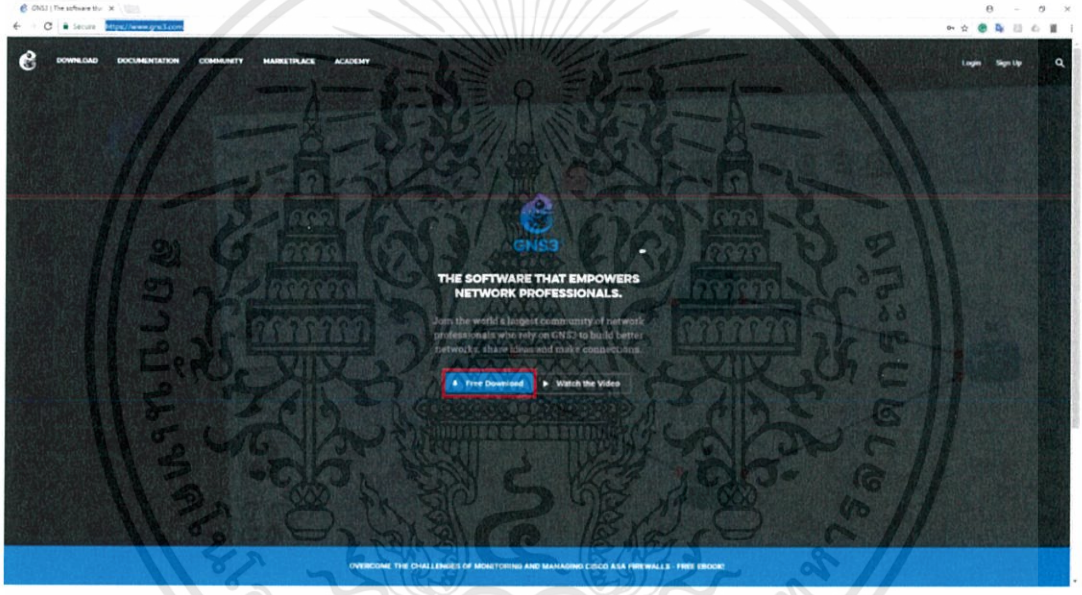
Device	IP Address
Cisco ACS	192.168.50.100
Switch IP	192.168.50.2
Com1	192.168.50.99
Com2	192.168.40.10

ตาราง 3.1 แสดง IP Address ที่ใช้การทดลอง

3.4 ติดตั้ง GNS 3

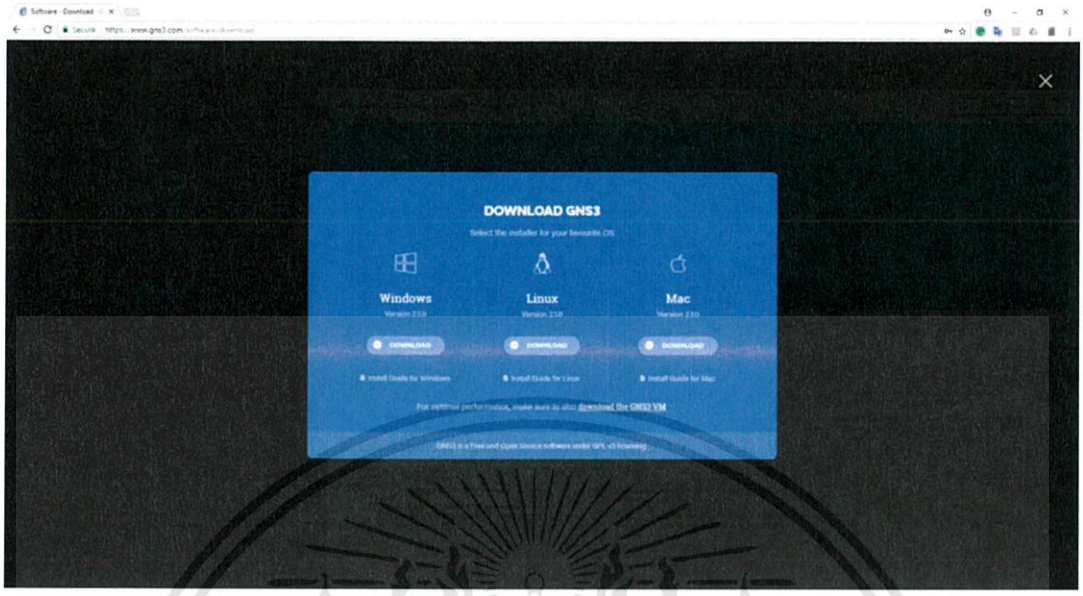
การทดลองนี้เป็นการทดลองเพื่อให้นักศึกษาได้มีความรู้และความเข้าใจในระบบการยืนยันตัวตนสำหรับการเข้าใช้งานระบบเครือข่าย เพื่อให้นักศึกษามีความเข้าใจกระบวนการทั้งหมดและสมารถนำไปใช้ในหน้างานจริงสำหรับบริการลูกค้าได้ และไม่สามารถทอลองได้จากอุปกรณ์จริง จึงต้องทำการติดตั้งโปรแกรมจำลองการทำงานของอุปกรณ์เครือข่ายขึ้นมา โดยมีขั้นตอนดังต่อไปนี้

- ทำการดาวน์โหลดโปรแกรม GNS3 ได้จาก https://www.gns3.com/ จากนั้นเลือกที่ Free Download ในกรอบสีแดงตามรูป 3.4



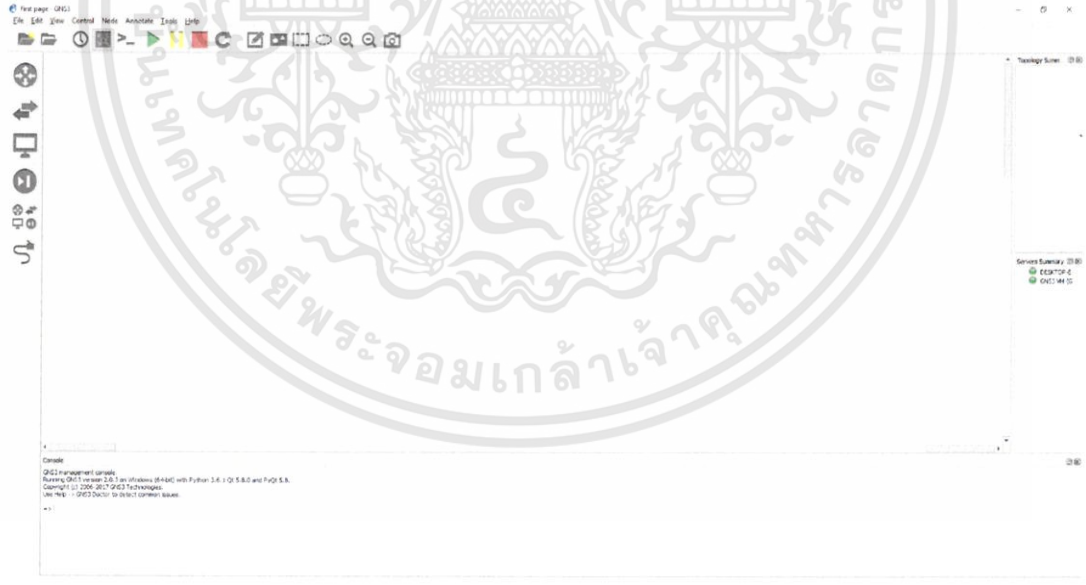
รูป 3.6 หน้าเว็บเพจของ GNS3

- ดำเนินการสมัครสมาชิกตามขั้นตอนให้เรียบร้อย จากนั้นทำการเข้าสู่ระบบจากอีเมล์ที่ได้การสมัครไว้แล้วเลือกดาวน์โหลดไฟล์สำหรับวินโดว์



รูป 3.7 หน้าเว็บเพจของ GNS3 สำหรับการดาวน์โหลดไฟล์

- เมื่อดาวน์โหลดเสร็จแล้วจะได้ไฟล์ชื่อ GNS3-2.0.3-all-in-one ดับเบิลคลิ๊กเพื่อทำการติดตั้ง



รูป 3.8 หน้าต่างโปรแกรม GNS 3

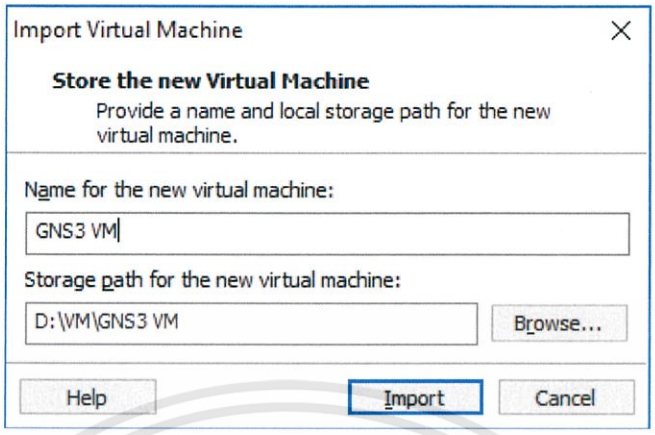
3.5 ติดตั้ง GNS3 VM บน Virtual Machine

โปรแกรมนี้เป็นโปรแกรมสำหรับจำลองอุปกรณ์เน็ตเวิร์คที่นอกเหนือจากตัวโปรแกรม GNS3

- ทำการดาวน์โหลดได้จาก https://www.gns3.com/
- เมื่อดาวน์โหลดเรียบร้อยแล้ว จะได้ไฟล์ GNS3.VM.VMware.Workstation.2.0.3.zip ทำการแตก zip ไฟล์ให้เรียบร้อย จะได้ไฟล์ที่ต้องการคือ GNS3 VM.ova ดังรูป3.8

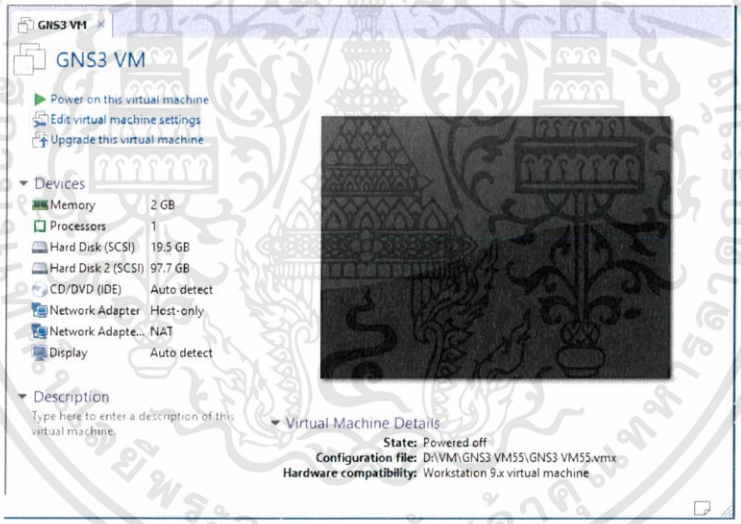
รูป 3.9 ไฟล์ GNS3 VM.ova

- ทำการดับเบิ้ลคลิ๊กที่ไฟล์ GNS3 VM.ova เพื่อทำการติดตั้ง
- จะประกฏหน้าต่างสำหรับการตั้งชื่อ Virtual Machine และ Storage Path ที่ต้องการจัดเก็บ Virtual Machine ดังรูป 3.9
- ในช่อง Name for the new virtual machine เป็นการตั้งชื่อให้กับ Virtual Machine ที่จะติดตั้ง ในที่จะใช้ชื่อว่า “GNS3 VM”
- ในช่อง Strong path for the new virtual machine เป็นการเลือกพื้นที่จะจัดเก็บ Virtual Machine
- จากนั้นคลิ๊กที่ปุ่ม Import



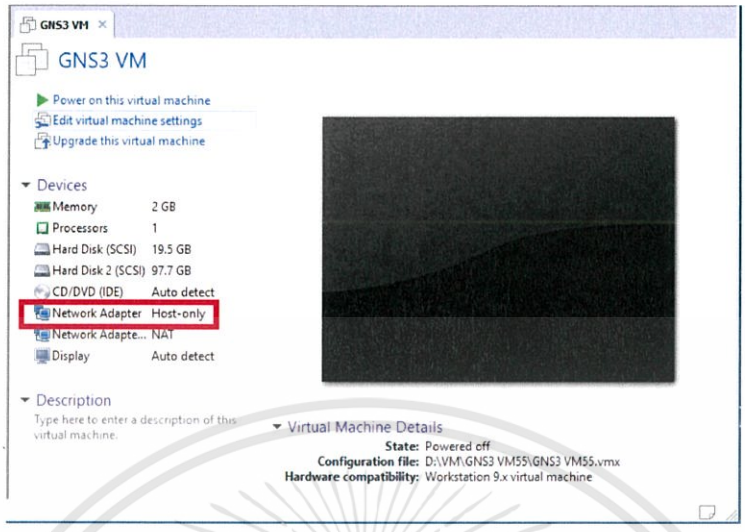
รูป 3.10 ตั้งชื่อ Virtual Machine และเลือก Storage path สำหรับการจัดเก็บ

- เมื่อ Import เสร็จแล้วจะแสดงหน้าต่างดังนี้



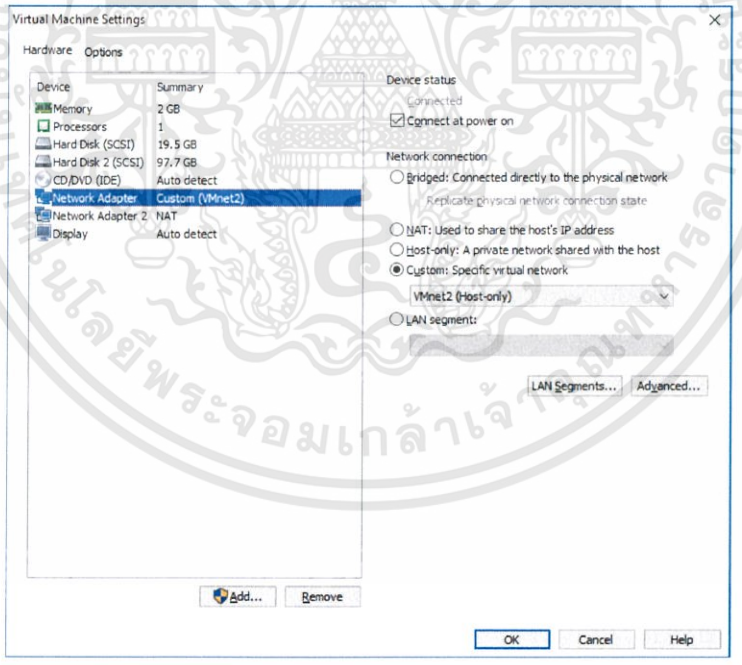
รูป 3.11 GNS3 VM บน Virtual Machine

- ขั้นตอนต่อไปเป็นการตั้งค่า Network Adapter ให้กับ GNS3 VM โดยทำการคลิ๊กที่ Network Adapter ตามกรอบสีแดงดังรูป 3.11



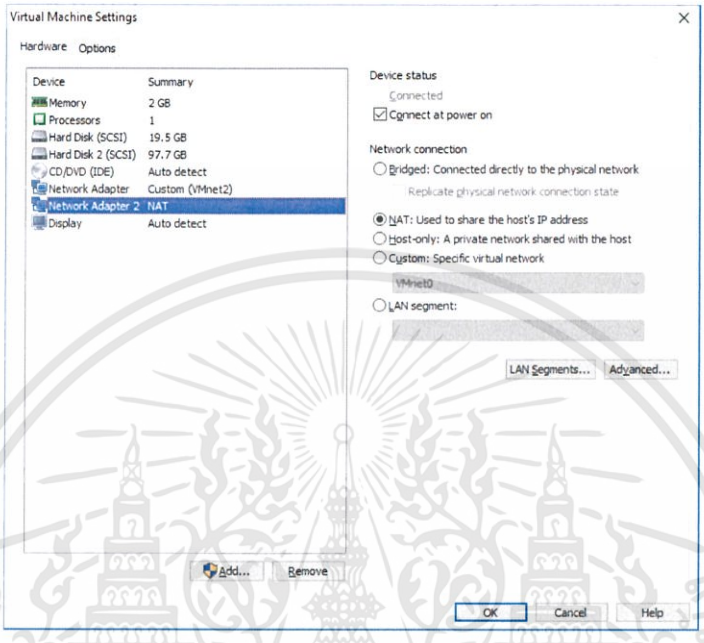
รูป 3.12 ตั้งค่า Network Adapter

- ทำการเลือกที่ Network Adapter Host-only เปลี่ยนการตั้งค่าจากเดิม Host-only เป็น Custom>VMnet2(Host-only) จากนั้นกด OK



