บทที่ 4
เทคนิคในการปฏิบัติงาน

หลักเกณฑ์ วิธีการและขั้นตอนการปฏิบัติงาน

หลักเกณฑ์ วิธีการและขั้นตอนการปฏิบัติงานของผู้ใช้งาน และขั้นตอนการทำงานของระบบตรวจสอบสถานะและปริมาณการใช้งานเครือข่าย มีหัวข้อที่เกี่ยวข้อง ดังนี้

1) การวิเคราะห์ภาพรวมของระบบ
2) การติดตั้ง SNMP Service สำหรับอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย
3) การติดตั้งโปรแกรม MIB Browser เพื่อทดสอบ SNMP Service
4) การติดตั้งโปรแกรม cacti และการปรับแต่งระบบ
5) การบริหารจัดการอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่ายในระบบ cacti
6) การเขียน php script เพื่อนำมาใช้งานร่วมกับระบบ cacti
7) การติดตั้ง template สำเร็จรูปสำหรับโปรแกรม cacti
8) การใช้งาน plugin (monitor, weather map, realtime)
9) การสร้างบัญชีผู้ใช้ และการกำหนดสิทธิ์ (User Management)
10) การสำรองข้อมูล และการกู้คืนระบบ cacti

4.1 การวิเคราะห์ภาพรวมของระบบ

ปัจจุบันนี้ระบบเครือข่ายมีความซับซ้อนมากขึ้น การบริหารจัดการระบบเครือข่ายไม่ใช่แค่เพียงติดตั้ง และใช้งาน แต่ต้องมีการตรวจสอบเฝ้าระวังประสิทธิภาพการทำงานเพื่อทำการบำรุงรักษาให้ระบบทำงานได้อย่างมีประสิทธิภาพ และต่อเนื่อง การลดลง หรือถดถอยของประสิทธิภาพการทำงานของระบบเครือข่ายในบางระบบงานอาจทำให้เกิดความเสียหายมูลค่าสูง ทั้งทางการเงิน หรือทรัพย์สิน รวมทั้งชีวิตได้ เช่น ระบบจำหน่ายไฟฟ้า หรือระบบท่อส่งแก๊สและน้ำมัน และนั่นคือที่มาของความต้องการโปรโตคอลในการบริหารจัดการระบบเครือข่าย หรือโปรโตคอล SNMP ซึ่งอยู่ในชุดโปรโตคอล TCP/IP (Transmission Control Protocol/Internet Protocol) [1]

โปรโตคอล SNMP ได้ถูกพัฒนาขึ้นในปี พ.ศ.2531 เนื่องจากมีความเจริญเติบโตในการใช้อุปกรณ์ที่สนับสนุนโปรโตคอล TCP/IP อย่างสูง โปรโตคอล SNMP ถูกออกแบบให้มีฟังก์ชัน และการทำงานแบบง่าย ๆ เหมาะกับคำว่าซิมเปิล (Simple) ตามชื่อของมัน โดยมีจุดประสงค์หลักเพื่อให้ผู้ดูแลระบบเครือข่าย

สามารถเข้ามาจัดการอุปกรณ์เครือข่ายได้จากระยะไกลโดยง่าย สิ่งที่สำคัญของโปรโตคอล SNMP ก็คือความง่ายในการใช้งาน ทำให้ผู้ดูแลระบบเครือข่ายสามารถควบคุมอุปกรณ์ที่สนับสนุน SNMP ได้จากที่ไหนก็ได้ที่ระบบเครือข่ายนั้นไปถึง ตัวอย่างคือ ผู้ดูแลระบบเครือข่ายสามารถทดลองแก้ไขปัญหาอย่างเร่งด่วนโดยทำการรีเซตพอร์ตอีเทอร์เน็ตสวิตช์ที่ต่อเข้ากับ PLC (Programmable Logic Controller) ที่ไม่สามารถติดต่อระบบควบคุมได้ หรือสามารถตรวจสอบอัตราการเข้าใช้งาน (Utilized Rate) หรือการเกิดจากเฟรมผิดพลาดของพอร์ต หรือแม้กระทั่งตรวจสอบอุณหภูมิของอุปกรณ์เครือข่ายว่าเป็นปกติ หรือไม่ เพื่อเข้าทำการบำรุงรักษาก่อนที่ระบบเครือข่ายจะขัดข้อง ซึ่งถือว่าเป็นการบำรุงรักษาแบบ CBM (Condition-based Maintenance) อีกหน้าที่หนึ่งของ SNMP ที่สำคัญคือ การใช้เฝ้าระวัง หรือมอนิเตอร์ระบบเครือข่ายทั้งระบบ แตกต่างจากการเข้าจัดการอุปกรณ์แบบรายอุปกรณ์ ซึ่งฟังก์ชันการมอนิเตอร์ระบบเครือข่ายดังกล่าวเรียกอีกอย่างว่า RMON (Remote Network Monitoring) ซึ่งได้ถูกพัฒนาเพื่อช่วยในการวิเคราะห์การทำงานของระบบเครือข่าย

