

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 ก็คือ ความง่ายในการใช้งาน ทำให้ผู้ดูแลระบบเครือข่ายสามารถควบคุมอุปกรณ์ที่สนับสนุน SNMP ได้จากที่ไหนก็ได้ที่ระบบเครือข่ายนั้นไปถึง ตัวอย่างคือ ผู้ดูแลระบบเครือข่ายสามารถทดลองแก้ไขปัญหาย่างเร่งด่วน โดยทำการรีเซตพอร์ตอีเทอร์เน็ตสวิตช์ที่ต่อเข้ากับ PLC (Programmable Logic Controller) ที่ไม่สามารถติดต่อระบบควบคุมได้ หรือสามารถตรวจสอบอัตราการเข้าใช้งาน (Utilized Rate) หรือการเกิดจากเฟรมผิดพลาดของพอร์ต หรือแม้กระทั่งตรวจสอบอุณหภูมิของอุปกรณ์เครือข่ายว่าเป็นปกติ หรือไม่ เพื่อเข้าทำการบำรุงรักษาก่อนที่จะ ระบบเครือข่ายจะขัดข้อง ซึ่งถือว่าการบำรุงรักษาแบบ CBM (Condition-based Maintenance) อีกหน้าที่หนึ่งของ SNMP ที่สำคัญคือ การใช้ไฟกระพริบ หรือมอนิเตอร์ระบบเครือข่ายทั้งระบบ แตกต่างจากการเข้าจัดการอุปกรณ์แบบรายอุปกรณ์ ซึ่งฟังก์ชันการมอนิเตอร์ระบบเครือข่ายดังกล่าว เรียกอีกอย่างว่า RMON (Remote Network Monitoring) ซึ่งได้ถูกพัฒนาเพื่อช่วยในการวิเคราะห์การทำงานของระบบเครือข่าย

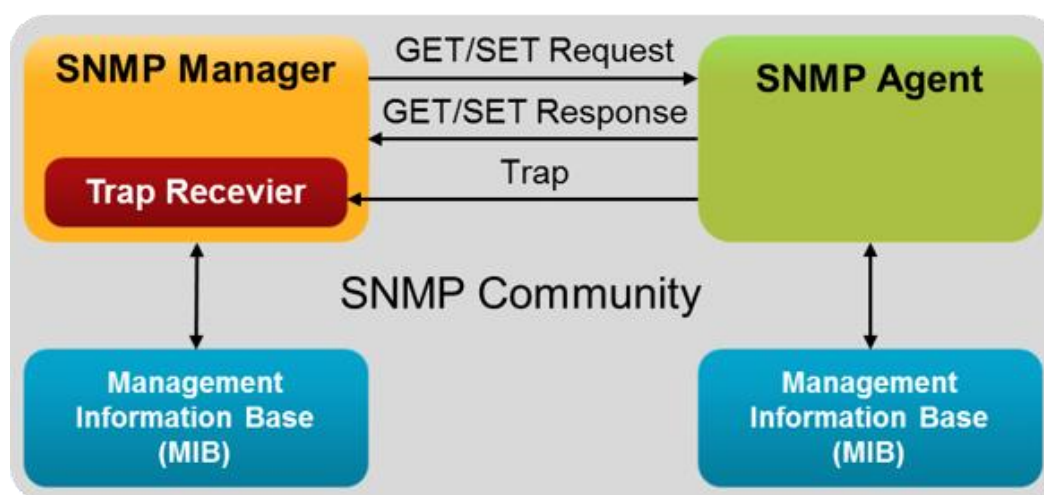
สำหรับมาตรฐานโปรโตคอล TCP/IP จะมีหน่วยงานสากลในชื่อ IETF (Internet Engineering Task Force) ที่คอยกำกับดูแลซึ่งรวมไปถึงโปรโตคอล SNMP ด้วย โดยทาง IETF จะทำการตีพิมพ์ข้อกำหนดมาตรฐานในชื่อ RFCs (Request for Comments) โดยเริ่มแรกข้อกำหนดจะถูกนำเสนอให้ทาง IETF ทำการพิจารณา หลังจากรับข้อกำหนด IETF จะพิจารณาขั้นต้น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