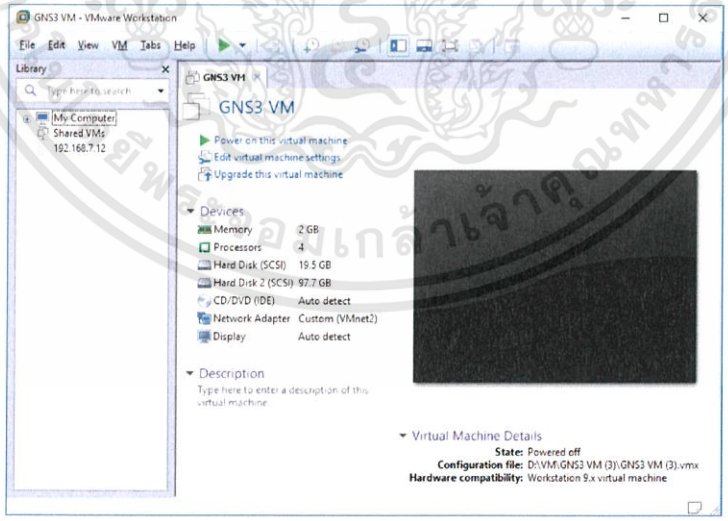
รูป 3.13 เปลี่ยนการตั้งค่า Network Adapter จาก Host-only เป็น Custom

- และเนื่องจากโปรแกรม GNS3 VM ใช้งานเพียง Network Adapter เดียว จึงลบ Network Adapter ที่เราไม่ได้ใช้งานได้ โดยกดที่ “Network Adapter 2 NAT" จากนั้น กด Remove



รูป 3.14 ลบ Network Adapter ที่ไม่ได้ใช้งาน

- ในการเรียกใช้งาน ให้กดที่ปุ่ม Power on this virtual machine



รูป 3.15 การจำลอง Virtual machine เสร็จสมบูรณ์

3.6 การตั้งค่า Virtual Interface

Virtual Interface เป็นการจำลอง Network Adapter ขึ้นมาสำหรับการใช้งาน VMware โดยจะประกอบไปด้วย 3 แบบหลักๆ ดังต่อไปนี้

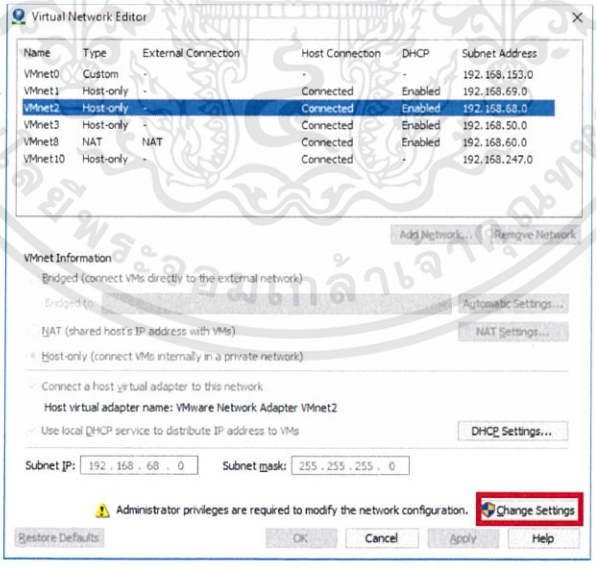
1. Bridge mode จะเป็นการเชื่อมต่อโดยตรงกับเน็ตเวิร์กที่คอมพิวเตอร์ที่รัน VMware ทำงานอยู่โดยจะมีการแจกไอพีแอดเดรสมาให้ตัว virtual machine นี้ด้วย เปรียบเสมือนเป็นคอมอีก 1 เครื่องที่อยู่บนเน็ตเวิร์ก

2. NAT จะทำการแปลงหมายเลขไอพีแอดเดรสจากเน็ตเวิร์กของคอมพิวเตอร์ที่ได้รับมาให้เป็นไอพีแอดเดรสที่เราต้องการยกตัวอย่างเช่นคอมพิวเตอร์เราใช้ 192.168.1.3/24 เราสามารถตั้งค่า NAT ให้เปลี่ยนจาก 192.168.1.3/24 เป็น 10.0.0.3/24 ได้

3. Host-only เป็นการสร้างเน็ตเวิร์กภายในซึ่งจะไม่เกี่ยวข้องกับเน็ตเวิร์กภายนอกที่เชื่อมต่อกับคอมพิวเตอร์ของเครื่องเรา

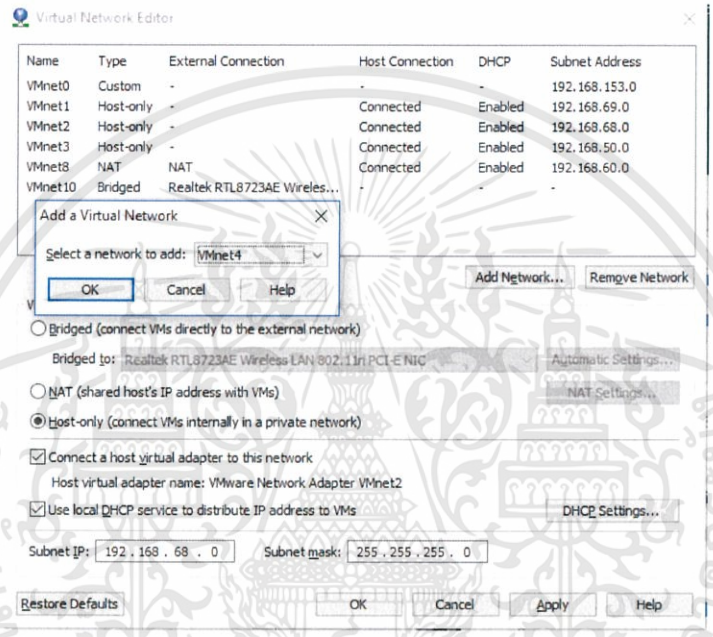
โดยในที่นี้เราจะการตั้งค่าอินเตอร์เฟสทั้งหมด 2 อินเตอร์เฟสสำหรับการนำไปใช้งานในการทดลองครั้งนี้ โดยประกอบไปด้วย GNS3 VM และ Cisco ACS ที่จะพูดถึงในหัวข้อถัดไป

- โดยในการสร้าง Virtual Interface ใน VMware นั้นเราต้องทำตามขั้นตอนดังนี้ เริ่มจาก Edit > Virtual Network Editor > Change Setting



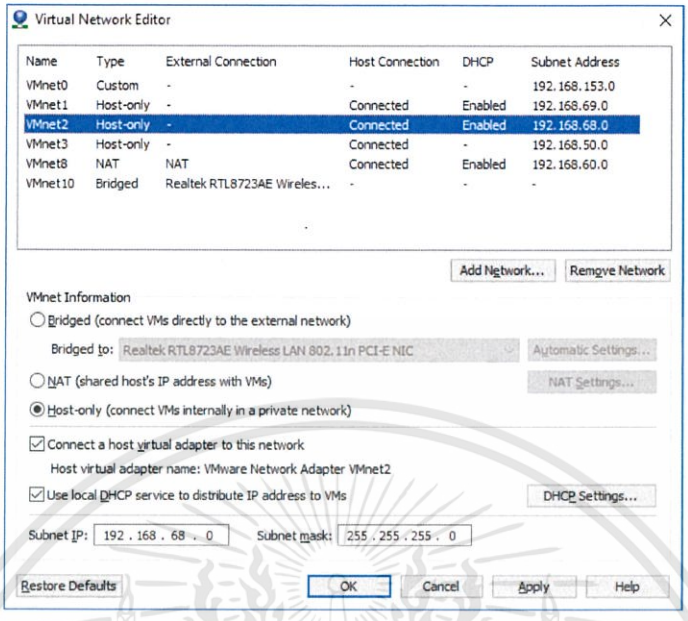
รูป 3.16 หน้าต่าง Virtual Network Editor

- จะเข้ามาสู่หน้าต่างสำหรับการตั้งค่า โดยในหน้านี้จะเป็นการตั้งค่า Network Adapter ทั้งหมด ในการเพิ่ม Network Adapter ทำได้โดยการกดที่ปุ่ม Add Network ปรากฏหน้าต่างดังรูป 3.16 ในช่อง Select a network to add ให้ทำการเลือก Network Adapter ที่ต้องการจากนั้น กด OK ในโครงงานนี้ ใช้ทั้งสิ้น 2 Network Adapter คือ VMnet2 (สำหรับเชื่อต่อ GNS3 VM กับ GNS3) และ VMnet3 (สำหรับ Cisco ACS)



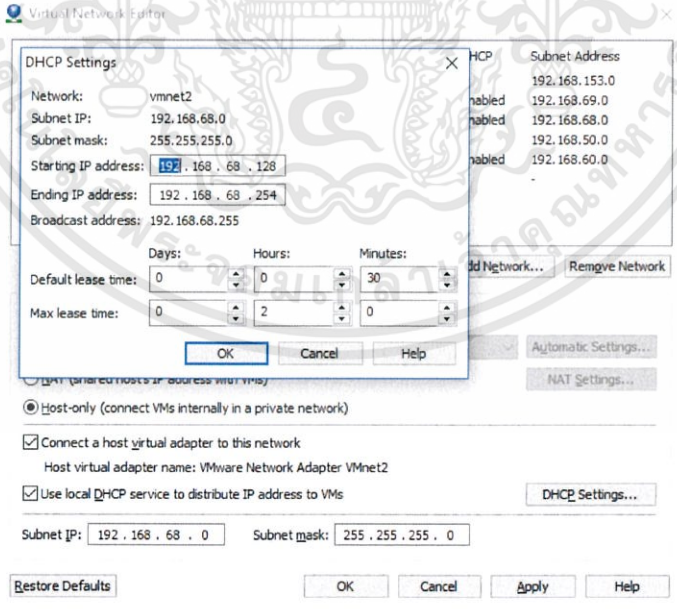
รูป 3.17 หน้าต่าง Add Network

- ต่อไปเป็นการตั้งค่า Network Adapter เริ่มจาก VMnet2 ทำการตั้งค่าเป็นแบบ Host-only และเลือกให้ทำการเชื่อมต่อกับเครื่อง Host ผ่านทาง Virtual Adapter VMnet2 บนเครื่อง Host เลือกใช้เซอร์วิส DHCP และตั้งค่า Network ในวง 192.168.68.0 ซับเนต 255.255.255.0 ดังรูป 3.17



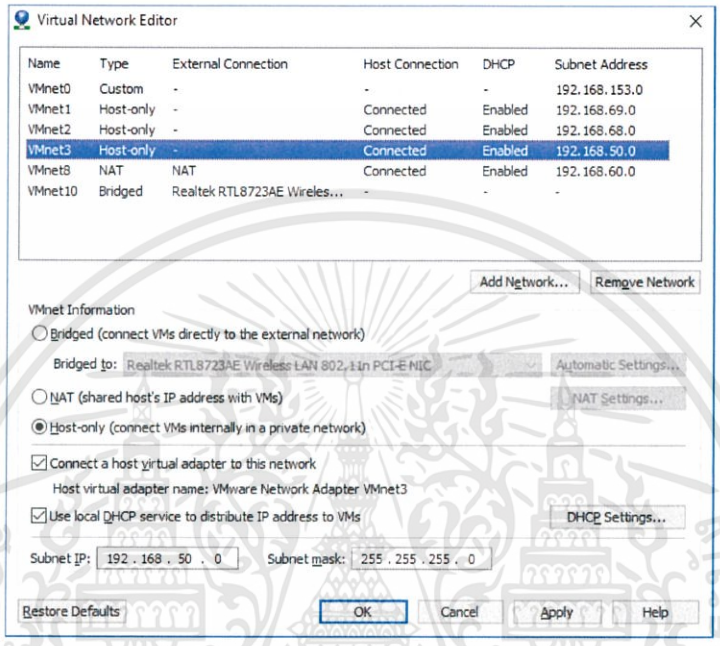
รูป 3.18 ตั้งค่า VMnet2

- การตั้งค่า DHCP กดที่ปุ่ม DHCP Setting จะปรากฏหน้าต่าง DHCP Setting ดังรูป 3.18 ทำการตั้งค่าดังรูป โดยจะเป็นตั้งค่าเพื่อให้แจก IP Address ของวง 192.168.68.0/24 ในช่วง IP ตั้งแต่ 192.168.68.128 ถึง 192.168.68.254 จากนั้นกด OK



รูป 3.19 ตั้งค่า DHCP

- ตั้งค่า VMnet3 ทำการตั้งค่าเป็นแบบ Host-only และเลือกให้ทำการเชื่อมต่อกับเครื่อง Host ผ่านทาง Virtual Adapter VMnet2 บนเครื่อง Host เลือกใช้เซอร์วิส DHCP และตั้งค่า Network ในวง 192.168.50.0 ซับเนต 255.255.255.0 ดังรูป 3.19



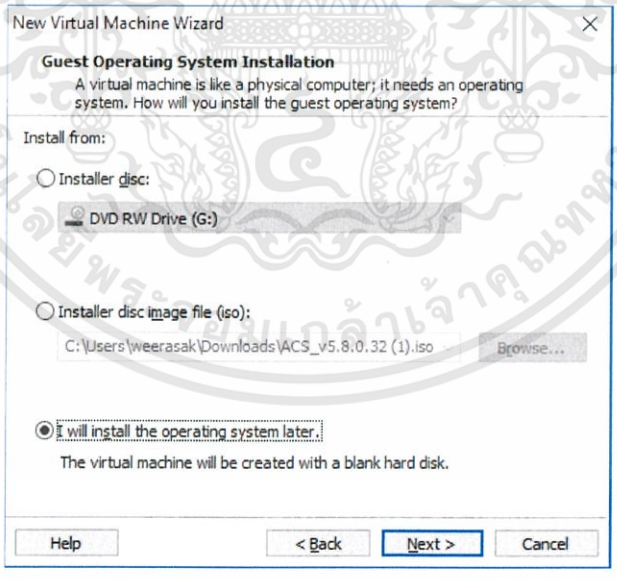
รูป 3.20 ตั้งค่า VMnet3

3.7 ติดตั้ง Cisco ACS บน Virtual Machine

- ดาวน์โหลดโปรแกรม Cisco ACS ได้จาก https://software.cisco.com/download จะได้ไฟล์สกุล (.iso) ชื่อ ACS_v5.8.0.32.iso
- เปิดโปรแกรม VMware Workstation จากนั้นเลือกที่ File > New virtual machine จะปรากฏหน้าต่างดังรูป 3.20 แล้วเลือกที่ Typical แล้วกด Next

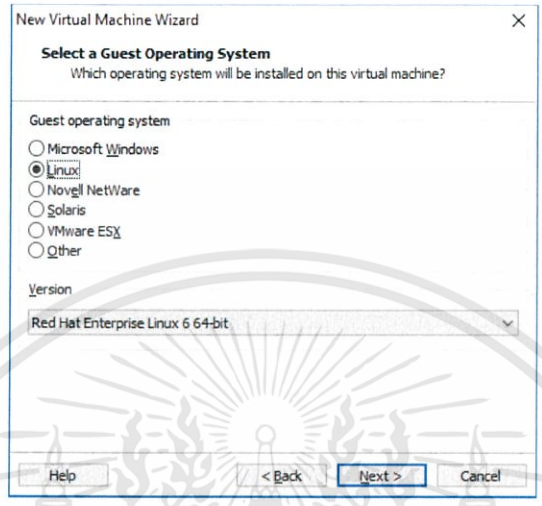
รูป 3.21 การสร้าง virtual machine ขึ้นมาใหม่

- ขั้นตอนนี้จำทำการสร้างเครื่อง virtual machine ที่จะมีเฉพาะระบบปฏิบัติการขึ้นมาโดยยังไม่ทำการติดตั้งตัวโปรแกรมลงไป โดยเลือกที่ I will install the operation system later จากนั้นกด Next