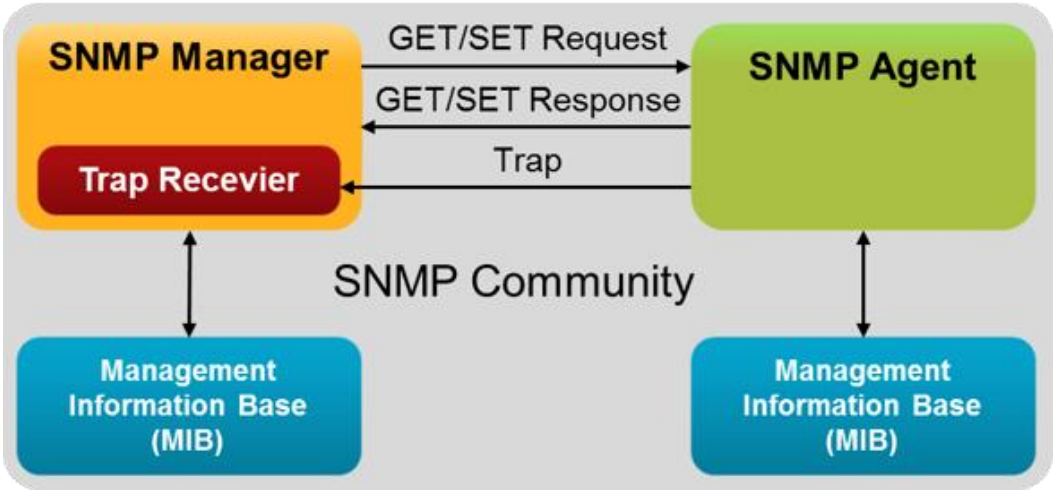
สำหรับมาตรฐานโปรโตคอล TCP/IP จะมีหน่วยงานสากลในชื่อ IETF (Internet Engineering Task Force) ที่คอยกำกับดูแลซึ่งรวมไปถึงโปรโตคอล SNMP ด้วย โดยทาง IETF จะทำการตีพิมพ์ข้อกำหนดมาตรฐานในชื่อ RFCs (Request for Comments) โดยเริ่มแรกข้อกำหนดจะถูกนำเสนอให้ทาง IETF ทำการพิจารณา หลังจากรับข้อกำหนด IETF จะพิจารณาขั้นต้น และข้อกำหนดนั้นจะเข้าสู่สถานะฉบับร่าง และท้ายสุดจะเข้าสู่สถานะอนุมัติเมื่อข้อกำหนดนั้นสมบูรณ์ และ RFC ฉบับนั้นจะถูกพิจารณาให้เป็นมาตรฐาน แต่อย่างไรก็ตามอันที่จริงมีไม่กี่ RFC ที่ถูกอนุมัติให้เป็นมาตรฐาน สืบเนื่องมาจากเทคโนโลยีทางด้านการสื่อสารมีความก้าวหน้าแบบก้าวกระโดด ทำให้เกิด RFC ตัวใหม่เข้ามาแทนที่ ทั้ง ๆ ที่ตัวเก่ายังไม่รับอนุมัติให้เป็นมาตรฐาน รายการดังต่อไปนี้เป็นเวอร์ชัน และ RFC ของโปรโตคอล SNMP [2] [3]

SNMP Version 1 (SNMPv1) เป็นมาตรฐานปัจจุบัน และเป็นที่นิยมเพราะความง่ายของโปรโตคอล SNMP ซึ่งถูกระบุใน RFC1157 และได้รับอนุมัติให้เป็นมาตรฐานที่สมบูรณ์ ระดับความปลอดภัย SNMPv1 จะขึ้นอยู่กับคอมมิวนิตี้สตริง (Community String) ที่ทำหน้าที่เหมือนรหัสผ่าน หรือพาสเวิร์ด (Password) โดยที่จริงแล้วเป็นเพียงข้อความแบบธรรมดา (Plain Text) ที่บ่งบอกถึงสิทธิการเข้าไปจัดการอุปกรณ์เครือข่าย โดยปกติคอมมิวนิตี้จะมีสามประเภทนั้นคือ อ่านอย่างเดียว (Read-only), อ่านเขียน (Read-write) และแทรป (Trap)

SNMP Version 2 (SNMPv2) คือ เวอร์ชันที่ทำงานบนคอมมิวนิตี้ที่ได้รับการปรับปรุง ในทางเทคนิคเรียกว่า SNMPv2c ซึ่งระบุใน RFC1905, RFC1906 และ RFC1907 และอยู่ในขั้นตอนทดสอบใช้งาน

แต่ก็มีบางผู้ผลิตได้นำมาใช้งานในอุปกรณ์ของพวกเขา SNMPv2 ออกแบบมาเพื่อแก้ไขข้อด้อยของ SNMPv1 ในเรื่องการร้องข้อมูลปริมาณมาก และปัญหาในการส่งข้อมูลแบบแทรป

SNMP Version 3 (SNMPv3) เป็นเวอร์ชันถัดไปของโปรโตคอล SNMP ที่ถูกคาดหวังให้เป็นมาตรฐานที่สมบูรณ์ ซึ่งในปัจจุบันอยู่ในสถานะนำเสนอระบุใน RFC1905, RFC1906, RFC1907, RFC2571, RFC2572, RFC2573, RFC2574 และ RFC2575 โดยมุ่งเน้นการเพิ่มระดับความปลอดภัยของโปรโตคอล SNMP