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

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

แต่ก็มีบางผู้ผลิตได้นำมาใช้งานในอุปกรณ์ของพวกเขา SNMPv2 ออกแบบมาเพื่อแก้ไขข้อด้อยของ SNMPv1 ในเรื่องการร้องข้อมูลปริมาณมาก และปัญหาในการส่งข้อมูลแบบแทรป

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



ภาพที่ 4-1 แสดงโครงสร้างของ SNMP Service [4]

โปรโตคอล SNMP ใช้ UDP เป็นโปรโตคอลในการส่ง และรับข้อมูลระหว่างตัวเมเนเจอร์ และเอเจนต์ เพราะว่าโปรโตคอล UDP ใช้การเชื่อมต่อแบบคอนเนกชันเลส (Connectionless) ซึ่งไม่มีการเชื่อมต่อสื่อสารหรือทำแฮนด์เช็กกิ้งก่อนที่จะรับ และส่งข้อมูลระหว่างเมเนเจอร์ และเอเจนต์ลักษณะการทำงานของโปรโตคอล UDP จริง ๆ มีระดับความเชื่อถือได้ที่ไม่สูง เพราะไม่มีการตอบรับแพ็กเกจถ้าเกิดการสูญหายระหว่างทางดังนั้นจึงตกเป็นหน้าที่ระดับแอปพลิเคชันที่ต้องประเมินว่าแพ็กเกจสูญหาย หรือไม่หรือต้องทำการส่งการร้องขอใหม่ หรือไม่ วิธีที่ใช้ทั่วไปคือการใช้ไทม์เมอร์ หรือไทม์เอาต์เมเนเจอร์ที่ส่งเมสเสจร้องขอไปยังตัวเอเจนต์จะคอยการตอบสนองในระยะเวลาหนึ่ง ซึ่งระยะเวลานั้นขึ้นอยู่กับค่าของผู้ดูแลระบบเครือข่าย ถ้าหมดระยะเวลาการรอคอยแล้วไม่มีการตอบสนองใด ๆ จากเอเจนต์ เมเนเจอร์จะประเมินว่าแพ็กเกจเกิดการสูญหาย และจะทำการส่งเมสเสจการร้องขออีกครั้ง จำนวนครั้งที่การร้องขอซ้ำนั้นขึ้นอยู่กับค่าเช่นกัน แต่ข้อดีของโปรโตคอล UDP คือการที่ UDP มีค่าไทม์เอาต์ที่ต่ำไม่ไปรบกวน หรือส่งผลกระทบต่อประสิทธิภาพของระบบเครือข่าย หรือตัวระบบงานหลัก อันที่จริงโปรโตคอล SNMP ก็สามารถใช้โปรโตคอล TCP แต่ก็เป็นเฉพาะกรณีพิเศษอย่างยิ่งเท่านั้น สำหรับระบบเครือข่ายที่ความคับคั่งสูงเป็น