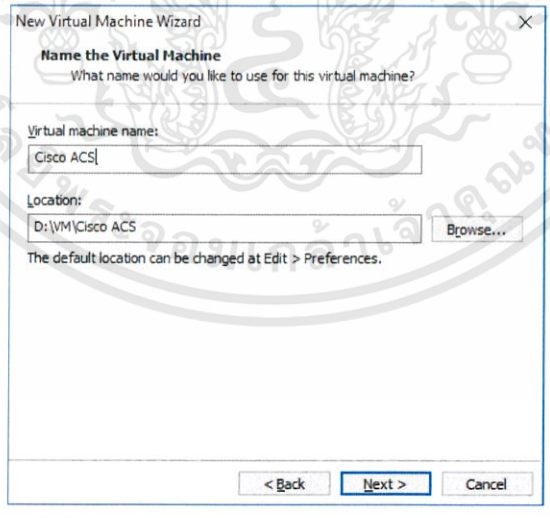
รูป 3.22 การสร้าง virtual machine โดยยังไม่ทำการติดตั้งโปรแกรม

- เลือกระบบปฏิบัติการที่ใช้สำหรับ Cisco ACS โดยจะเลือกใช้ Linux เวอร์ชั่น Red Hat Enterprise Linux 6 64-bit ในการติดตั้งโปรแกรมครั้งนี้ จากนั้นกด Next



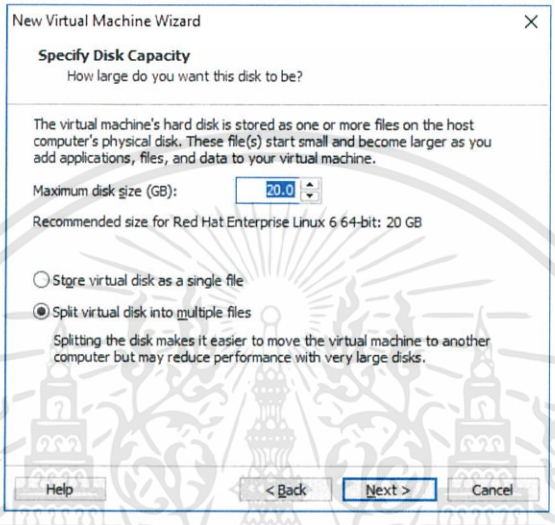
รูป 3.23 เลือกระบบปฏิบัติการสำหรับโปรแกรม Cisco ACS

- ตั้งชื่อ Virtual machine และเลือกพื้นที่สำหรับการจัดเก็บโดยในที่นี้จะใช้ชื่อว่า Cisco ACS ส่วนพื้นที่ในการใช้เก็บไฟล์ควรใช้พื้นที่ว่างที่มีขนาดตั้งแต่ 25 GB เป็นต้นไป เมื่อตั้งชื่อและกำหนดที่จัดเก็บไฟล์เรียบร้อยแล้ว กด Next



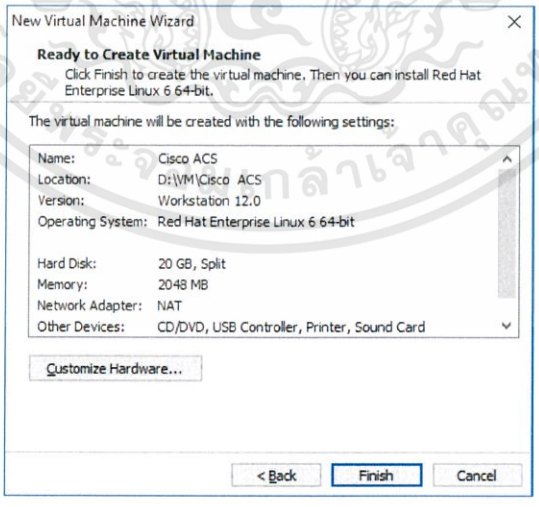
รูป 3.24 เลือกพื้นที่จัดเก็บและตั้งชื่อ Virtual Machine

- เลือกขนาดของพื้นที่จัดเก็บไฟล์ของ Virtual Machine หรือจะเรียกว่าเป็นฮาร์กดิสของ VM เลยก็ได้ โดยจะเป็นการจองพื้นที่ไว้ล่วงหน้าและจะขยายขนาดขึ้นเรื่อยๆจนถึงค่าที่เราตั้งไว้ จะกำหนดไว้ที่ 60 GB และเลือกเป็นแบบ Split virtual disk into multiple file เสร็จเรียบร้อยแล้วกด Next



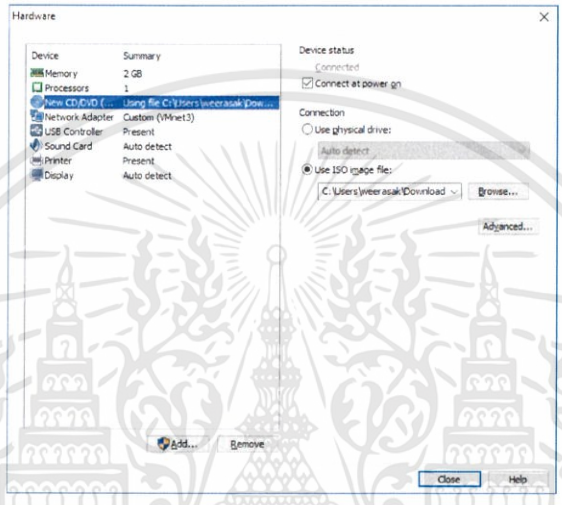
รูป 3.25 ตั้งค่าพื้นที่จัดเก็บไฟล์ของ Virtual Machine

- ต่อไปทำการตั้งค่าสเปคของ Virtual Machine ที่เราจะใช้งานโดยเลือกที่ Customize Hardware

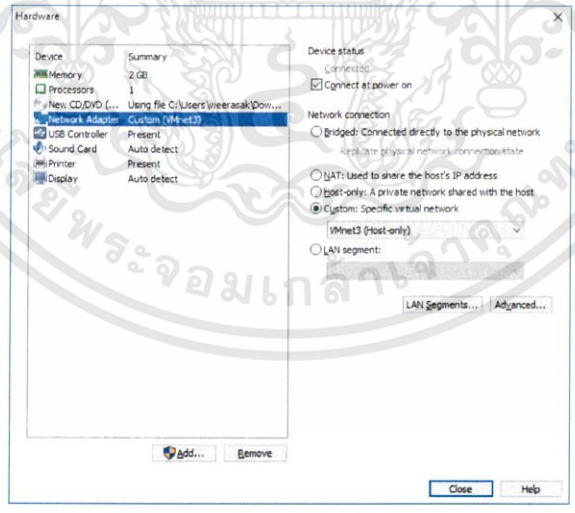


รูป 3.26 ตั้งค่าสเปคพื้นฐานของ Virtual Machine

- เพิ่มแรมจาก 2 GB เป็น 4 GB เพิ่มอิมเมจสำหรับการติดตั้งเข้าไปใน Virtual Machine โดยเลือกที่ New CD/DVD (SATA) > Use ISO image file > Browse และเลือกไฟล์ Cisco ACS ที่เราทำการดาวน์โหลดมาเป็นไฟล์(.ISO) และทำการเปลี่ยน Network Adapter จากเป็น VMmet3 โดยเลือกที่ Network Adapter > Custom > VMnet3(host-only) เมื่อเสร็จเรียบร้อยแล้ว กด Close ตามด้วยกด Finish

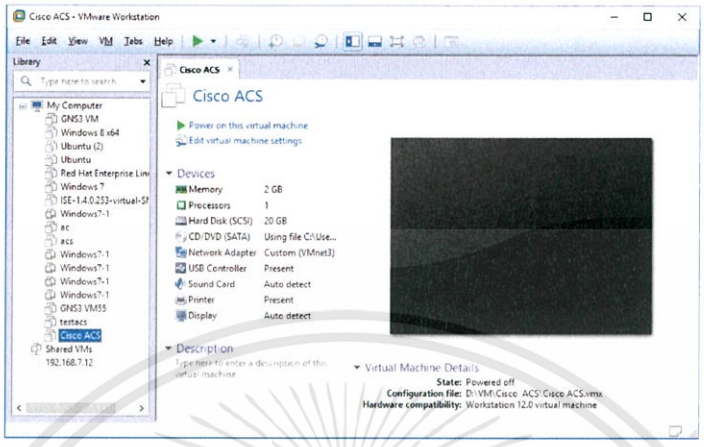


รูป 3.27 เลือกไฟล์ Cisco ACS



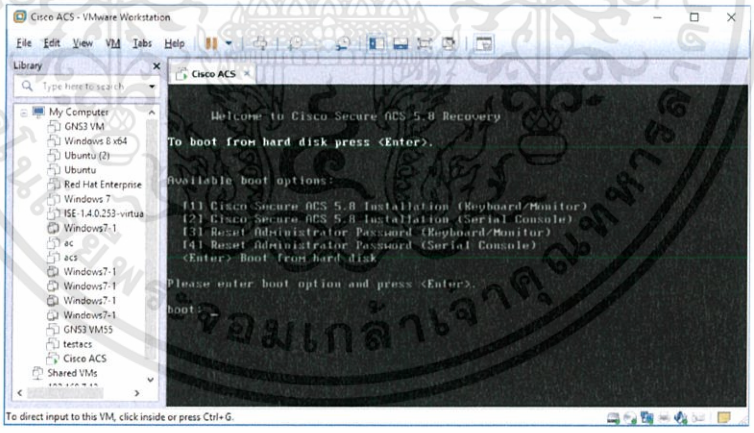
รูป 3.28 ตั้งค่า Network Adapter เป็น VMnet3

- จะได้เครื่อง Virtual Machine ที่พร้อมสำหรับการติดตั้ง Cisco ACS



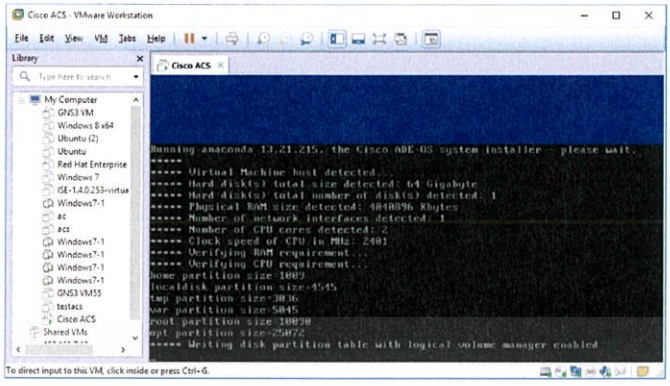
รูป 3.29 เครื่อง virtual machine ที่พร้อมสำหรับการติดตั้ง Cisco ACS

- ทำการเปิด Virtual Machine ที่สร้างขึ้นมาโดยกดที่ปุ่ม Power on this virtual machine
- จากนั้นเครื่อง VM ของเราจะเปิดขึ้นมาแล้วจะถามว่าจะให้เราบูทผ่านตัวเลือกไหน ให้เราทำการเลือก [1] Cisco Secure ACS 5.8 installation (Keyboard/Monitor) โดยพิมพ์ “1” แล้วกด Enter

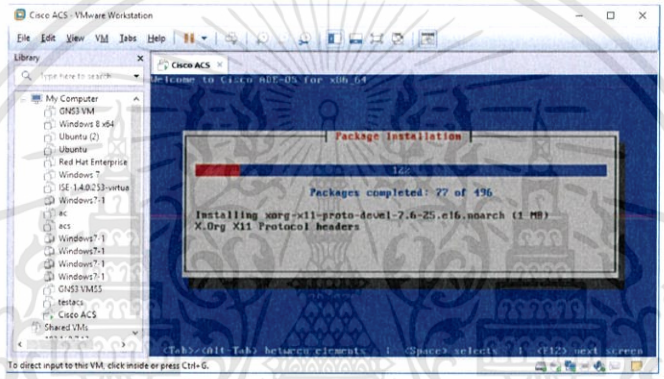


รูป 3.30 หน้าต่างสำหรับเลือก startup boot

- จากนั้นจะเป็นการทำงานของระบบ คือการเช็คค่าที่จำเป็นต่างๆต่อการติดตั้งว่าผ่านตามข้อกำหนดของโปรแกรมหรือไม่

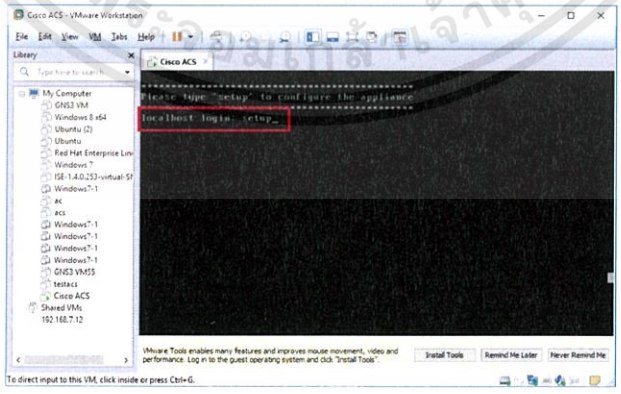


รูป 3.31 ขั้นตอนการตรวจเช็คค่าที่จำเป็นต่างๆ



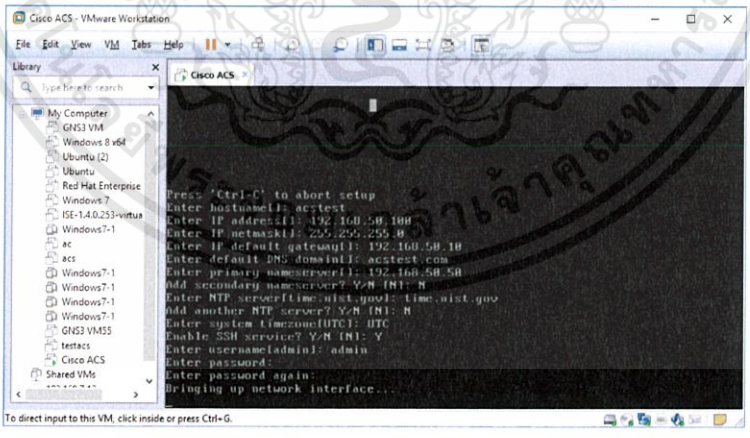
รูป 3.32 หน้าต่างขณะติดตั้งโปรแกรม

- เมื่อติดตั้งเรียบร้อยแล้ว virtual machine จะทำการรีบูท 1 ครั้ง แล้วจะเปิดขึ้นมาเป็นหน้าต่างของโปรแกรม Cisco ACS โดยจะเป็นรูปแบบของ Command line ในการพิมพ์คำสั่งต่างๆ เริ่มต้นให้พิมพ์ว่า “setup” จากนั้นกด Enter เพื่อเริ่มการตั้งค่า



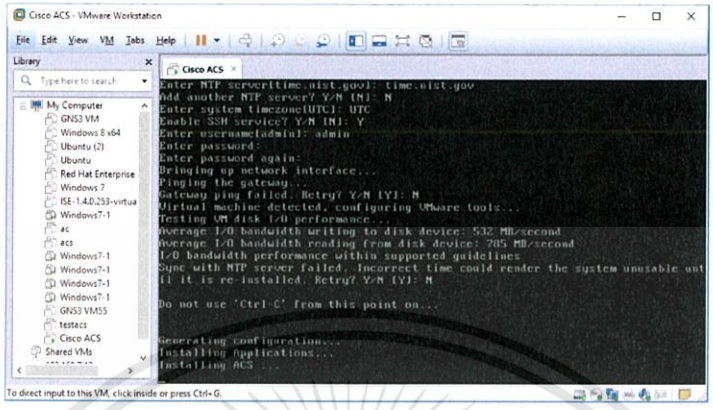
รูป 3.33 หน้าแรกของ Cisco ACS

- โดยในการตั้งค่าต่างๆนั้นให้ตั้งค่าดังต่อไปนี้
    - Enter hostname [ ]: acstest
    - Enter IP address [ ]: 192.168.50.100
    - Enter IP netmask [ ]: 255.255.255.0
    - Enter IP default gateway [ ]: 192.168.50.10
    - Enter default DNS domain [ ]: acstest.com
    - Enter primary nameserver [ ]: 192.168.50.50
    - Add secondary nameserver? Y/N [N]: N
    - Enter NTP server[time.nist.gov]: time.nist.gov
    - Add another NTP server? Y/N [N]: N
    - Enter system timezone[UTC]: UTC
    - Enable SSH service? Y/N [N]: Y
    - Enter username[admin]: admin
    - Enter password: ********
    - Enter password again: *********