ภาพที่ 4-1 แสดงโครงสร้างของ SNMP Service [4]

โปรโตคอล SNMP ใช้ UDP เป็นโปรโตคอลในการส่ง และรับข้อมูลระหว่างตัวเมเนเจอร์ และเอเยนต์ เพราะว่าโปรโตคอล UDP ใช้การเชื่อมต่อแบบคอนเน็กชันเลส (Connectionless) ซึ่งไม่มีการเชื่อมต่อสื่อสารหรือทำแฮนด์แช็กกิ้งก่อนที่จะรับ และส่งข้อมูลระหว่างเมเนเจอร์ และเอเยนต์ลักษณะการทำงานของโปรโตคอล UDP จริง ๆ มีระดับความเชื่อถือได้ที่ไม่สูง เพราะไม่มีการตอบรับแพ็กเกจถ้าเกิดมีการสูญหายระหว่างทางดังนั้นจึงตกเป็นหน้าที่ระดับแอพพลิเคชั่นที่ต้องประเมินว่าแพ็กเกจสูญหาย หรือไม่ หรือต้องทำการส่งการร้องขอใหม่ หรือไม่ วิธีที่ใช้ทั่วไปคือการใช้ไทเมอร์ หรือไทม์เอาต์เมเนเจอร์ที่ส่งเมสเซสร้องขอไปยังตัวเอเยนต์จะคอยการตอบสนองในระยะเวลาหนึ่ง ซึ่งระยะเวลานั้นขึ้นอยู่กับการตั้งค่าของผู้ดูแลระบบเครือข่าย ถ้าหมดระยะเวลาการรอคอยแล้วไม่มีการตอบสนองใด ๆ จากเอเยนต์ เมเนเจอร์จะประเมินว่าแพ็กเกจเกิดการสูญหาย และจะทำการส่งเมสเซสการร้องขออีกครั้ง จำนวนครั้งที่การร้องขอซ้ำนั้นขึ้นอยู่กับการตั้งค่าเช่นกัน แต่ข้อดีของโปรโตคอล UDP คือการที่ UDP มีค่าโอเวอร์เฮดที่ต่ำไม่ไปรบกวน หรือส่งผลกระทบกระเทือนต่อประสิทธิภาพของระบบเครือข่าย หรือตัวระบบงานหลัก อันที่จริงโปรโตคอล SNMP ก็สามารถใช้โปรโตคอล TCP แต่ก็เป็นเฉพาะกรณีพิเศษอย่างยิ่งเท่านั้น สำหรับระบบเครือข่ายที่ความคับคั่งสูงเป็น

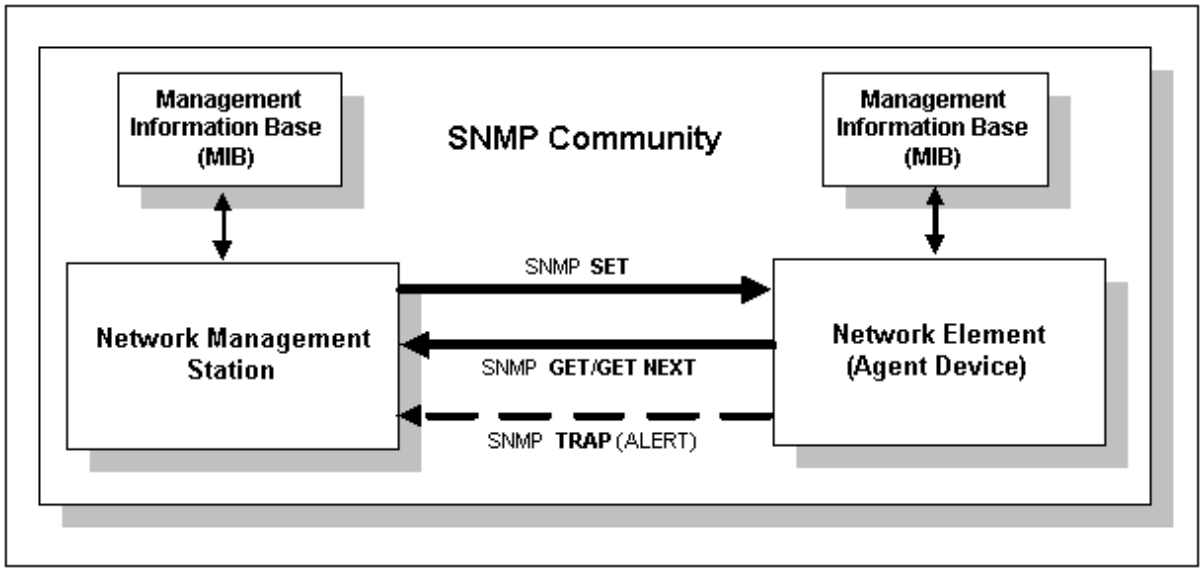
ความคิดที่ไม่ถูกต้องที่จะใช้โปรโตคอล TCP ก็เพราะว่าโปรโตคอล TCP อันที่จริงก็ไม่เหมาะสมกับทุกระบบงานโดยเฉพาะกับระบบเครือข่ายที่ไม่สมบูรณ์ หรือคับคั่งสูง โปรโตคอล SNMP ถูกคาดหวังว่าสามารถทำงานได้ดีแม้ในระบบเครือข่ายที่ไม่สมบูรณ์ แต่ถ้าระบบเครือข่ายมีปัญหาอยู่ และยังมีระบบจัดการเครือข่ายที่เพิ่มปัญหาเข้าไปอีก เช่น การใช้โปรโตคอล TCP ที่มีค่าโอเวอร์เฮดที่สูง เป็นต้น ก็ไม่น่าจะเป็นความคิดที่ถูกต้อง

