บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎีที่เกี่ยวข้อง

2.1.1 Network Monitoring (การดูแลระบบเครือข่าย)

ปัจจุบันนี้ระบบเครือข่ายมีความซับซ้อนมากขึ้น เพราะเทคโนโลยีที่ก้าวหน้าทำให้การบริหารจัดการระบบเครือข่ายไม่ใช่แค่เพียงติดตั้งเพื่อให้สามารถใช้งานได้เพียงอย่างเดียวแค่นั้น เพราะยังต้องมีการตรวจสอบเฝ้าระวังประสิทธิภาพการทำงานของระบบเครือข่าย เพื่อทำการบำรุงรักษาให้ระบบทำงานได้อย่างมีประสิทธิภาพสูงสุดและต่อเนื่อง การลดลงหรือถดถอยของประสิทธิภาพการทำงานของระบบเครือข่ายนั้น ในบางระบบงานอาจทำให้เกิดความเสียหายเป็นมูลค่าที่นับไม่ถ้วนต่อองค์กร หรือหน่วยงาน เช่น ระบบเครือข่ายล่ม ระบบการเงินธนาคาร เป็นต้น และนี่คือที่มาของการทำ Network Monitoring

2.1.2 Network Monitoring คืออะไร

Network Monitoring คือ การเฝ้าระวังระบบเครือข่ายเพื่อไม่ให้เกิดความเสียหายต่อระบบโดยการเฝ้าระวังการทำงานของระบบเครือข่ายและคอยบันทึกสถานะ การทำงานต่าง ๆ ของแต่ละอุปกรณ์ในเครือข่ายและสามารถแจ้งเตือนให้ผู้ดูแลระบบรับรู้ หากมีส่วนใดส่วนหนึ่งในระบบเกิดทำงานผิดพลาด เช่น เครือข่ายช้าผิดปกติ ส่งเอกสารภายในเครือข่ายมีปัญหา หรือ หน้าเว็บไซต์ไม่สามารถเข้าถึงได้เป็นต้น ซึ่งเมื่อพบข้อผิดพลาดก็จะสามารถแก้ไขได้ทันท่วงทีก่อนที่ระบบจะมีปัญหามากขึ้นจนจำไปสู่ความเสียหายทั้งระบบ นอกจากนี้จะช่วยให้สามารถดูแลอุปกรณ์ Network จำนวนมากที่อยู่ในพื้นที่เดียวกันได้ทั่วถึง หรืออยู่ห่างออกไปได้อย่างครอบคลุม

2.1.3 โพรโทคอล SNMP คืออะไร

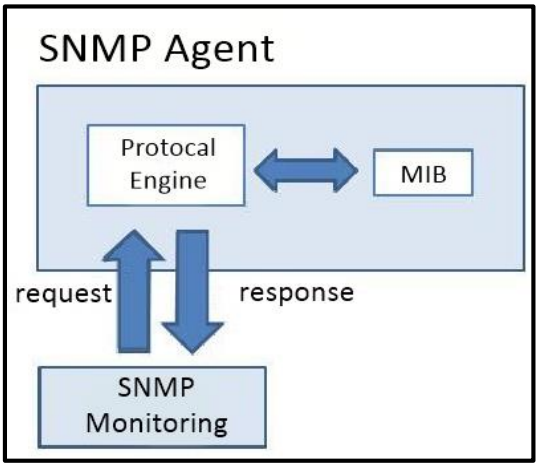
Simple Network Management Protocol เป็นโพรโทคอลที่ประยุกต์เพื่อใช้ในการกำหนดรูปแบบและวิธีการจัดการเครือข่าย ซึ่งจะเป็นการจัดการเครือข่ายใน TCP/IP อุปกรณ์เครือข่ายที่เป็นเอเจนต์ (อุปกรณ์ใด ๆ ที่มีฟังก์ชันให้ตรวจสอบและปรับเปลี่ยนการทำงานได้) โดยจะเป็นตัวกลางในการดูข้อมูลการทำงานของอุปกรณ์ภายในเครือข่าย โดยทำงานผ่าน โพรโทคอล SNMP