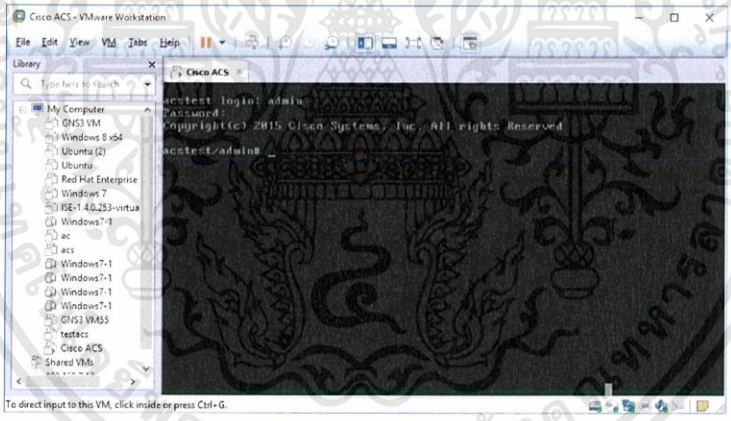
รูป 3.34 ตั้งค่าพื้นฐานต่างๆ

- รอการติดตั้งโปรแกรม ขั้นตอนนี้อาจใช้เวลาประมาณ 20-30 นาที



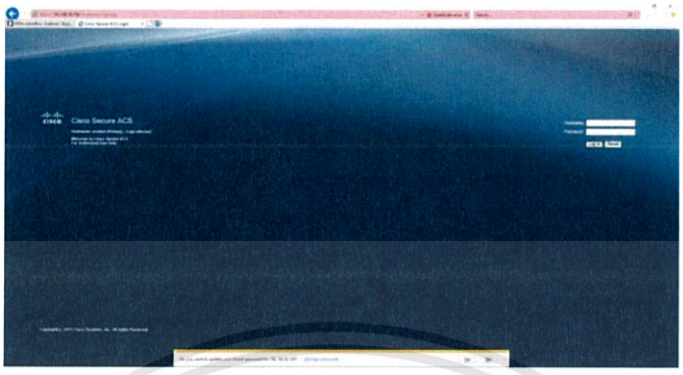
รูป 3.35 ขณะที่โปรแกรมกำลังดำเนินการติดตั้ง

- เมื่อทำการติดตั้งเรียบร้อย จะกลับเข้าสู่หน้า login อีกครั้งนึง ให้ใส่ username และ password ที่กำหนดไว้ จะเข้าสู่หน้า CLI สามารถทำการ Configuration ค่าต่างๆผ่านหน้านี้ได้



รูป 3.36 หน้า CLI ของโปรแกรม Cisco ACS

- นอกจากนี้ยังสามารถเข้าสู่ระบบผ่านทางเว็บอินเตอร์เฟสโดยใช้เว็บบราวน์เซอร์ต่างๆ ในที่นี้จะใช้ Internet explorer ในการใช้งาน โดยเริ่มจากเปิด Internet explorer ขึ้นมา ในช่อง URL ให้ใส่ https://192.168.50.100 จากนั้นกด Enter ในการเข้าใช้งานนี้เป็นการเข้าใช้งานโดยไม่มี security certificate เพราะฉะนั้นให้กดเลือกที่ More information > Go on to the webpage (not recommended)

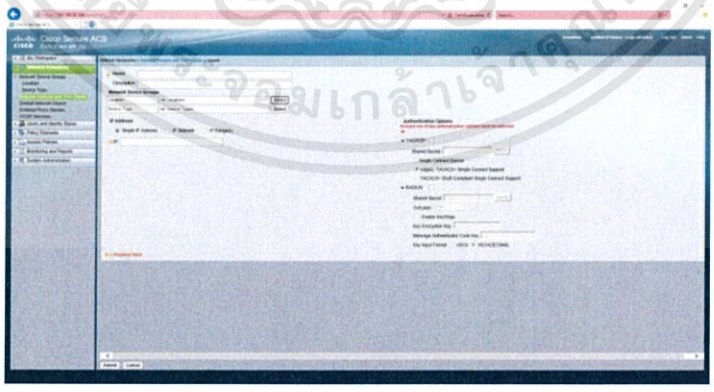


รูป 3.37 หน้า Web Interface ของ Cisco ACS

- ในการเข้าสู่ระบบสำหรับหน้า GUI ในครั้งแรกนั้นให้ใช้งาน username : acsadmin และ password : default จากนั้นจะเข้าสู่ขั้นตอนการตั้งค่าพาสเวิร์ดสำหรับการเข้าใช้งานให้เราทำการตั้งพาสเวิร์ดใหม่ให้เรียบร้อยเพื่อนำมาเข้าใช้งาน
- และในการใช้งานนั้นจำเป็นต้องมีการยืนยันใบอนุญาต โดยในรูปแบบทดลองใช้จะใช้งานได้เพียง 80 วันเท่านั้นโดยการยืนยันสามารถเข้าไปขอใบอนุญาตได้จากเว็บไซต์ของซิสโก้เท่านั้นและต้องใช้บัญชีของทางบริษัทเท่านั้น

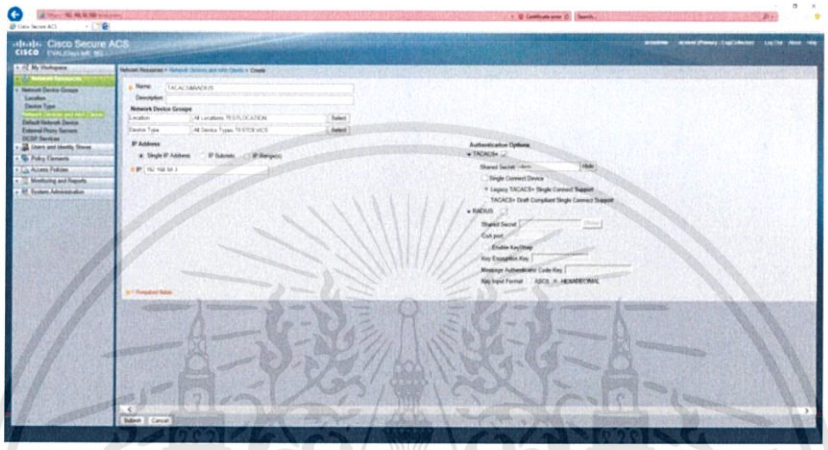
3.8 ตั้งค่า TACACS บน Cisco ACS

- ลงทะเบียนอุปกรณ์ที่ต้องการใช้งานในระบบโดยเลือกที่ Network Devices and AAA Clients > Create



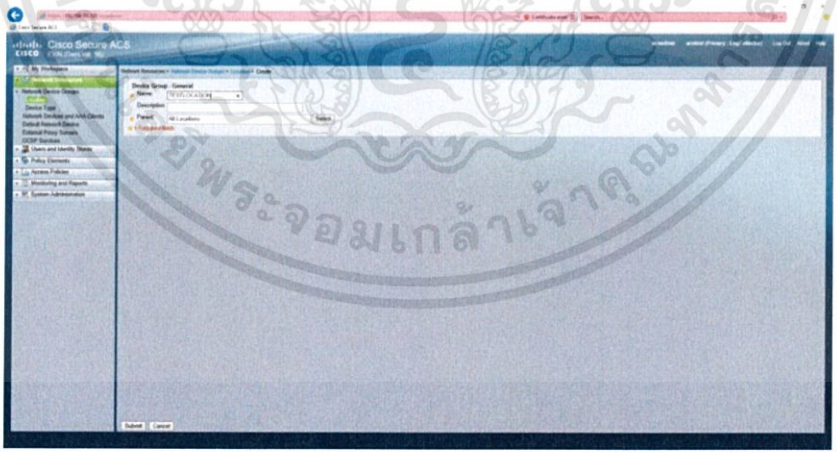
รูป 3.38 การสร้างอุปกรณ์เน็ตเวิร์คที่จะใช้งาน

- ทำการตั้งค่าอุปกรณ์โดย ใส่ชื่อ คำอธิบาย จัดกลุ่มของอุปกรณ์ตามสถานที่และชนิดของอุปกรณ์ ตั้งค่า IP Address ของอุปกรณ์ โดย IP ในที่นี้จะเป็น IP Management ของอุปกรณ์ตัวนั้น และติ๊กที่ช่อง TACACS+ และในช่อง Shared Secret ใส่ว่า “cisco” เมื่อตั้งค่าทุกอย่างเสร็จแล้ว กด Submit



รูป 3.39 การตั้งค่าอุปกรณ์ให้ใช้งาน TACACS+

- การตั้งค่า Location Group ไปที่ Network Resources > Network Device Groups > Location > Create ในช่อง Name ใส่ชื่อ TESTLOACTION จากนั้นกด Submit



รูป 3.40 การสร้าง Location Group

- การตั้งค่า Device Group เข้าไปที่ Network Resources > Network Device Groups > Device Type > Create ในช่อง Name ใส่ชื่อ TESTDEVICE จากนั้นกด Submit

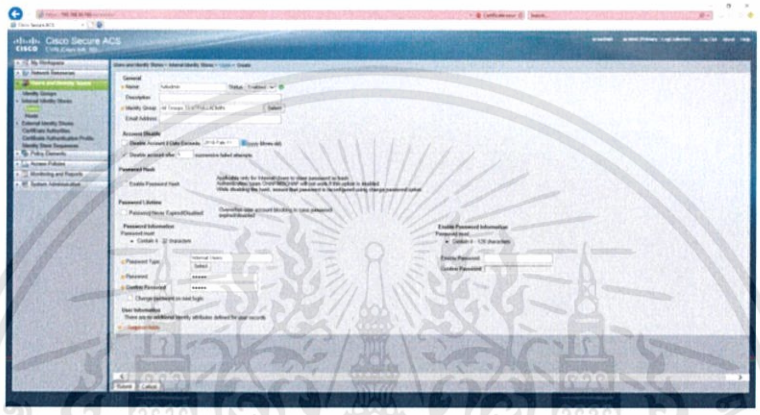
รูป 3.41 การสร้าง Device Group

- ทำการสร้าง User ที่ต้องการใช้งานโดยจะเริ่มจากการสร้างกลุ่มของ User ที่สร้างขึ้นมาโดยไปที่ Users and Identity Stores > Identity Groups > Create ในช่อง Name ใส่ว่า TESTFULLADMIN เป็นการตั้งกลุ่มของ User ที่ชื่อว่า TESTFULLADMIN และทำตามขั้นตอนเดิมอีกครั้งเพื่อสร้างกลุ่ม TESTOPERATOR

รูป 3.42 การสร้าง User Group

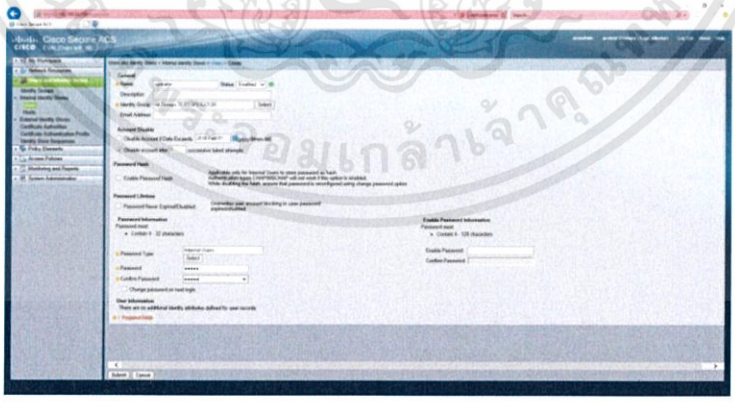
- ทำการสร้าง User สำหรับ Full Admin และ Operator โดยเข้าไปที่ Users and Identity Stores > Internal Identity Stores > Users > Create ที่ช่อง Name ใส่ว่า fulladmin เป็น user ที่ใช้สำหรับการเข้าสู่ระบบ ช่อง Status เลือกเป็น Enable ช่อง Identity Group ทำการ

เลือกให้อยู่ในกลุ่ม TESTFULLADMIN โดยเข้าไปที่ Choose > All Group > ติ๊กช่อง TESTFULLADMIN > OK ในส่วน Account Disable ติ๊กที่ช่อง Disable account after "5"(บอกถึงจำนวนครั้งที่หากใส่รหัสผิดพลาดจะทำการล็อค User) successive failed attempts สุดท้ายส่วนของ Password ช่อง Password Type เลือกเป็น Internal Users ช่อง Password ใส่ว่า cisco และ Confirm Password ใส่ว่า Cisco อีกครั้งหนึ่ง



รูป 3.43 การสร้าง User fulladmin

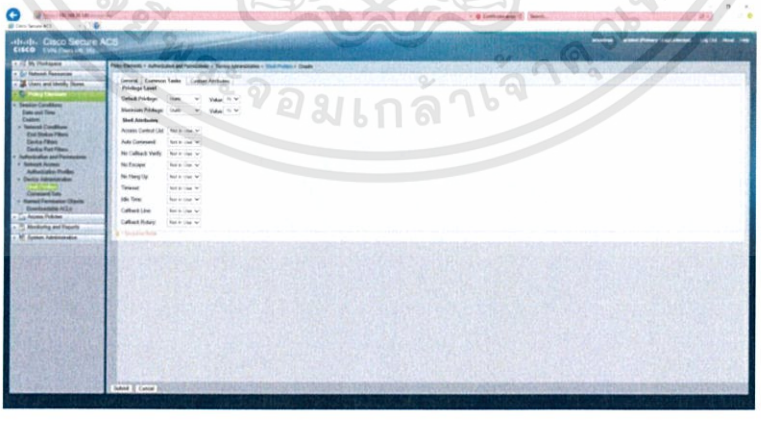
- สำหรับ User ที่ Operator จะใช้ชื่อว่า operator โดยขั้นตอนการสร้างต่างๆจะเหมือนกับ fulladmin โดยในช่อง Name ให้ใส่ว่า operator และ Identity Group เลือกเป็น TESTOPERATOR ส่วนการตั้งค่าที่เหลือจะเหมือนกัน fulladmin ทั้งหมด



รูป 3.44 การสร้าง User operator

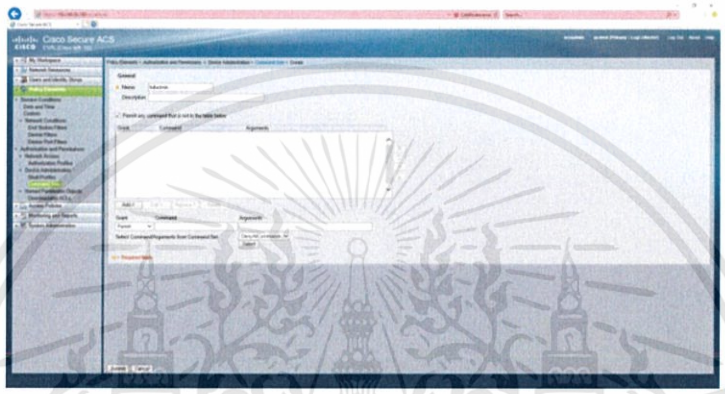
- ตั้งค่า Shell Profile โดยเข้าไปที่ Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Create สำหรับ fulladmin ไปที่แถบ General ช่อง Name ใส่ว่า fulladmin ที่แถบ Common Task ในหัวข้อ Default Privilege เลือกเป็น Static ส่วน Value เลือกเป็น 15 และในหัวข้อ Maximum Privilege เลือกเป็น Static ส่วน Value เลือกเป็น 15 เช่นกัน จากนั้นกด Submit และในส่วนของ operator จะทำการตั้งค่าดังนี้ General ช่อง Name ใส่ว่า operator ที่แถบ Common Task ในหัวข้อ Default Privilege เลือกเป็น Static ส่วน Value เลือกเป็น 5 และในหัวข้อ Maximum Privilege เลือกเป็น Static ส่วน Value เลือกเป็น 5

รูป 3.45 การตั้งค่า Shell Profile(1)