โปรโตคอล SMNP ใช้พอร์ต UDP หมายเลข 161 สำหรับส่ง และรับแบบการร้องขอข้อมูล และใช้พอร์ตหมายเลข 161 สำหรับรับเมสเซจชนิดแทรปจากเอเยนต์ของอุปกรณ์เครือข่ายที่ถูกจัดการ ทุกอุปกรณ์เครือข่ายต้องใช้พอร์ตหมายเลขดังกล่าวเป็นหมายเลขดีฟอลต์ แต่อย่างไรก็ตามบางผู้ผลิตอนุญาตให้เปลี่ยนหมายเลขพอร์ต ซึ่งเมเนเจอร์ต้องรับทราบ และเปลี่ยนหมายเลขพอร์ตให้ตรงกับอุปกรณ์เครือข่ายเพื่อให้สามารถติดต่อรับส่งเมสเซจได้

4.1.2 SNMP คอมมิวนิตี้ (SNMP Communities)

สำหรับ SNMPv1 และ SNMPv2 ที่เป็นที่นิยม จะใช้ระบบคอมมิวนิตี้ในการสร้างความปลอดภัยในการรับส่งข้อมูลระหว่างเมเนเจอร์ และเอเยนต์ โดยทั่วไปเอเยนต์จะถูกตั้งค่าให้มีคอมมิวนิตี้ 3 ประเภท โดยวิธีการตั้งชื่อ นั้นคือ อ่านได้อย่างเดียว สามารถอ่านเขียน และแทรป ชื่อคอมมิวนิตี้ หรือคอมมิวนิตี้สตริง อันที่จริงทำงานเสมือนเป็นรหัสผ่าน โดยผู้ผลิตทั่วไปจะให้คอมมิวนิตี้สตริง ชื่อพับลิก (Public) สำหรับการอ่านได้อย่างเดียว คอมมิวนิตี้สตริง ชื่อไพรเวต (Private) สำหรับการอ่าน และเขียน หรือเซตติ้งตั้งค่า เป็นสิ่งที่ดีที่จะเปลี่ยนชื่อคอมมิวนิตี้สตริงที่เป็นดีฟอลต์ให้เป็นชื่อเฉพาะเพื่อเพิ่มระดับความปลอดภัย การสร้างแทรปเพื่อแจ้งผู้ดูแลระบบเครือข่ายเมื่อมีการพยายามเข้ามาตั้งค่า หรือร้องขอข้อมูลจากตัวเอเยนต์ด้วยชื่อคอมมิวนิตี้สตริงที่ไม่ถูกต้อง หรือไม่ตรงกับที่กำหนดก็เป็นสิ่งที่ดี ก็เพราะเป็นการแจ้งเตือนว่าอาจเกิดมีผู้ไม่หวังดีพยายามเข้ามาเจาะระบบเครือข่าย

เนื่องจากชื่อคอมมิวนิตี้สตริงเสมือนเป็นรหัสผ่านของระบบจัดการเครือข่าย ดังนั้นการตั้งชื่อคอมมิวตี้สตริงก็ควรตั้งตามกฎการตั้งรหัสผ่านของเซิร์ฟเวอร์ เช่น ไม่เป็นคำในพจนานุกรม คำควรมีทั้งตัวเล็กตัวใหญ่รวมทั้งตัวเลข เป็นต้น

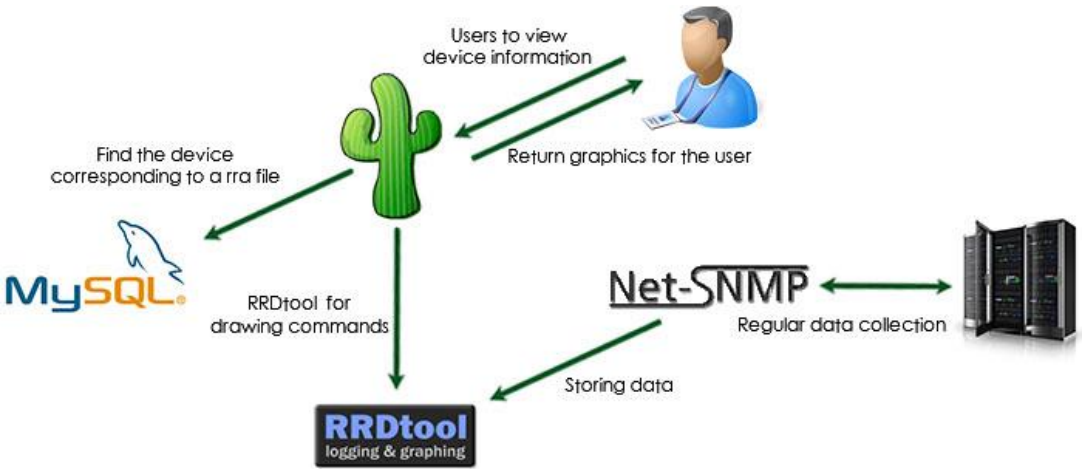


ภาพที่ 4-2 แสดงโครงสร้างการทำงานของ SNMP Community [4]