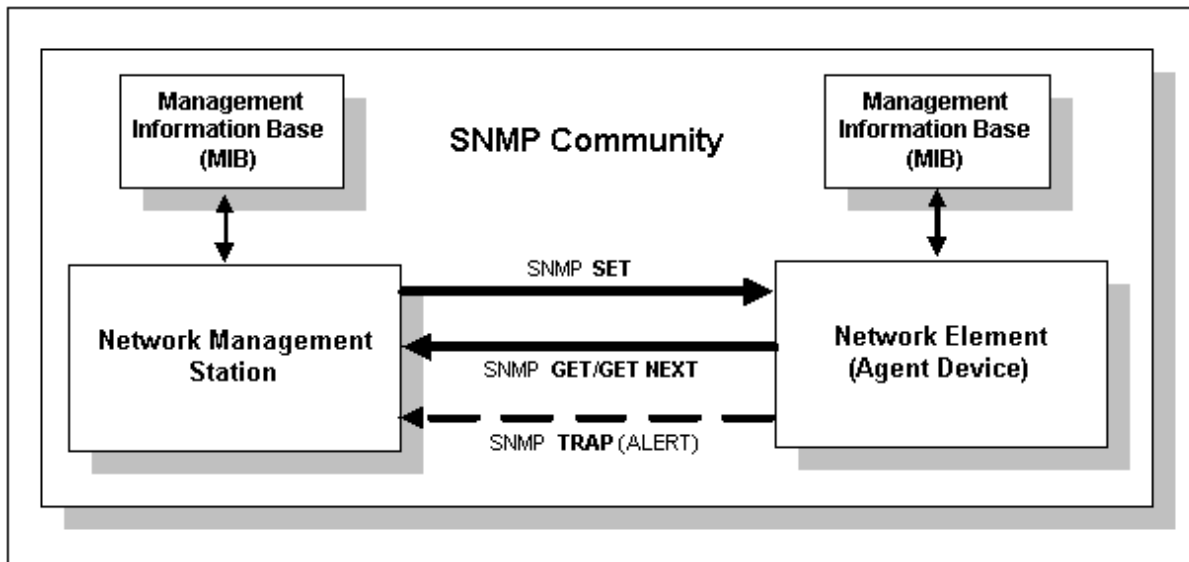
ความคิดที่ไม่ถูกต้องที่จะใช้โปรโตคอล TCP ก็เพราะว่าโปรโตคอล TCP อันที่จริงก็ไม่เหมาะสมกับทุกระบบงานโดยเฉพาะกับระบบเครือข่ายที่ไม่สมบูรณ์ หรือคับคั่งสูง โปรโตคอล SNMP ถูกคาดหวังว่าสามารถทำงานได้ดีแม้ในระบบเครือข่ายที่ไม่สมบูรณ์ แต่ถ้าระบบเครือข่ายมีปัญหาอยู่ และยังมีระบบจัดการเครือข่ายที่เพิ่มปัญหาเข้าไปอีก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

โปรโตคอล SNMP ใช้พอร์ต UDP หมายเลข 161 สำหรับส่ง และรับแบบการร้องขอข้อมูล และใช้พอร์ตหมายเลข 161 สำหรับรับเมสเสจชนิดแทรปจากเอเจนต์ของอุปกรณ์เครือข่ายที่ถูกจัดการ ทุกอุปกรณ์เครือข่ายต้องใช้พอร์ตหมายเลขดังกล่าวเป็นหมายเลขดีพอลต์ แต่อย่างไรก็ตามบางผู้ผลิตอนุญาตให้เปลี่ยนหมายเลขพอร์ต ซึ่งเมเนเจอร์ต้องรับทราบ และเปลี่ยนหมายเลขพอร์ตให้ตรงกับอุปกรณ์เครือข่ายเพื่อให้สามารถติดต่อรับส่งเมสเสจได้