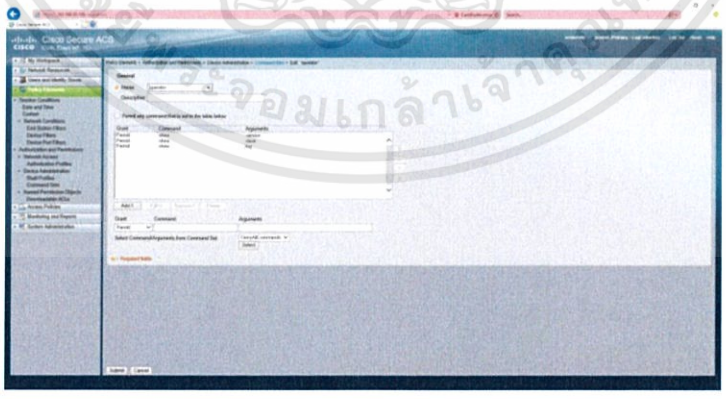
รูป 3.46 การตั้งค่า Shell Profile(2)

- สร้างชุด Command สำหรับแต่ละ User โดยเข้าไปที่ Policy Elements > Authorization and Permissions > Device Administration > Command Sets > Create ในช่อง Name ใส่ว่า fulladmin เป็นการตั้งชื่อชุดคำสั่ง แล้วติ๊กที่ช่อง Permit any command that is not in the table(เป็นการอนุญาตให้ใช้คำสั่งทั้งหมดที่ไม่ได้อยู่ในตารางด้านล่าง ในที่นี้คือการยอมให้ใช้ทุกคำสั่งที่มี) จากนั้นกด Submit



รูป 3.47 การตั้งค่า Command set สำหรับ fulladmin

- และในส่วนของ operator ในช่อง Name ให้ใส่ว่า operator โดยจะให้ใช้คำสั่งได้แค่บางคำสั่งเท่านั้นเช่น show version, show clock, show log เป็นต้น ในช่อง Command ให้ใส่ว่า show และช่อง Argument ใส่ว่า version สำหรับคำสั่ง show version กดนั้นกด Add/\ ทำขั้นตอนนี้อีกครั้งกับคำสั่ง show clock และ show log เมื่อเรียบร้อยแล้ว กด Submit

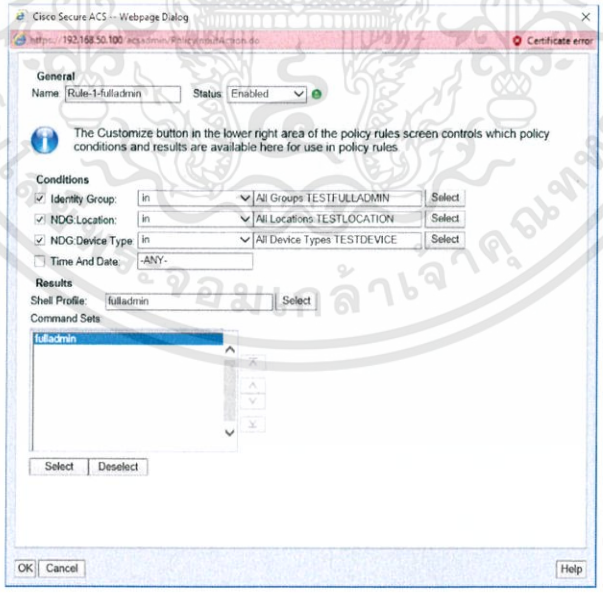


รูป 3.48 การตั้งค่า Command set สำหรับ operator

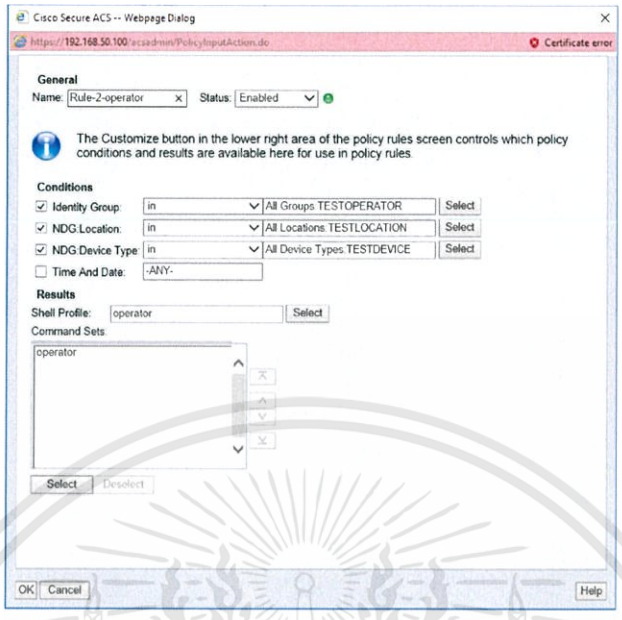
- ตั้งค่า Access Policies สำหรับ TACACS+ ไปที่ Access Policies > Access Services > Default Device Admin > Identity ในช่อง Identity Source เลือกเป็น Internal Users

รูป 3.49 เลือก Identity Source

- สร้าง Authorization Rule โดยไปที่ Access Policies > Access Services > Default Device Admin > Authorization แล้วกด Create ทำการสร้างทั้งหมด 2 Rule สำหรับ fulladmin และ operator โดยทำการตั้งค่าดังรูปที่ 3.45 และ 3.46 เมื่อตั้งค่าทุกอย่างเรียบร้อยแล้วให้กด OK และกด Save Changes เพื่อบันทึกการตั้งค่า

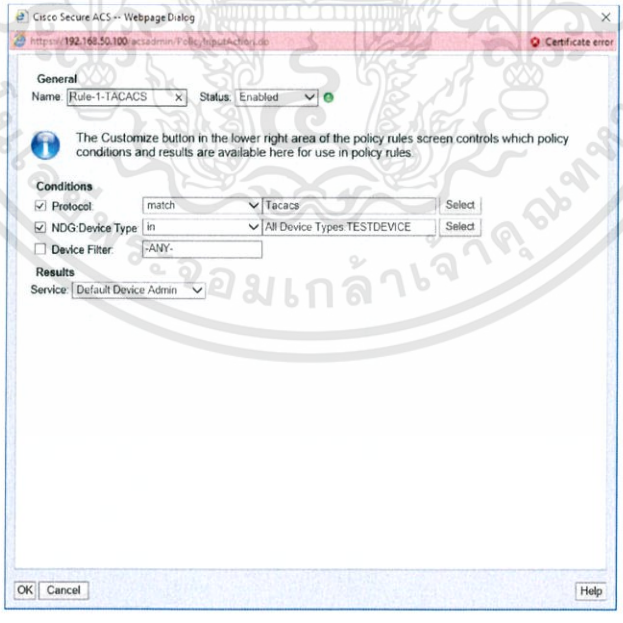


รูป 3.50 สร้าง Authorization Rule สำหรับ fulladmin



รูป 3.51 สร้าง Authorization Rule สำหรับ operator

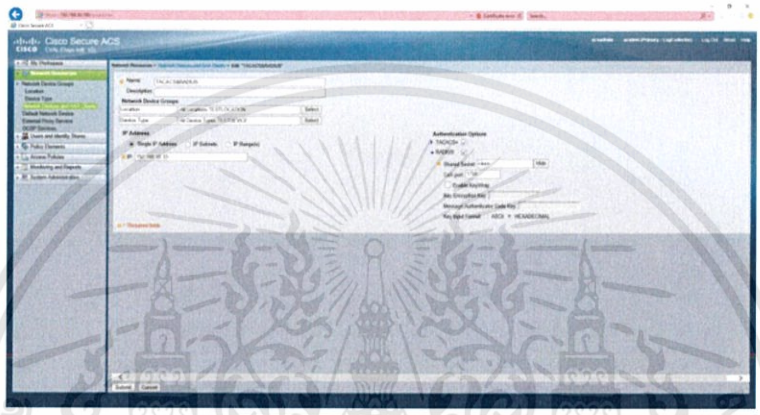
- ตั้งค่า Service Selection Rules โดยเข้าไปที่ Access Policies > Access Services > Service Selection Rules แล้วกด Create และทำการตั้งค่าตามรูป 3.47 เพื่อสร้าง Policy สำหรับ TACACS+ จากนั้นกด OK และ Save Changes เพื่อบันทึกการตั้งค่า



รูป 3.52 สร้าง Service Selection Rules

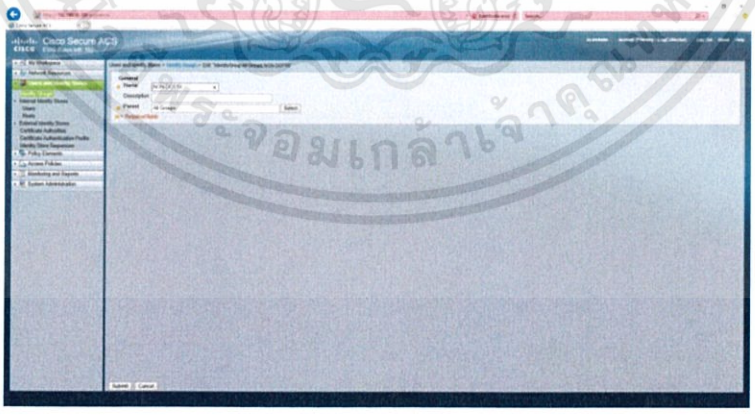
3.9 ตั้งค่า RADIUS บน Cisco ACS

- โดยในเริ่มต้นต้องทำการเพิ่มอุปกรณ์ที่จะใช้งาน RADIUS เข้าไปในระบบก่อน ซึ่งในการเพิ่มอุปกรณ์เข้าไปนั้นจะเหมือนกับการเพิ่มอุปกร์ของ TACACS+ ให้หัวข้อที่ 3.8 แต่จะการเพิ่มฟังก์ชันการใช้งาน RADIUS เขาไป โดยในหัวข้อ Authentication Option ให้ติ๊กถูกที่ช่อง RADIUS และใส่ Share Secret : cisco



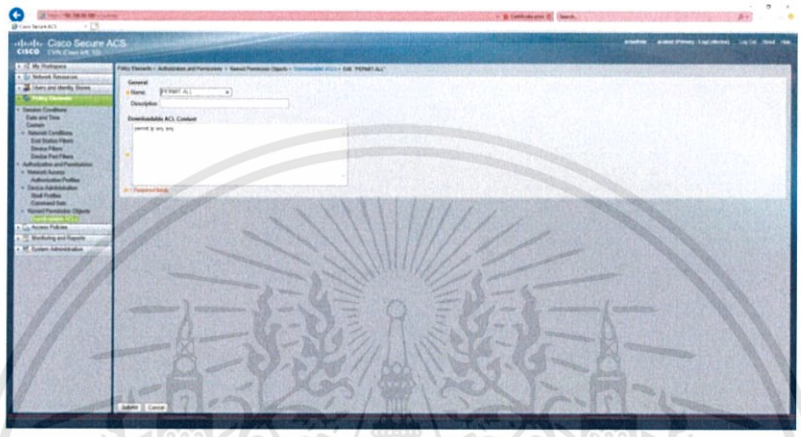
รูป 3.53 เพิ่มอุปกรณ์ที่ใช้งาน RADIUS

- ทำการสร้าง Identity Group สำหรับที่ต้องทำการยืนยันตัวตนใช้ชื่อว่า NON-DOT1X โดยเข้าไปที่ Users and Identity Stores > Identity Groups จากนั้นกด Create ในช่อง Name: ใส่ว่า NON-DOT1X แล้วกด Submit



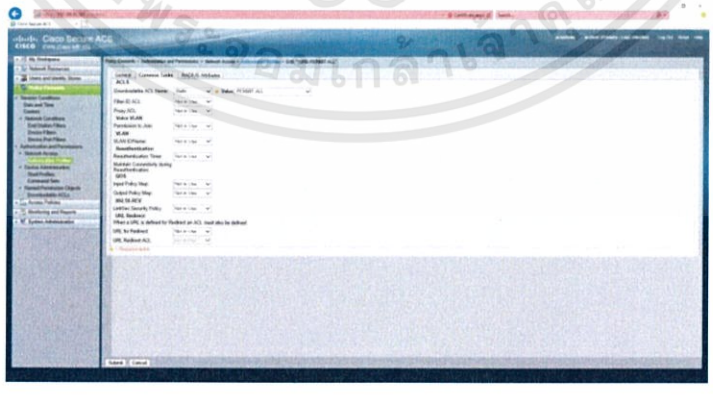
รูป 3.54 สร้าง Identity Group สำหรับ RADIUS

- สร้าง Authorization Profile เริ่มต้นจากสร้าง Downloadable ACLs เข้าไปที่ Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs แล้วกด Create ในช่อง Name ใส่ว่า PERMIT-ALL ส่วนช่อง Downloadable ACL Content ใส่ว่า permit ip any any



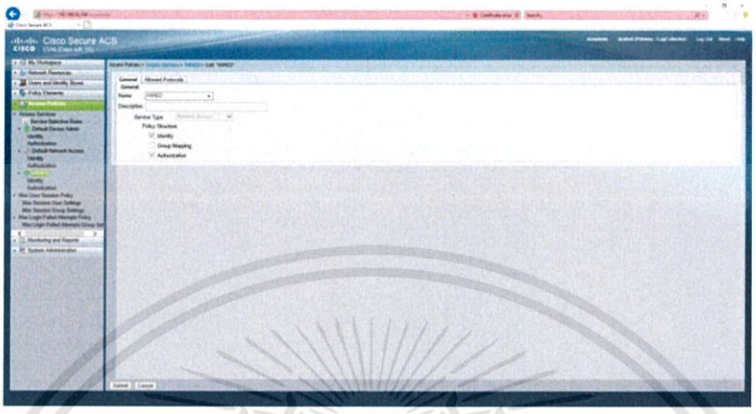
รูป 3.55 สร้าง Downloadable ACLs

- สร้าง Authorization Profile โดยเข้าไปที่ Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles แล้วกด Create ในแท็บ General ที่ช่อง Name ให้ตั้งชื่อว่า WIRE-PERMIT-ALL แท็บ Common Tasks ที่หัวข้อ Downloadable ACL Name เลือกเป็น Static และ Value เลือกเป็น PERMIT-ALL เสร็จแล้วกด Submit



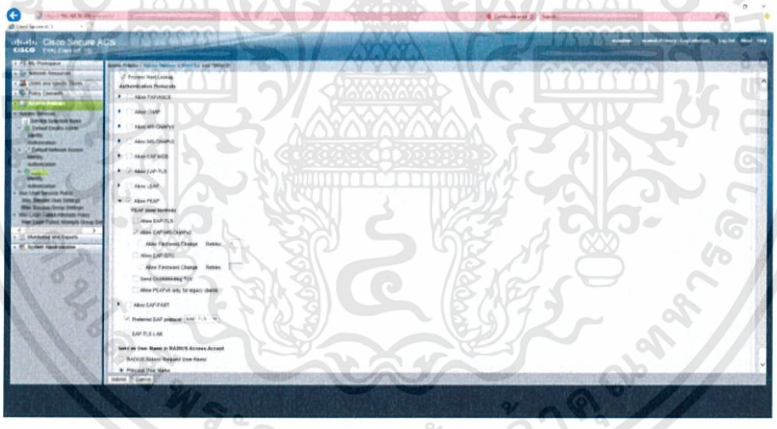
รูป 3.56 สร้าง Authorization Profile

- สร้าง Access Service โดยไปที่ Access Policies > Access Services แล้วกด Create ในช่อง Name ใส่ว่า WIRED และติ๊กถูกในช่อง Identity และ Authorization



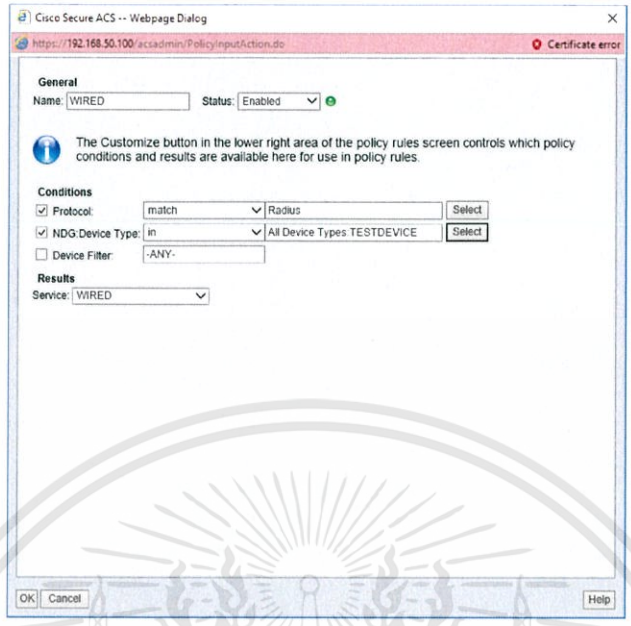
รูป 3.57 สร้าง Access Service(1)