แต่อย่างไรก็ตามระดับความปลอดภัยด้วยคอมมิวนิตี้สตริงก็ยังต่ำอยู่ เนื่องจากคอมมิวนิตี้สตริงถูกส่งแบบข้อความธรรมดาไม่มีการเข้ารหัส ทำให้ง่ายต่อผู้บุกรุกที่มีความชำนาญสูงสามารถทำการดักจับชื่อคอมมิวนิตี้สตริงได้ และใช้มันเป็นจุดเริ่มต้นในการเจาะเข้าระบบเครือข่าย ดังนั้นจึงได้มีออกข้อกำหนดเพิ่มระดับความปลอดภัยให้สูงขึ้นในมาตรฐาน SNMPv3 แต่อย่างไรก็ตามยังมีวิธีการลดระดับความเสี่ยงต่อการเจาะระบบ ก็คือการติดตั้งไฟล์วอลล์ (Firewall) ซึ่งสามารถกำหนดให้ไฟร์วอลล์อนุญาตเฉพาะโฮสต์ที่รู้จักเข้ามาจัดการระบบเครือข่ายได้เท่านั้น เป็นสิ่งสำคัญที่ต้องตระหนักว่าถ้ามีใครซักคนสามารถอ่านเขียนอุปกรณ์เครือข่ายด้วย SNMP ก็คือสามารถเข้ามาควบคุมระบบเครือข่ายได้ เช่น ปิดพอร์ตเราเตอร์ การเปลี่ยนตารางเราเตอร์ซึ่งทำให้ระบบเครือข่ายล้มเหลวได้ อีกวิธีการหนึ่งในการเพิ่มระดับความปลอดภัย คือการใช้ฟังก์ชัน VPN (Virtual Private Network) เนื่องจากทราฟิกของ VPN จะถูกเข้ารหัสไว้ทำให้ดักจับได้ยาก อีกวิธีการหนึ่งแบบง่าย ๆ คือการเปลี่ยนชื่อคอมมิวนิตี้สตริงอย่างสม่ำเสมอ แต่ก็เป็นการยากสำหรับระบบเครือข่ายขนาดใหญ่ที่จำนวนเมเนเจอร์ และเอเยนต์จำนวนมาก

4.1.3 ภาพรวมการทำงานของ SNMP Service และระบบ Cacti

เนื่องจาก cacti มีการเรียกเก็บข้อมูลจากอุปกรณ์ต่าง ๆ ผ่านทาง SNMP Service เพราะฉะนั้นสามารถแสดงภาพรวมในการทำงานของระบบ cacti และ SNMP Service ได้ดังภาพ



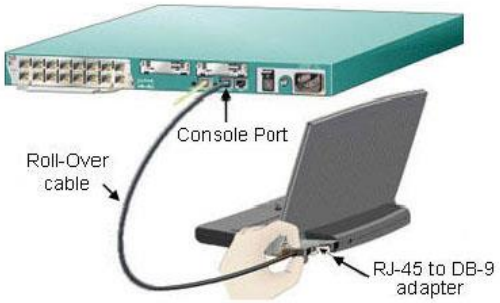
ภาพที่ 4-3 แสดงโครงสร้างการทำงานของ cacti และ SNMP Service [5]

4.2 ขั้นตอนการเปิดใช้งาน SNMP

โดยอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย ที่ทางมหาวิทยาลัยเทคโนโลยีราชมงคลพระนครใช้งานอยู่มีความหลากหลาย รวมถึงระบบปฏิบัติการที่ใช้อยู่ด้วยเช่นกัน ดังนั้นขั้นตอนต่อไปนี้จะแสดงวิธีการในการเปิด SNMP Service ของอุปกรณ์แต่ล่ะประเภท