4.1.2 SNMP คอมมูนิตี (SNMP Communities)

สำหรับ SNMPv1 และ SNMPv2 ที่เป็นที่ยอมรับ จะใช้ระบบคอมมูนิตีในการสร้างความปลอดภัย ในการรับส่งข้อมูลระหว่างเมเนเจอร์ และเอเจนต์ โดยทั่วไปเอเจนต์จะถูกตั้งค่าให้มีคอมมูนิตี 3 ประเภท โดยวิธีการตั้งชื่อ นั่นคือ อ่านได้อย่างเดียว สามารถอ่านเขียน และแทรป ชื่อคอมมูนิตี หรือคอมมูนิตีสตริง อันที่จริงทำงานเสมือนเป็นรหัสผ่าน โดยผู้ผลิตทั่วไปจะให้คอมมูนิตีสตริง ชื่อพบลิก (Public) สำหรับการอ่านได้อย่างเดียว คอมมูนิตีสตริง ชื่อไพรเวต (Private) สำหรับการอ่าน และเขียน หรือเซตตั้งตั้งค่า เป็นสิ่งที่ดี ที่จะเปลี่ยนชื่อคอมมูนิตีสตริงที่เป็นดีพอลต์ให้เป็นชื่อเฉพาะเพื่อเพิ่มระดับความปลอดภัย การสร้างแทรป เพื่อแจ้งผู้ดูแลระบบเครือข่ายเมื่อมีการพยายามเข้ามาตั้งค่า หรือร้องขอข้อมูลจากตัวเอเจนต์ด้วยชื่อคอมมูนิตีสตริงที่ไม่ถูกต้อง หรือไม่ตรงกับที่กำหนดก็เป็นสิ่งที่ดี ก็เพราะเป็นการแจ้งเตือนว่าอาจเกิดมีผู้ไม่หวังดีพยายามเข้ามาเจาะระบบเครือข่าย

เนื่องจากชื่อคอมมูนิตีสตริงเสมือนเป็นรหัสผ่านของระบบจัดการเครือข่าย ดังนั้นการตั้งชื่อคอมมูนิตีสตริง ก็ควรตั้งตามกฎการตั้งรหัสผ่านของเซิร์ฟเวอร์ เช่น ไม่เป็นคำในพจนานุกรม คำควรมีทั้งตัวเล็กตัวใหญ่รวมทั้งตัวเลข เป็นต้น

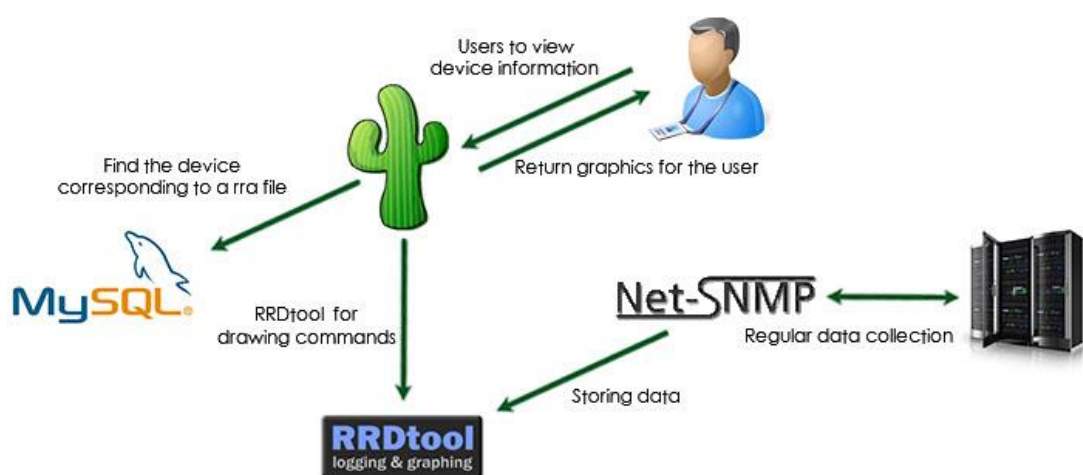


ภาพที่ 4-2 แสดงโครงสร้างการทำงานของ SNMP Community [4]