- ที่แท็บ Allowed Protocols ทำการตั้งค่าดังนี้



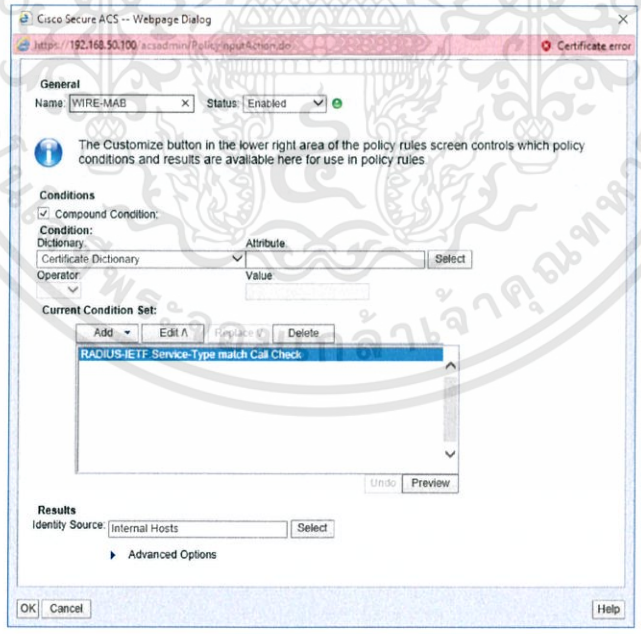
รูป 3.58 สร้าง Access Service(2)

- สร้าง Service Selection Rules สำหรับ Radius โดยไปที่ Access Policies > Access Services > Service Selection Rules จากนั้นกด Create จากนั้นทำการตั้งค่าดังนี้



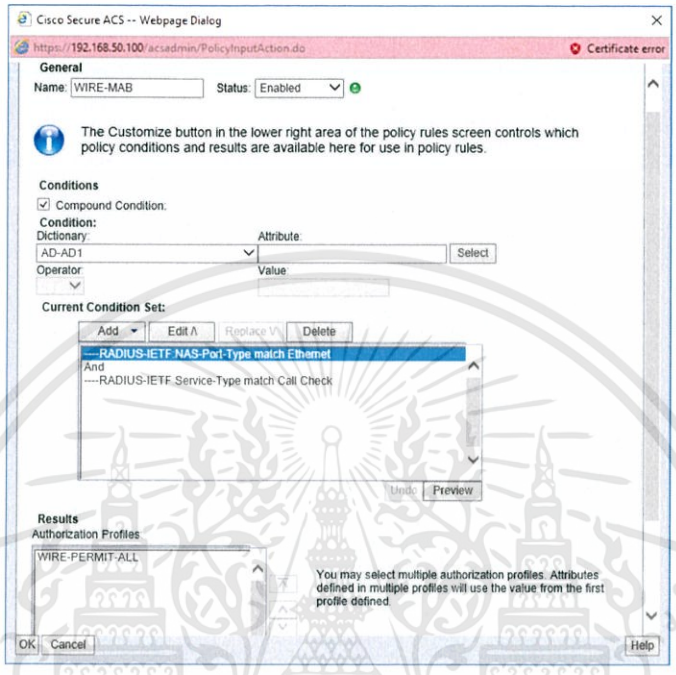
รูป 3.59 สร้าง Service Selection Rule สำหรับ Radius

- สร้าง Identity ให้กับเซอร์วิส WIRED โดยไปที่ Access Policies > Access Services > WIRED > Identity แล้วกด Create จากนั้นทำการตั้งค่าดังรูป



รูป 3.60 สร้าง Identity ให้กับเซอร์วิส WIRED

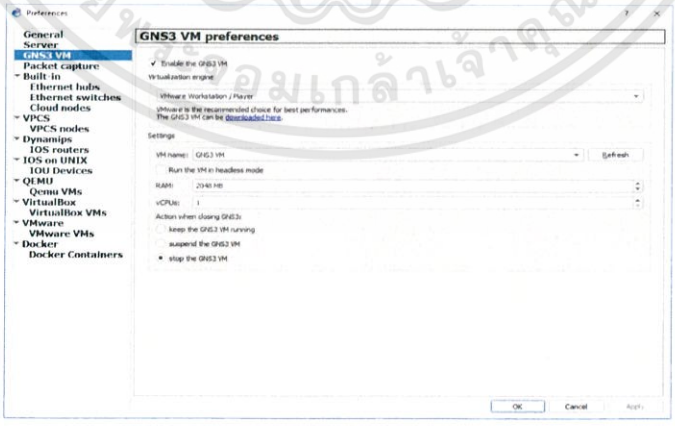
- สร้าง Authorization ให้กับเซอร์วิส WIRED โดยไปที่ Access Policies > Access Services > WIRED > Authorization แล้วกด Create จากนั้นทำการตั้งค่าดังรูป



รูป 3.61 สร้าง Authorization ให้กับเซอร์วิส WIRED

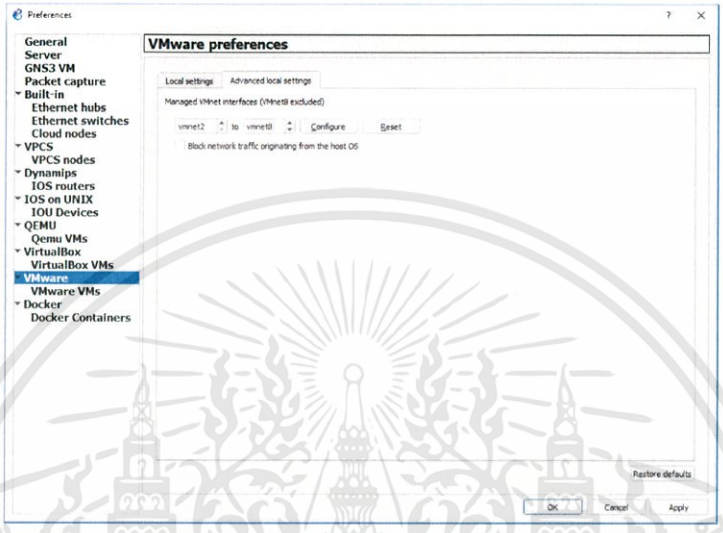
3.10 ตั้งค่า GNS3

- เชื่อมต่อ GNS3 VM กับ GNS3 เริ่มจากเปิดโปรแกรม GNS3 จากนั้นไปที่ Edit > Preferences > GNS3 VM และทำการตั้งค่าดังนี้



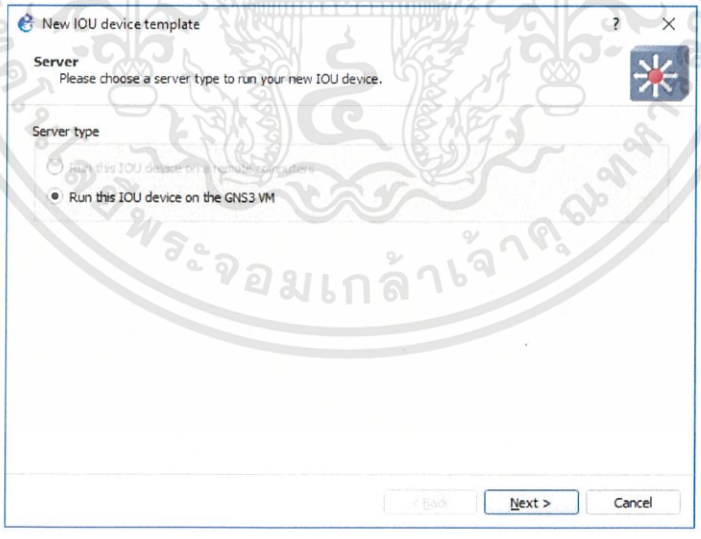
รูป 3.62 ตั้งค่าการเชื่อมต่อ GNS3 VM

- เพิ่ม Virtual Network Adapter สำหรับการเชื่อต่อไปยัง Cisco ACS และ ใช้เป็นคอมพิวเตอร์จำลอง โดยเข้าไปที่ Edit > Preferences > VMware > Advanced local setting และตั้งค่าดังรูป จากนั้นกด Configure แล้วกด OK



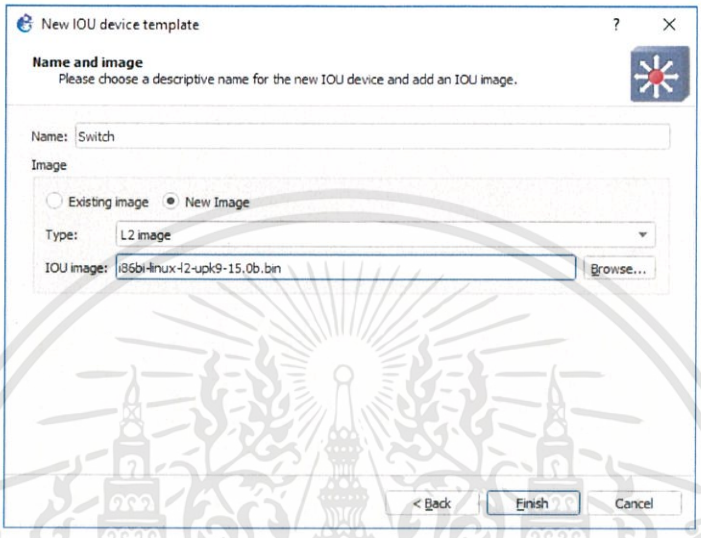
รูป 3.63 เพิ่ม Virtual Network Adapter

- เพิ่ม IOS switch โดยไปที่ Edit > Preferences > IOU Device แล้วเลือก New



รูป 3.64 เพิ่ม New IOU Device

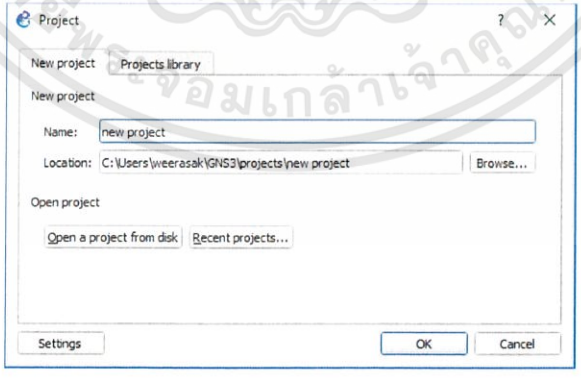
- เลือกที่ Run this IOU device on the GNS3 VM แล้วกด Next ช่อง Name ใส่ว่า Switch เลือกที่ New Image และ Type เลือกเป็น L2 image จากนั้นเลือกไฟล์ IOU ที่จัดเตรียมไว้ แล้วกด Finish



รูป 3.65 เลือก IOU ที่เตรียมไว้

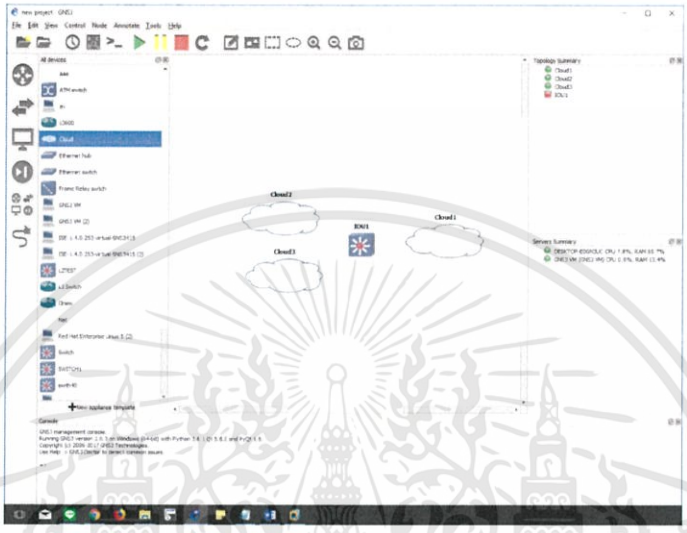
3.10 สร้าง Project และจำลอง Network Diagram

- เปิดโปรแกรม GNS3 สร้างโปรเจคขึ้นมาใหม่โดยไปที่ File > New blank project จะปรากฏหน้าต่างการสร้างโปรเจคใหม่ขึ้นมา ให้ตั้งชื่อว่า new project และเลือกที่จัดเก็บไฟล์ จากนั้นกด OK



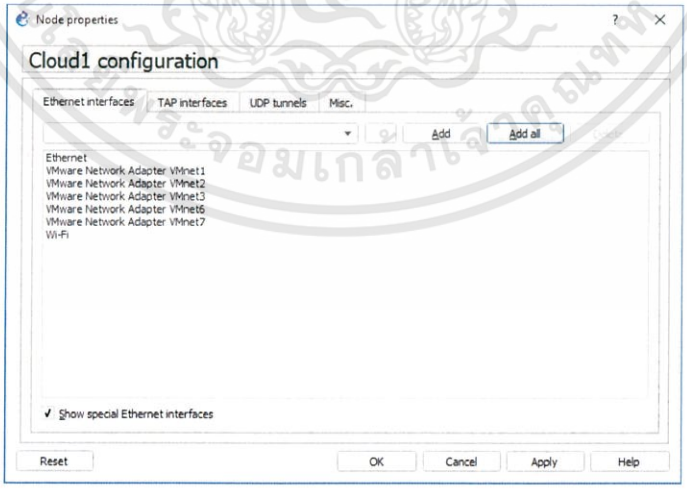
รูป 3.66 สร้างโปรเจคใหม่

- จะเข้ามาสู่หน้าต่างสำหรับการจำลองระบบเครือข่าย ทำการจำลองระบบเครือข่ายขึ้นมา โดยจะใช่ Switch ที่ได้ทำการติดตั้งไปในหัวข้อที่ผ่านมา และ Cloud สำหรับการเชื่อมต่อไปยัง Cisco ACS และจำลองเป็นคอมพิวเตอร์ที่ต้องใช้งานในระบบ



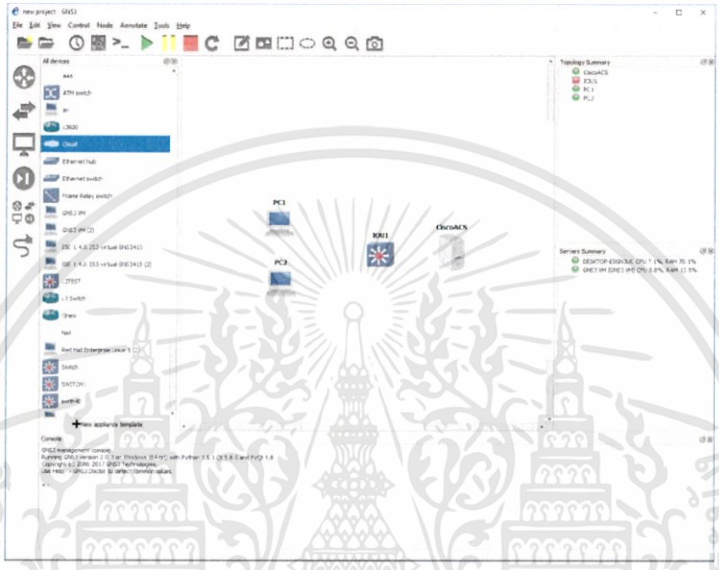
รูป 3.67 อุปกรณ์จำลองทั้งหมดที่ต้องใช้งาน

- ทำการตั้งค่า Network Adapter ให้ Cloud แต่ละตัวโดย คลิ๊กขวาที่ Cloud แล้วเลือก Configure จะแสดงหน้าต่าง Cloud configuration ติ๊กถูกที่ช่อง Show special Ethernet interface กด Add all จากนั้นกด OK