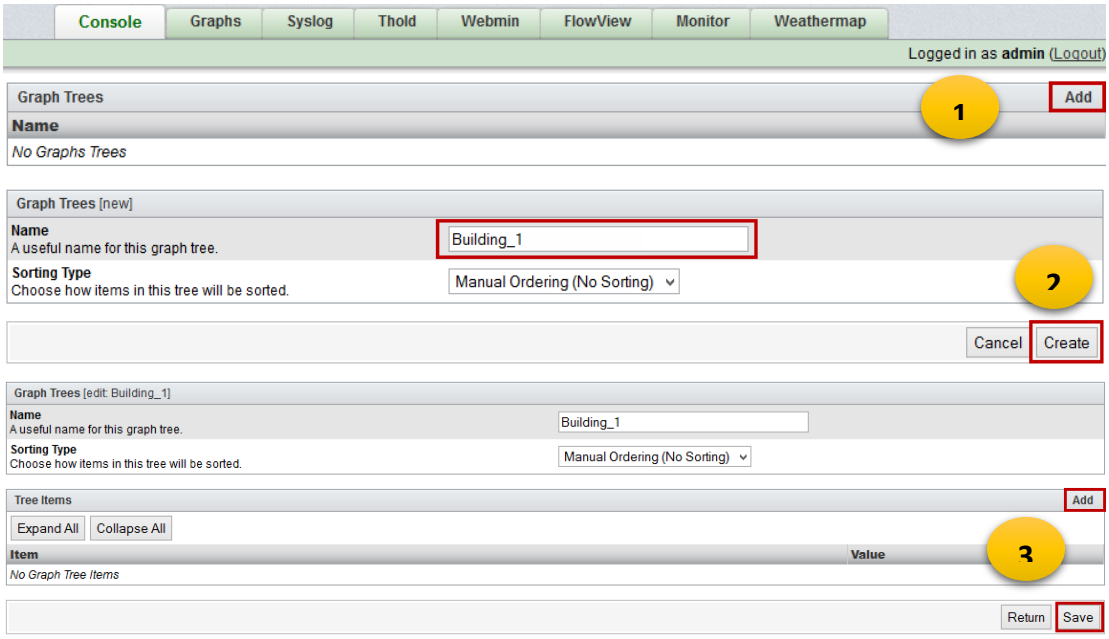
4.2.1 ขั้นตอนการเปิด SNMP บนอุปกรณ์ Switch และ Router Cisco

- เปิดโปรแกรม Putty แล้วเลือก Connection type เป็น รูปแบบ Serial ในกรณี ที่เชื่อมต่ออุปกรณ์ด้วยสายคอนโทรล หรือ เลือก Telnet หรือ SSH ในกรณี ที่ Remote



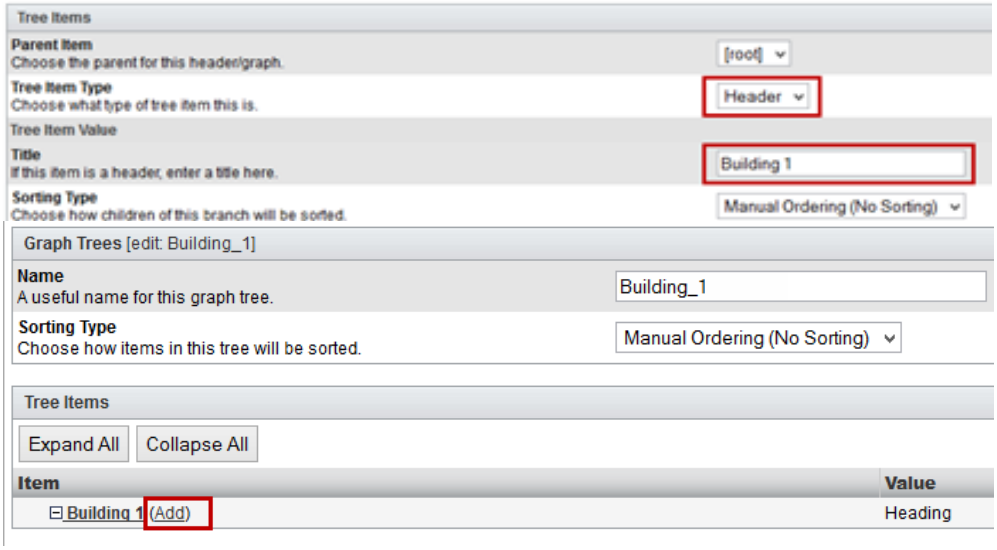
ภาพที่ 4-4 แสดงการเชื่อมต่อสาย console เข้ากับอุปกรณ์ router [6]

การสร้าง Graph Tree เป็นการจัดการอุปกรณ์ตามคุณลักษณะต่างๆ เช่นแบ่งหมวดหมู่จากสถานที่ติดตั้งของอุปกรณ์ เช่น อุปกรณ์ที่ติดตั้งตามอาคาร ตามชั้นต่าง ๆ การแบ่งตามประเภทของอุปกรณ์ หรือแบ่งได้จากลักษณะการทำงาน โดยมีวิธีการดังนี้คือ ไปที่แถบเมนู Console เลือกเมนู Graph Trees คลิกที่ปุ่ม Add เพื่อทำการสร้าง Graph Trees ทำการกำหนดชื่อให้กับ Graph Trees โดยเริ่มจากการสร้างส่วนที่จะนำมาเป็น Header สำหรับ Tree ก่อนแล้วจึงค่อยนำอุปกรณ์มาไว้ใน Tree นี้ ดังภาพที่ 4-75