แต่อย่างไรก็ตามระดับความปลอดภัยด้วยคอมมินิตีส์ตริงก็ยังต่ำอยู่ เนื่องจากคอมมินิตีส์ตริงถูกส่งแบบข้อความธรรมดาไม่มีการเข้ารหัส ทำให้ง่ายต่อผู้บุกรุกที่มีความชำนาญสูงสามารถทำการดักจับชื่อคอมมินิตีส์ตริงได้ และใช้มันเป็นจุดเริ่มต้นในการเจาะเข้าระบบเครือข่าย ดังนั้นจึงได้มีออกข้อกำหนดเพิ่มระดับความปลอดภัยให้สูงขึ้นในมาตรฐาน SNMPv3 แต่อย่างไรก็ตามยังมีวิธีการลดระดับความเสี่ยงต่อการเจาะระบบ ก็คือการติดตั้งไฟร์วอลล์ (Firewall) ซึ่งสามารถกำหนดให้ไฟร์วอลล์อนุญาตเฉพาะโฮสต์ที่รู้จักเข้ามาจัดการระบบเครือข่ายได้เท่านั้น เป็นสิ่งสำคัญที่ต้องตระหนักว่าถ้ามีใครซักคนสามารถอ่านเขียนอุปกรณ์เครือข่ายด้วย SNMP ก็คือสามารถเข้ามาควบคุมระบบเครือข่ายได้ เช่น ปิดพอร์ตเราเตอร์ การเปลี่ยนตารางเราเตอร์ซึ่งทำให้ระบบเครือข่ายล่มเหลวได้ อีกวิธีการหนึ่งในการเพิ่มระดับความปลอดภัย คือการใช้ฟังก์ชัน VPN (Virtual Private Network) เนื่องจากทราฟฟิกของ VPN จะถูกเข้ารหัสไว้ ทำให้ดักจับได้ยาก อีกวิธีการหนึ่งแบบง่าย ๆ คือการเปลี่ยนชื่อคอมมินิตีส์ตริงอย่างสม่ำเสมอ แต่ก็เป็นการยากสำหรับระบบเครือข่ายขนาดใหญ่ที่จำนวนเมเนเจอร์ และเอเจนต์จำนวนมาก

4.1.3 ภาพรวมการทำงานของ SNMP Service และระบบ Cacti

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



ภาพที่
4-3
แสดง

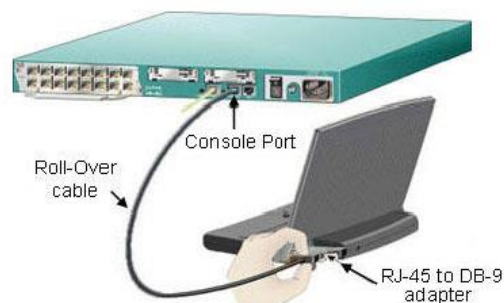
โครงสร้างการทำงานของ cacti และ SNMP Service [\[5\]](#)

4.2 ขั้นตอนการเปิดใช้งาน SNMP

โดยอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย ที่ทางมหาวิทยาลัยเทคโนโลยีราชมงคลพระนครใช้งานอยู่มีความหลากหลาย รวมถึงระบบปฏิบัติการที่ใช้อยู่ด้วยเช่นกัน ดังนั้นขั้นตอนต่อไปนี้จะแสดงวิธีการในการเปิด SNMP Service ของอุปกรณ์แต่ละประเภท

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 การแบ่งตามประเภทของอุปกรณ์หรือแบ่งได้จากลักษณะการทำงาน โดยมีวิธีการดังนี้คือ ไปที่แถบเมนู Console เลือกเมนู Graph Trees คลิกที่ปุ่ม Add เพื่อทำการสร้าง Graph Trees ทำการกำหนดชื่อให้กับ Graph Trees โดยเริ่มจากการสร้างส่วนที่จะนำมาเป็น Header สำหรับ Tree ก่อนแล้วจึงค่อยนำอุปกรณ์มาไว้ใน Tree นี้ ดังภาพที่ 4-75

The screenshot displays the 'Graph Trees' management interface. At the top, there's a navigation bar with tabs: Console, Graphs, Syslog, Thold, Webmin, FlowView, Monitor, and Weathermap. Below this, a status bar indicates 'Logged in as admin (Logout)'. The main content area is divided into three sections:

- Graph Trees**: A table showing existing trees. The 'Add' button is highlighted with a red box and a yellow circle labeled '1'.
- Graph Trees [new]**: A form to create a new tree. The 'Name' field is set to 'Building_1' and is highlighted with a red box. The 'Sorting Type' is set to 'Manual Ordering (No Sorting)'. The 'Create' button is highlighted with a red box and a yellow circle labeled '2'.
- Graph Trees [edit: Building_1]**: A form to edit an existing tree. The 'Name' field is set to 'Building_1' and is highlighted with a red box. The 'Sorting Type' is set to 'Manual Ordering (No Sorting)'. The 'Add' button is highlighted with a red box and a yellow circle labeled '3'.

At the bottom, there are 'Return' and 'Save' buttons.

ภาพที่ 4-76 แสดงวิธีการสร้าง Graph Trees

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

Tree Items

Parent Item
Choose the parent for this header/graph. [root] v

Tree Item Type
Choose what type of tree item this is. Header v

Tree Item Value
Title
If this item is a header, enter a title here. Building 1

Sorting Type
Choose how children of this branch will be sorted. Manual Ordering (No Sorting) v

Graph Trees [edit: Building_1]

Name
A useful name for this graph tree. Building_1

Sorting Type
Choose how items in this tree will be sorted. Manual Ordering (No Sorting) v

Tree Items

Expand All Collapse All

Item	Value
[-] Building 1 (Add)	Heading

ภาพที่ 4-77 แสดงการเพิ่มใส่อุปกรณ์ใน Graph Trees

- ☐ ในหัวข้อ Tree Item Type ให้เลือกเป็น Host
- ☐ ในหัวข้อ Host ให้เลือกอุปกรณ์ที่ทำการสร้าง

Tree Items

Parent Item
Choose the parent for this header/graph. --- Building 1 v

Tree Item Type
Choose what type of tree item this is. Host v

Tree Item Value
Host
Choose a host here to add it to the tree. Device-4 (172.16.254.23) v

Graph Grouping Style
Choose how graphs are grouped when drawn for this particular host on the tree. Graph Template v

Round Robin Archive
Choose a round robin archive to control how Graph Thumbnails are displayed when using Tree Export. Hourly (1 Minute Average) v

Cancel Create

Graph Trees [edit: Building_1]

Name
A useful name for this graph tree. Building_1

Sorting Type
Choose how items in this tree will be sorted. Manual Ordering (No Sorting) v

Tree Items Add

Expand All Collapse All

Item	Value		
[-] Building 1 (Add)	Heading	⬇ ⬆	✖
Host: Device-4 (172.16.254.23) (Edit host)	Host	⬇ ⬆	✖