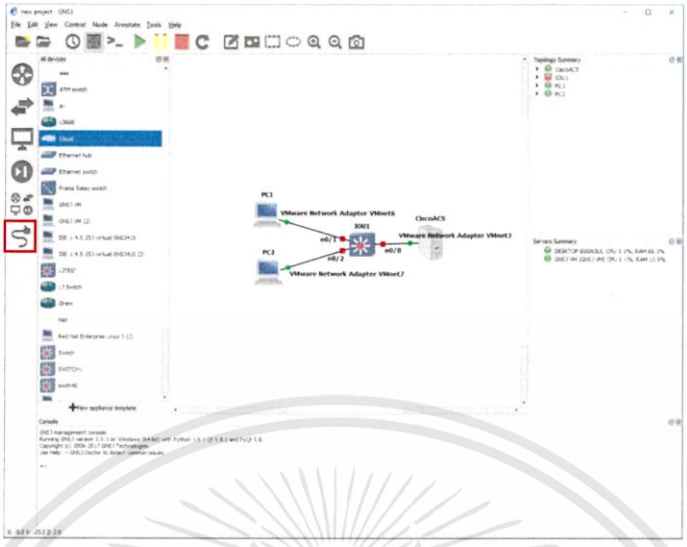
รูป 3.68 เพิ่ม Network Adapter

- เปลี่ยนชื่อและสัญลักษณ์ให้กับ Cloud เพื่อให้ง่ายต่อการทำงาน ในการเปลี่ยนชื่อนั้น คลิ๊กขวาที่ Cloud แล้วเลือก Change hostname แล้วทำการเปลี่ยนชื่อเป็น CiscoACS, PC1, PC2 ตามลำดับ และเปลี่ยนสัญลักษณ์โดยคลิ๊กขวาที่ Cloud แล้วเลือก Change symbol อุปกรณ์ Cloud1 เลือกเป็น อุปกรณ์ server ส่วนที่ Cloud2 และ Cloud3 เลือกเป็น computer



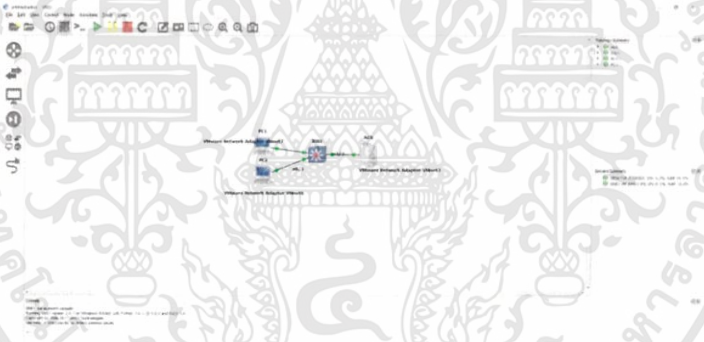
รูป 3.69 เปลี่ยนชื่อและแก้ไขสัญลักษณ์

- ทำการเชื่อมต่ออุปกรณ์เข้าด้วยกันโดยกดที่ Add a link และทำการเชื่อต่ออุปกรณ์ดังนี้
    - Interface ethernet 3/3 เชื่อมต่อกับ Cisco ACS Interface VMware Network Adapter3
    - Interface ethernet 0/0 เชื่อมต่อกับ PC1 Interface VMware Network Adapter7
    - Interface ethernet 0/1 เชื่อมต่อกับ PC2 Interface VMware Network Adapter6



รูป 3.70 เชื่อมต่ออุปกรณ์แต่ละตัวเข้าด้วยกัน

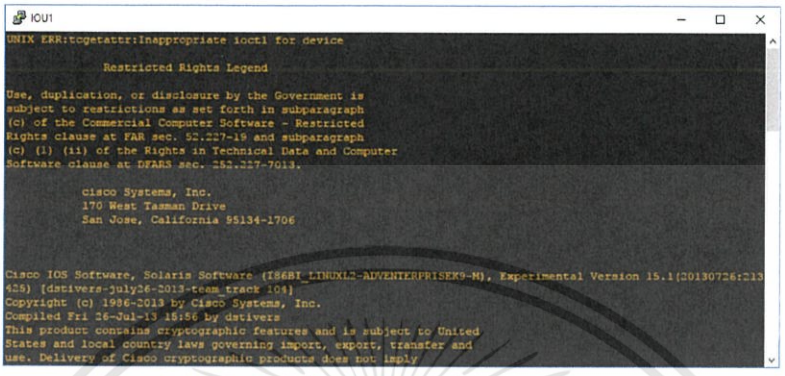
- เริ่มต้นการทำงานของทั้งระบบโดยคลิ๊กที่ Start/Resume All node



รูป 3.71 เริ่มต้นการทำงานของอุปกรณ์

3.11 Config อุปกรณ์สำหรับเชื่อมต่อกับ TACACS+ และ RADIUS Server

- ดับเบิ้ลคลิ๊กที่ Switch เพิ่มเปิดหน้าต่าง CLI สำหรับการ Configuration



รูป 3.72 หน้าต่าง CLI สำหรับการ Configuration

- ใน Global Config นั้นให้ใช้ Command ดังนี้

```
aaa new-model
!
aaa authentication login default local
aaa authentication login TAC none
aaa authentication login TACTEST group tacacs+ local
aaa authentication dot1x default group radius
aaa authorization exec default group tacacs+ local
aaa authorization exec CON local
aaa authorization commands 0 default group tacacs+ local
aaa authorization commands 1 TACTEST group tacacs+ local
aaa authorization commands 15 TACTEST group tacacs+ local
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
```

```
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa server radius dynamic-author
 client 192.168.50.100 server-key cisco
!
aaa session-id common
authentication mac-move permit
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
!
ip dhcp snooping
ip device tracking
!
dot1x system-auth-control
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
```

```
no ip http server
!
ip access-list extended ACL_DEFAULT
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 deny   ip any any log
!
tacacs-server host 192.168.50.100
tacacs-server key cisco
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 5 tries 3
radius-server host 192.168.50.100
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
```

- Config Interface ต่างๆดังนี้

```
interface Ethernet3/3
switchport access vlan 50
 switchport mode access
 duplex auto
!
```

```
interface Ethernet0/1
 switchport access vlan 50
 switchport mode access
 ip access-group ACL-DEFAULT in
 duplex auto
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface Ethernet0/2
 switchport access vlan 50
 switchport mode access
```

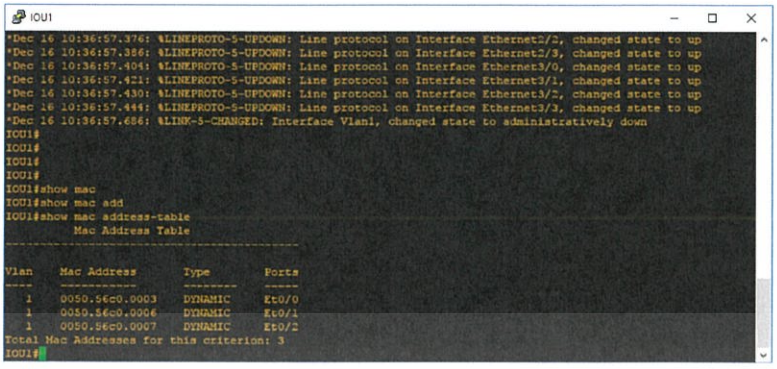
```
 ip access-group ACL-DEFAULT in
 duplex auto
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan50
 ip address 192.168.50.2 255.255.255.0
!
```

- Config line console และ line vty สำหรับการเข้าสู่ระบบผ่าน telnet, ssh และ console line

```
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 login authentication TACTEST
line vty 0 4
 authorization commands 1 TACTEST
 authorization commands 15 TACTEST
 login authentication TACTEST
 transport input all
!
```

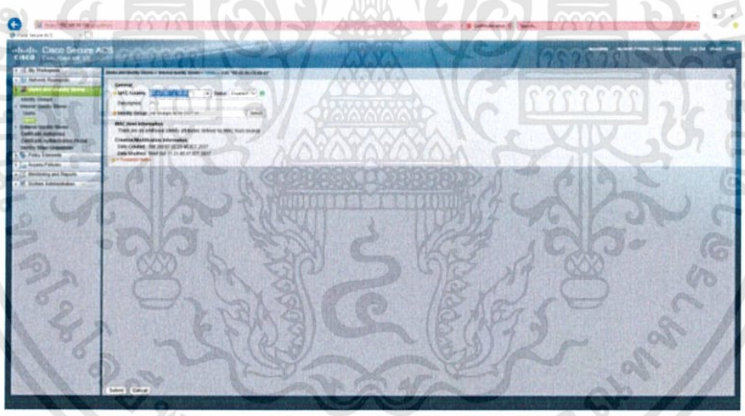
3.11 เพิ่ม Mac Address สำหรับการยืนยันตัวตน

- เราสามารถตวรจสอบ MAC Address ของอุปกรณ์ที่เชื่อมอยู่โดยใช้ Command “show mac address-table”



รูป 3.73 ตรวจสอบ MAC Address ของอุปกรณ์ที่เชื่อมต่อ

- จากนั้นเข้าไปที่ Cisco ACS แล้วไปที่ Users and Identity Stores > Internal Identity Stores > Hosts แล้วกด Create ในช่อง MAC Address ใส่ 00-50-56-C0-00-06 ซึ่งเป็นของ PC1 และ 00-50-56-C0-00-07 สำหรับ PC2 ในช่อง Description ใส่ว่า PC1 และ PC2 ตามลำดับ Identity Group เลือกเป็น NON-DOT1X จากนั้นกด Submit



รูป 3.74 เพิ่ม MAC Address ของอุปกรณ์ใน Cisco ACS

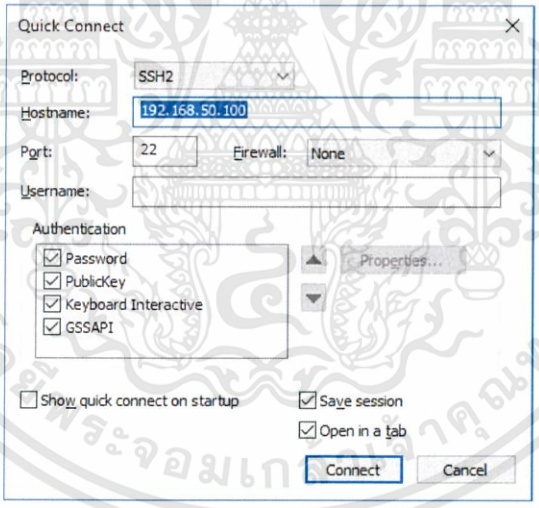
บทที่ 4

ผลการทดลอง

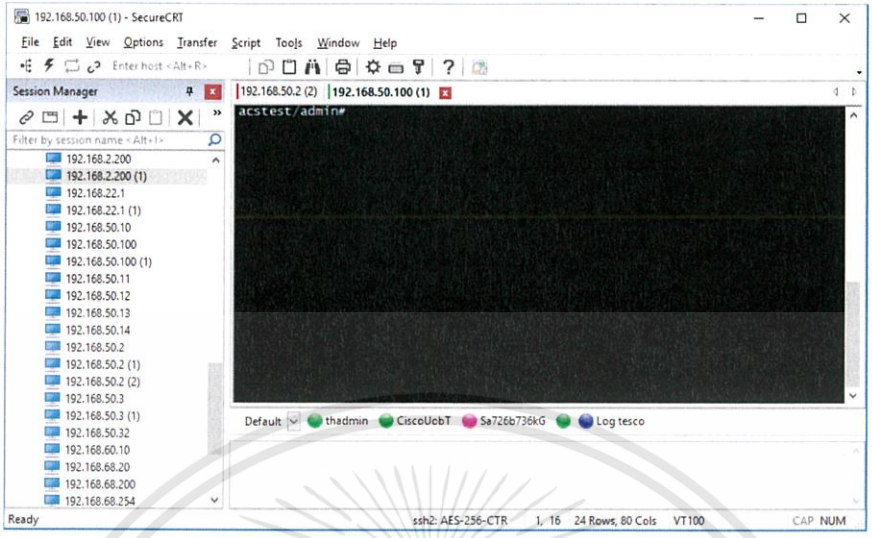
หลังจากที่ได้ทำการตั้งค่าต่างๆเรียบร้อยแล้วการติดตั้งโปรแกรม Cisco ACS การตั้งค่าต่างๆ สำหรับ TACACS+ server และ RADIUS server รวมถึงการจำลองตัวอย่างของระบบขึ้นมา จึงต้องมีการทดลองระบบต่างๆที่ได้ทำการติดตั้งว่าทำงานได้อย่างเต็มประสิทธิภาพ ตามความต้องการหรือไม่

- การเข้าใช้งาน Cisco ACS ผ่าน Secure Shell Service
- ตรวจสอบว่าอุปกรณ์เชื่อมต่อกับ RADIUS และ TACACS+ Server
- การเข้าใช้งานด้วย User ที่ลงทะเบียนกับ TACACS+
- ทดสอบการใช้ Command ผ่านแต่ละ User
- คอมพิวเตอร์สามารถเข้าใช้งานระบบได้โดย MAC Authentication

4.1 การเข้าใช้งาน Cisco ACS ผ่าน Secure Shell Service



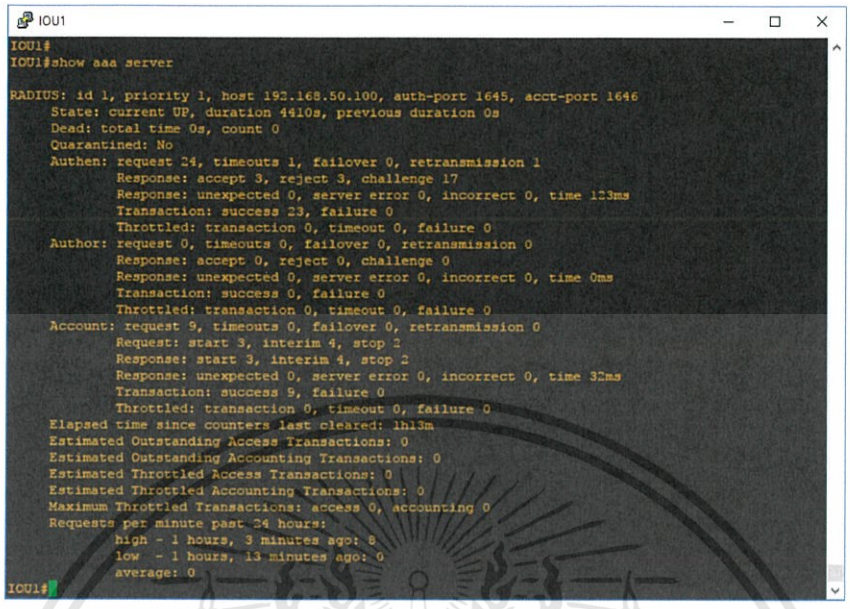
รูป 4.1 Secure Shell Service โดย SecureCRT