ภาพที่ 4-76 แสดงวิธีการสร้าง Graph Trees

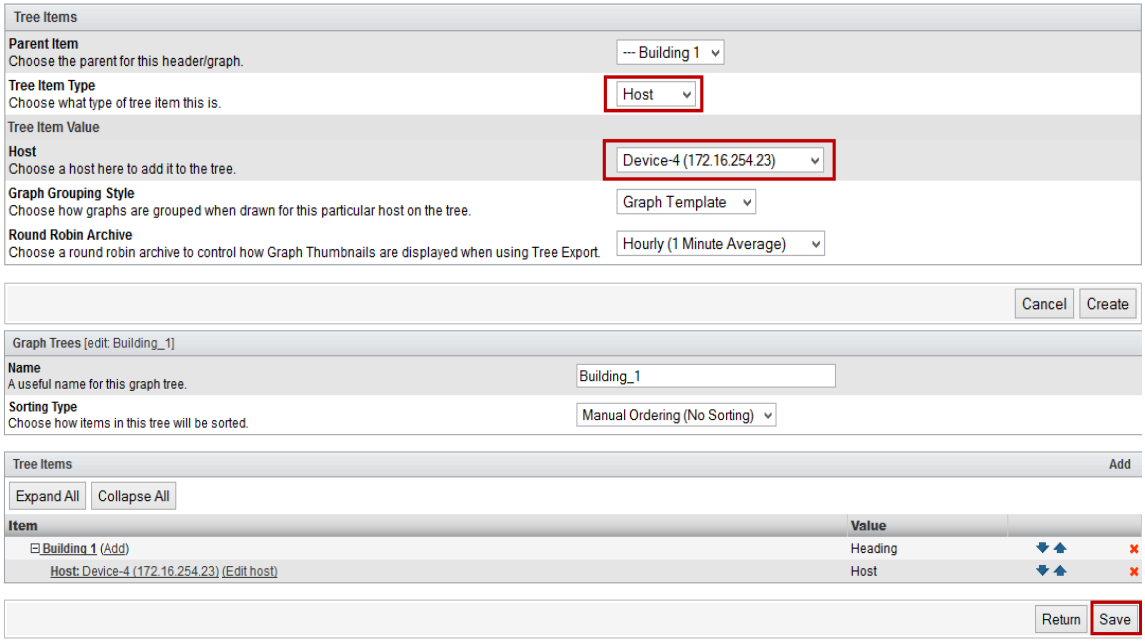
- ☐ ในหัวข้อ Tree Item Type ให้เลือกเป็น Header
- ☐ ให้หัวข้อ Title ให้ทำการตั้งชื่อให้สอดคล้องกับสถานที่ติดตั้งอุปกรณ์จากนั้นกดที่ปุ่ม Create
- ☐ จากนั้นกดที่ปุ่ม Add เพื่อนำอุปกรณ์เพิ่มเข้าไปใน Graph Trees