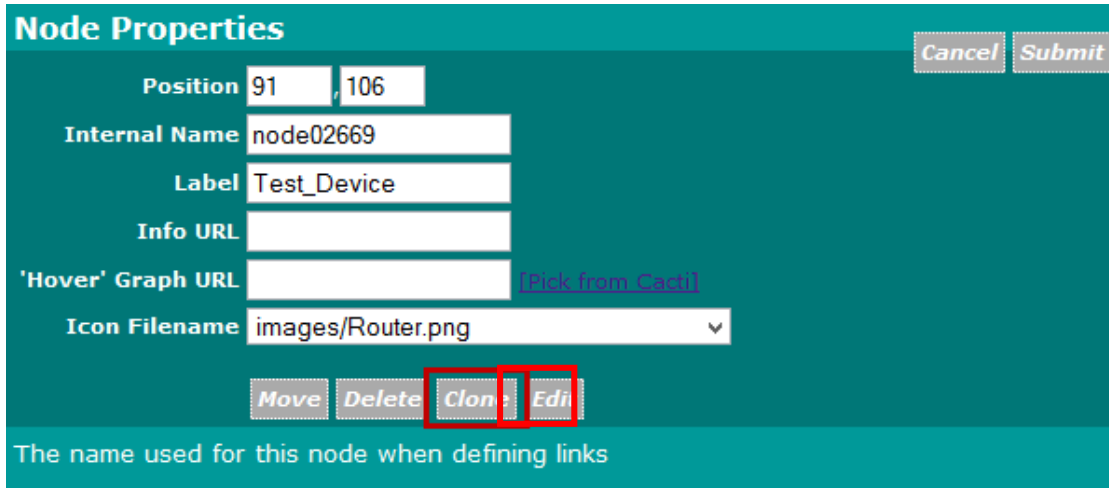
Return Save

ภาพ
ที่ 4-
78

แสดงการบันทึกอุปกรณ์ลงใน Graph Trees

เมนู Clone ใช้สำหรับการคัดลอก Node หรืออุปกรณ์

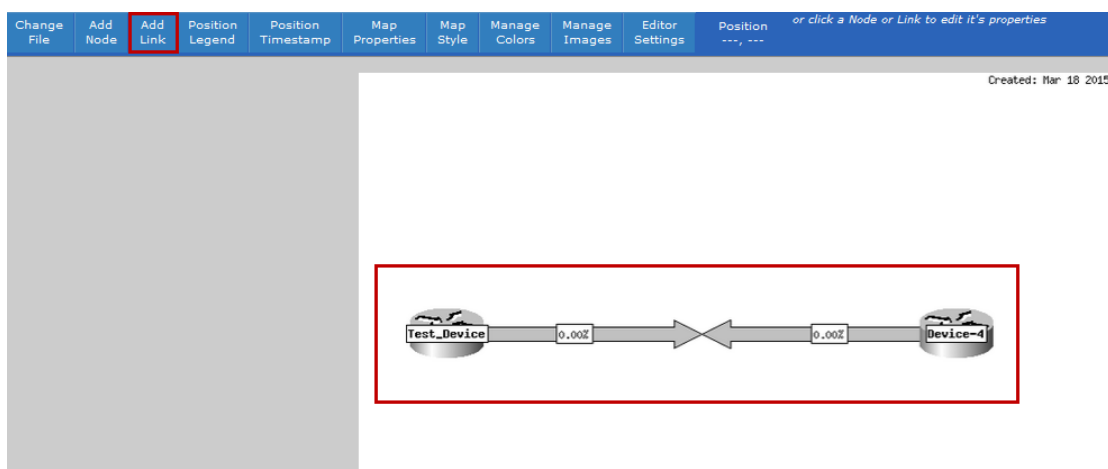
☐ เมนู Edit ใช้สำหรับการแก้ไขรายละเอียดของ Node หรืออุปกรณ์



The image shows a 'Node Properties' dialog box with a teal background. It contains several input fields: 'Position' with values 91 and 106, 'Internal Name' with 'node02669', 'Label' with 'Test_Device', 'Info URL' (empty), and 'Hover Graph URL' (empty). There is a dropdown for 'Icon Filename' showing 'images/Router.png'. At the bottom, there are four buttons: 'Move', 'Delete', 'Clone', and 'Edit'. The 'Clone' and 'Edit' buttons are highlighted with a red rectangle. In the top right corner, there are 'Cancel' and 'Submit' buttons. Below the dialog box, there is a note: 'The name used for this node when defining links'.

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 เพื่อเลือกกราฟที่ต้องการนำมาแสดงบนแผนภาพ weathermap โดยคลิกที่สายสัญญาณ แล้วเลือกที่ [Pick from Cacti]

Link Properties Cancel Submit

Link from 'node02669' to 'node09547'

Maximum Bandwidth Into 'node02669' bits/sec

Maximum Bandwidth Out of 'node02669' ☒ Same As 'In' or bits/sec

Data Source

Link Width pixels

Info URL

'Hover' Graph URL

IN Comment ▾

OUT Comment ▾

Delete Link Edit Vert Horiz Via

This is where help appears for links

ภาพที่ 4-94 แสดงการกำหนด Data Source