รูป 4.2 Secure Shell Service เข้าได้สำเร็จ

4.2 ตรวจสอบว่าอุปกรณ์เชื่อมต่อกับ RADIUS และ TACACS+ Server

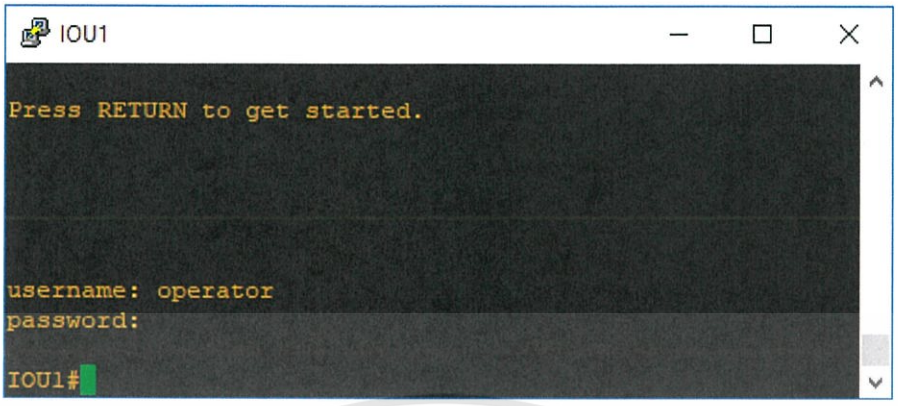
รูป 4.3 Ping ไปยัง CiscoACS



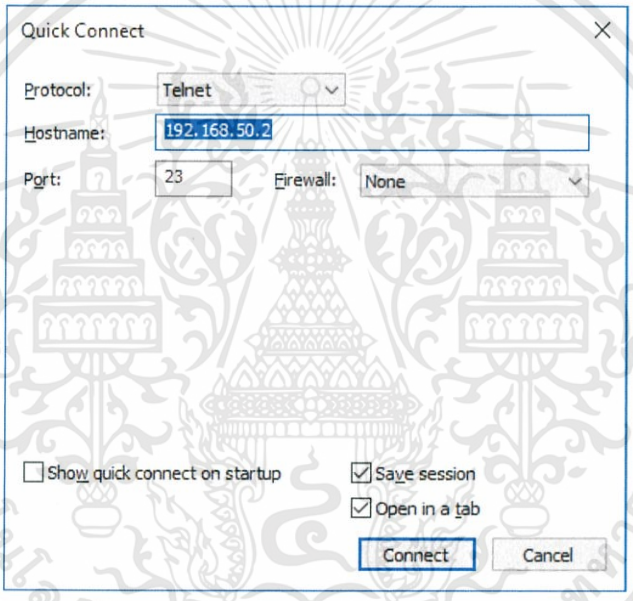
รูป 4.4 ตรวสอบด้วย show aaa server

4.3 การเข้าใช้งานด้วย User ที่ลงทะเบียนกับ TACACS+

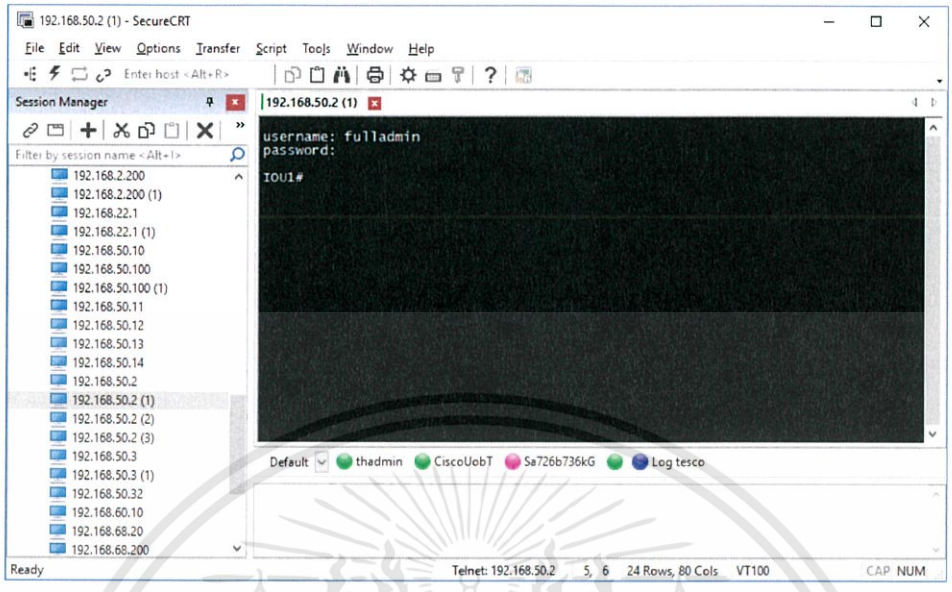
รูป 4.5 เข้าสู่อุปกรณ์ผ่านสายคอนโซลด้วย ชื่อผู้ใช้ fulladmin



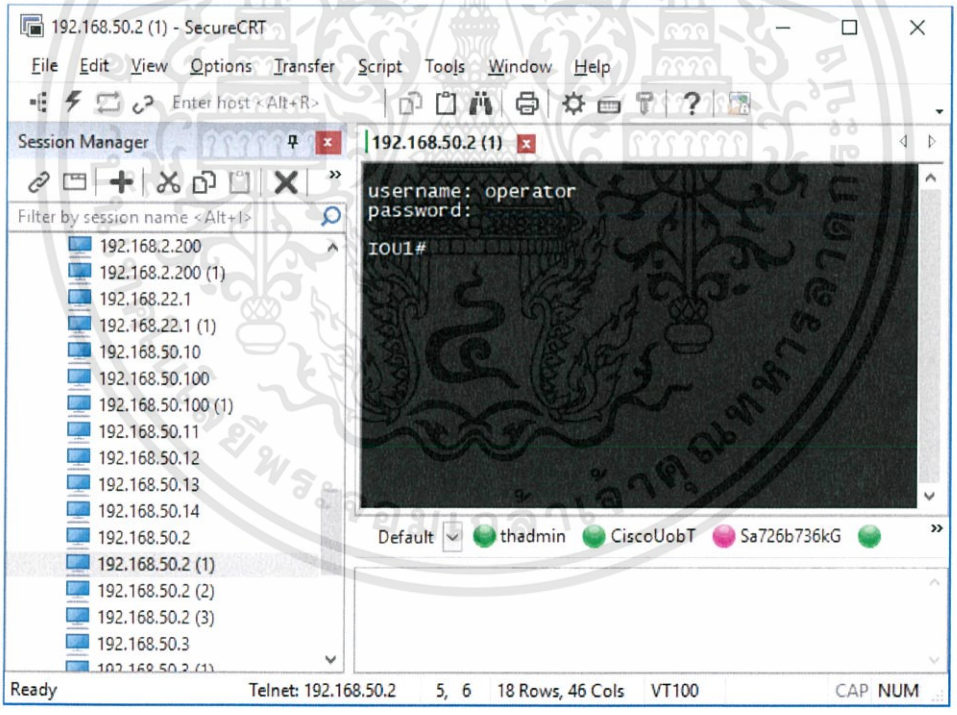
รูป 4.6 เข้าสู่อุปกรณ์ผ่านสายคอนโซลด้วย ชื่อผู้ใช้ operator



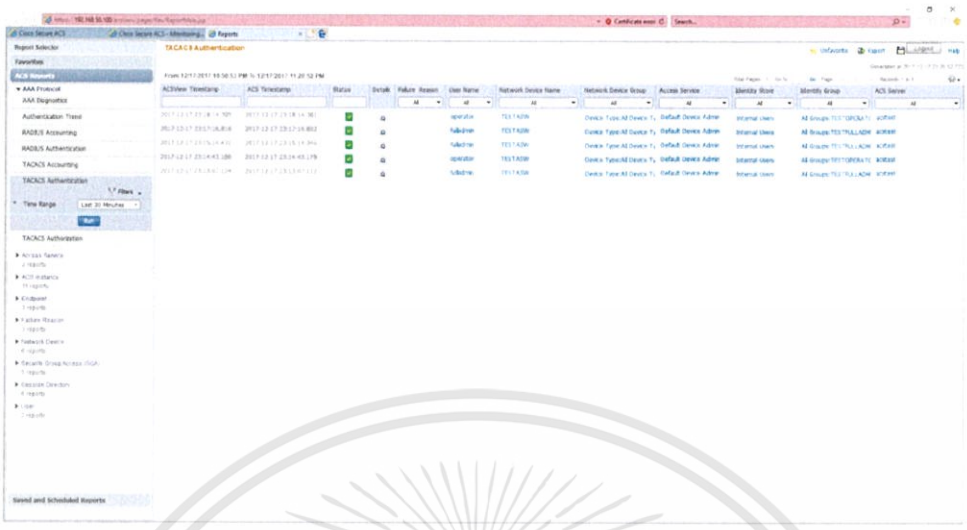
รูป 4.7 เข้าสู่อุปกรณ์ผ่านโปรโตคอล Telnet



รูป 4.8 เข้าสู่อุปกรณ์ผ่านโปรโตตอล Telnet ชื่อผู้ใช้ fulladmin

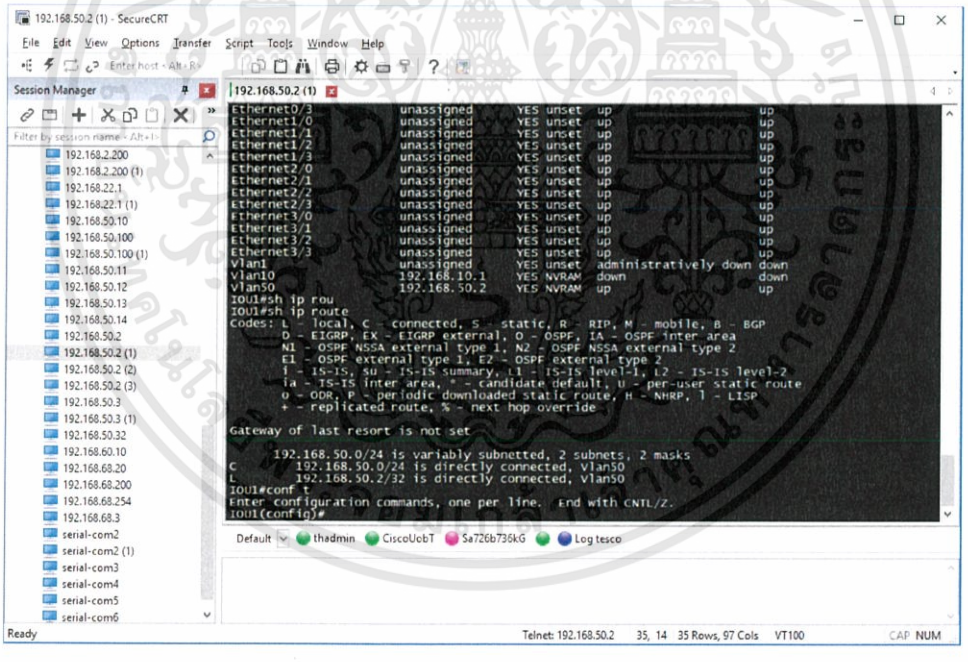


รูป 4.9 เข้าสู่อุปกรณ์ผ่านโปรโตตอล Telnet ชื่อผู้ใช้ operator

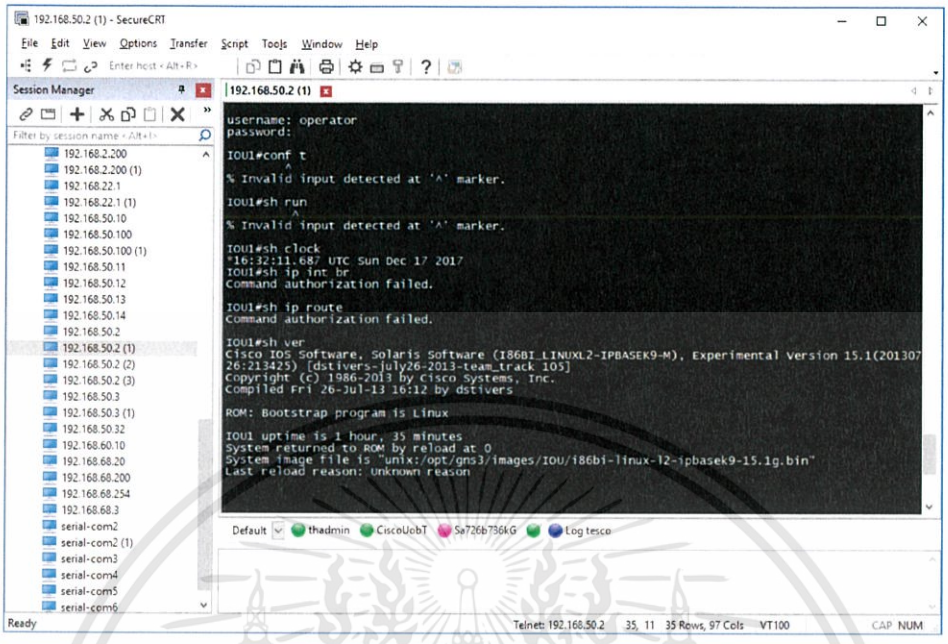


รูป 4.10 ตรวจสอบผู้ที่เข้าใช้งานผ่าน CiscoACS

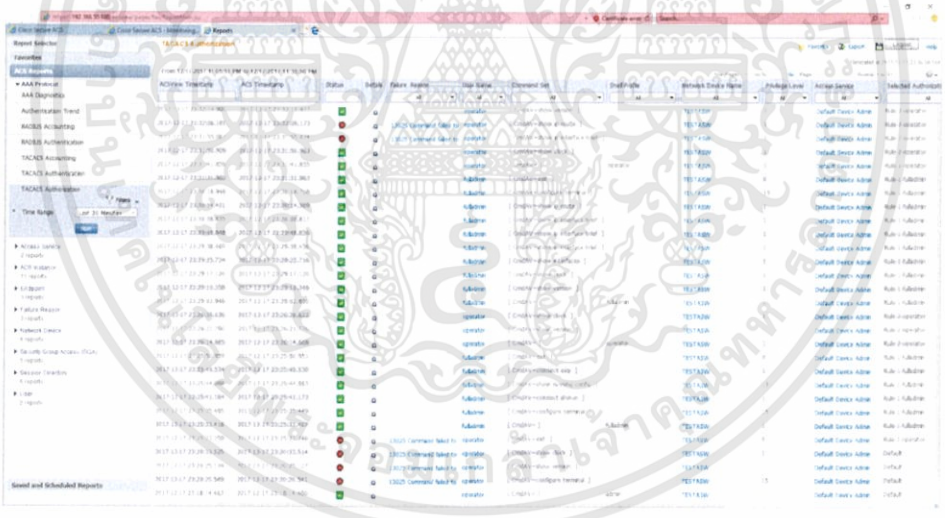
4.4 ทดสอบการใช้ Command ผ่านแต่ละ User



รูป 4.11 User fulladmin ใช้งานได้ทุก Command



รูป 4.12 User operator ใช้งานได้เฉพาะ Command ที่กำหนดไว้



รูป 4.13 Command ที่ใช้โดยแต่ละ User

4.5 คอมพิวเตอร์สามารถเข้าใช้งานระบบได้โดย MAC Authentication

ตรวจสอบโดยใช้ Command “show authentication session interface [interface]”

รูป 4.14 การยืนยันตัวตนสำเร็จ (1)

รูป 4.15 การยืนยันตัวตนสำเร็จ (2)

บทที่ 5

สรุปผล

ระบบความปลอดภัยขององค์กรนั้นเป็นสิ่งสำคัญขั้นพื้นฐานที่ทุกองค์กรควรมี และในการตรวจสอบสิทธิ์การเข้าใช้งานเครือข่ายนั้นก็เป็น ระบบความปลอดภัยขั้นต้นรูปแบบหนึ่งที่จะเพิ่มประสิทธิภาพของความปลอดภัยของระบบ และเพิ่มประสิทธิภาพการทำงานของระบบภาพรวม ที่เป็นการจำกัดทรัพยากรณ์ให้บุคคลในองค์กรได้ใช้งานได้อย่างเต็มที่ และสามารถควบคุมและจัดการสิทธิในการเข้าถึงเครือข่ายในด้านต่างๆ ซึ่งไม่ใช่แค่การยืนยันตัวตนเพื่อใช้ในการเข้าสู่เครือข่าย ทั้งในด้านการจัดการและการบริหารของผู้ดูแลระบบ สามารถจัดกลุ่มและแบ่งระดับการทำงานได้ตามงานที่ได้รับมอบหมาย และแบ่งหน้าที่การทำงานกันได้อย่างชัดเจน และตรวจสอบการเปลี่ยนแปลงต่างๆได้ว่าเกิดจากจุดใด ซึ่งเป็นส่วนช่วยในการบริหารจัดการได้ดี สำหรับซอฟท์แวร์ในการยืนยันตัวตนนั้นก็มีหลายชนิดและจากหลายบริษัทเช่นกัน สำหรับองค์กรที่ต้องการก็สามารถเลือกใช้ได้ตามความต้องการ และในการติดตั้งระบบนั้นสามารถทำได้ง่ายและไม่ซับซ้อนมากนัก แต่จำเป็นต้องมีการวิเคราะห์ระบบและวางแผนล่วงหน้าสำหรับการขยายตัวในอนาคตไว้ด้วย เนื่องจากหากเครื่อข่ายมีขนาดใหญ่มากค่าใช้จ่ายก็อาจจะมากขึ้นตามไปด้วย แต่เพื่อความปลอดภัยของระบบเครื่อข่ายและข้อมูลแล้วการลงทุนในด้านความปลอดภัยก็เป็นการลงทุนที่คุ้มค่า เนื่องจากจะได้เรื่องความปลอยภัยในด้านต่างๆแล้ว ยังได้ประโยชน์ในการจัดการการทำงานและเพิ่มประสิทธิภาพของระบบอีกด้วย

เอกสารอ้างอิง

[1] Cisco system, **User Guide for Cisco Secure Access Control System 5.8**

[2] Cisco system, **Cisco IOS Security Configuration Guide, Release 12.2**

[3] Cisco system, **Cisco Secure Access Control Server Deployment Guide**

[4] Cisco system, **MAC Authentication Bypass Deployment Guide**

[5] Cisco system, **Installation and Upgrade Guide for Cisco Secure Access Control System 5.8**

[6] RADIUS Server **Retrieved from http://networkradius.com/doc/3.0.10/concepts/introduction/radius_server.html**