ภาพที่ 4-77 แสดงการเพิ่มใส่อุปกรณ์ใน Graph Trees

☐ ในหัวข้อ Tree Item Type ให้เลือกเป็น Host

☐ ในหัวข้อ Host ให้เลือกอุปกรณ์ที่ทำการสร้าง

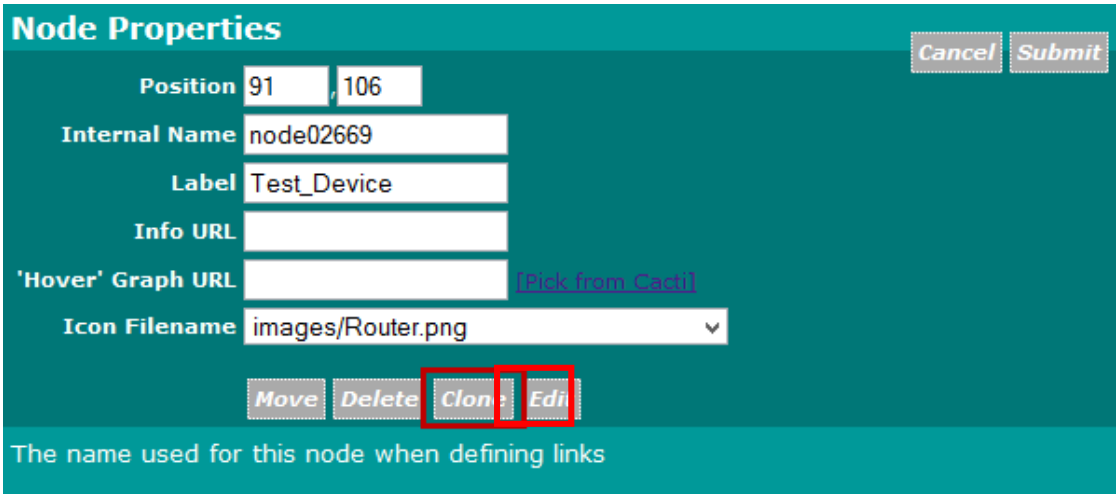


ภาพที่ 4-78

แสดงการบันทึกอุปกรณ์ลงใน Graph Trees

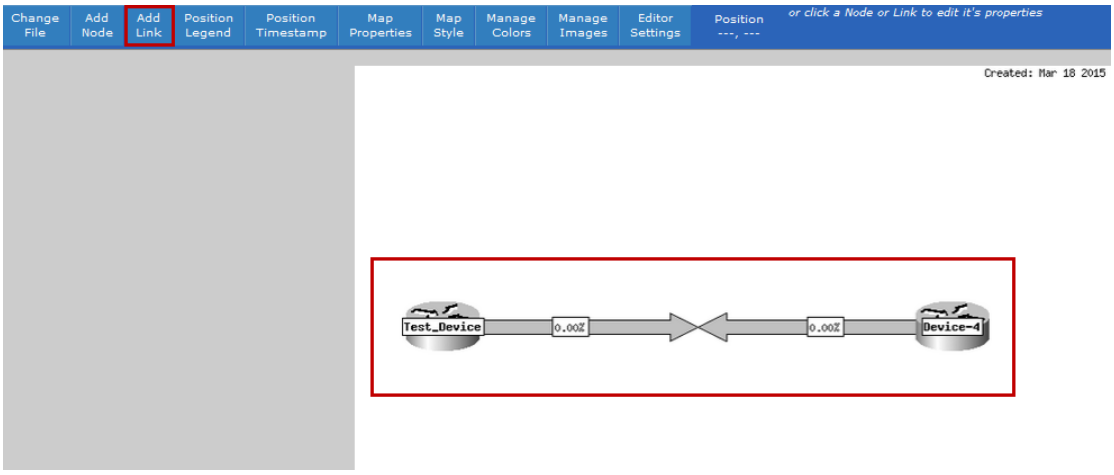
เมนู Clone ใช้สำหรับการคัดลอก Node หรืออุปกรณ์

- เมนู Edit ใช้สำหรับการแก้ไขรายละเอียดของ Node หรืออุปกรณ์



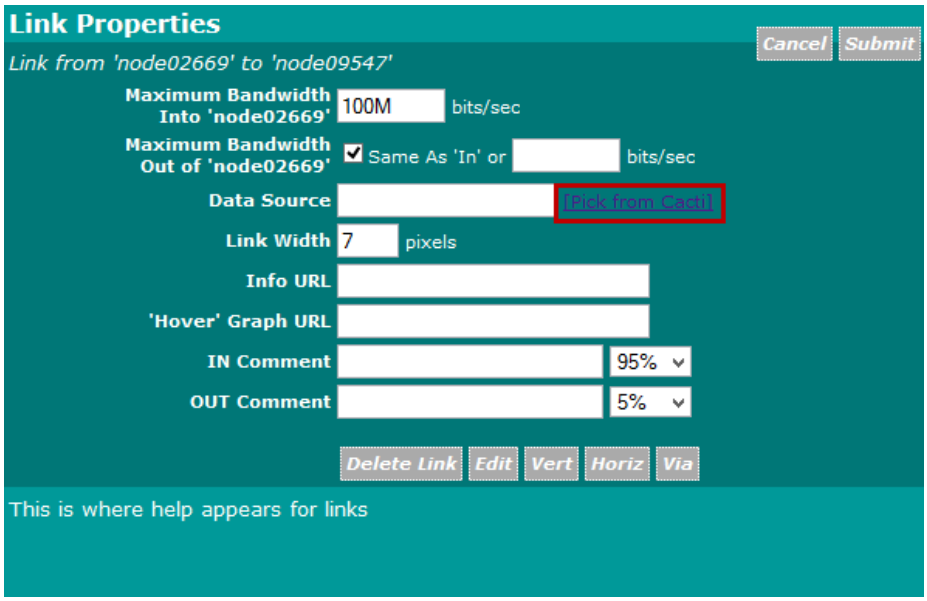
ภาพที่ 4-92 แสดงเมนูการ Clone และการ Edit Node

- การเพิ่มสายสัญญาณเพื่อเชื่อมต่อระหว่างอุปกรณ์เพื่อทำการดูจำนวนข้อมูลที่ผ่านตัวอุปกรณ์ โดยสามารถทำได้โดยเลือกที่เมนู Add Link คลิกที่อุปกรณ์ต้นทาง จะมีสัญลักษณ์เป็นกรอบสี่เหลี่ยมสีแดงเพิ่มขึ้นมาที่ตัวอุปกรณ์ และคลิกอีกครั้งที่อุปกรณ์ปลายทาง



ภาพที่ 4-93 การเลือกเมนู Add Link

- การปรับแต่งรูปแบบของสายสัญญาณ
  - การลดขนาดของสายสัญญาณการลดขนาดของสายสัญญาณสามารถทำได้โดยคลิกที่สายสัญญาณ แล้วทำการเปลี่ยนแปลงค่าในเมนู Link Width
  - การกำหนดระดับปริมาณการใช้งานผ่านสายสัญญาณ
  - การกำหนดระดับปริมาณการใช้งานผ่านสายสัญญาณด้วยสัญลักษณ์สี ซึ่งสัญลักษณ์สีสามารถบ่งบอกปริมาณการใช้งานของอุปกรณ์ผ่านสายสัญญาณ
- การกำหนด Data Source เพื่อเลือกกราฟที่ต้องการนำมาแสดงบนปผนภาพ weathermap โดยคลิกที่สายสัญญาณ แล้วเลือกที่ [Pick from Cacti]



ภาพที่ 4-94 แสดงการกำหนด Data Source