ให้ Node Js เป็นตัวกลางในการร้องขอข้อมูลการทำงานจากอุปกรณ์เครือข่ายที่เราต้องการ สามารถใช้ SNMP ในการดูค่าการทำงานต่าง ๆ ของอุปกรณ์ อุปกรณ์เหล่านี้อาจมีส่วนการทำงานที่เป็นซอฟท์แวร์และฮาร์ดแวร์และมี SNMP AGENT เชื่อมต่อจะนำข้อมูลจากส่วนซอฟท์แวร์หรือฮาร์ดแวร์เมื่อ NMS ร้องขอข้อมูล และปรับเปลี่ยนการ ทำงานของซอฟท์แวร์หรือฮาร์ดแวร์ เมื่อ NMS สั่งงาน โดยมีการแจ้งยืนยันสิทธิ์ในรูปรหัสผ่านว่า NMS จะมีอำนาจหน้าที่ในการร้องขอและปรับค่า ปัจจุบันโพรโทคอล SNMP ได้รับความนิยมและใช้กันอย่างแพร่หลายในการจัดการอุปกรณ์ ในระบบเครือข่าย โพรโทคอล SNMP ช่วยให้ผู้ดูแลระบบเครือข่ายสามารถรวบรวมข้อมูล เพื่อนำไปวิเคราะห์ค้นหาปัญหาและแก้ไขปัญหาความผิดพลาดของระบบเครือข่ายที่เกิดขึ้นอีกทั้งใช้ในการจัดการประสิทธิภาพและการวางแผนการพัฒนาของระบบเครือข่ายองค์กรในอนาคต

ส่วนประกอบของ โพรโทคอล SNMP ประกอบไปด้วย 3 ส่วนหลัก

2.1.3.1 ส่วนควบคุมการจัดการ (Management Console) หน้าที่รับผิดชอบ คือ ตรวจตราและควบคุมเอเจนต์โดยตัวควบคุมจะส่งคำสั่งสอบถามหรือคำสั่งปรับค่าของเอเจนต์ในเครือข่ายหนึ่ง อาจจะมีตัวควบคุมเพียงตัวเดียวหรือหลายเครื่องดูแลจัดการเอเจนต์จำนวนมากได้

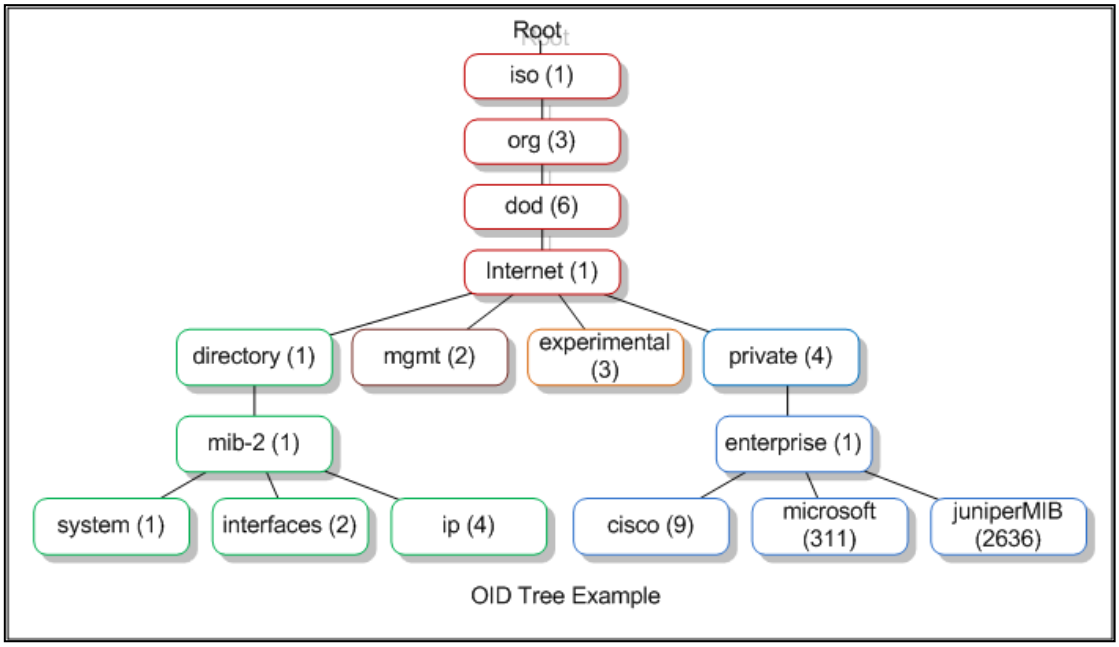
2.1.3.2 ส่วนจัดการเอเจนต์ (Management Agent) อุปกรณ์ที่เป็นเอเจนต์อาจจะเป็น พีซี สวิตซ์ เราเตอร์ และอุปกรณ์ด้านเครือข่าย ในกรณีที่ส่งข้อมูลไปยังระบบได้นั้นที่ตัวอุปกรณ์จำเป็นต้องมี โพรโทคอล SNMP Agent ฝังตัวอยู่ในอุปกรณ์ เมื่อส่วนควบคุมร้องขอข้อมูลข้อมูลก็จะถูกส่งไปยังสถานีจัดการเครือข่าย โดยก่อนจะทำการส่งข้อมูลไปยังสถานีจัดการเครือข่ายได้นั้นโดยส่วนใหญ่จะมีการตรวจสอบสิทธิ์ในรูปแบบของค่าคอมมิวนิตี้ (Community) ว่ามีสิทธิ์ในการร้องขอข้อมูลหรือไม่



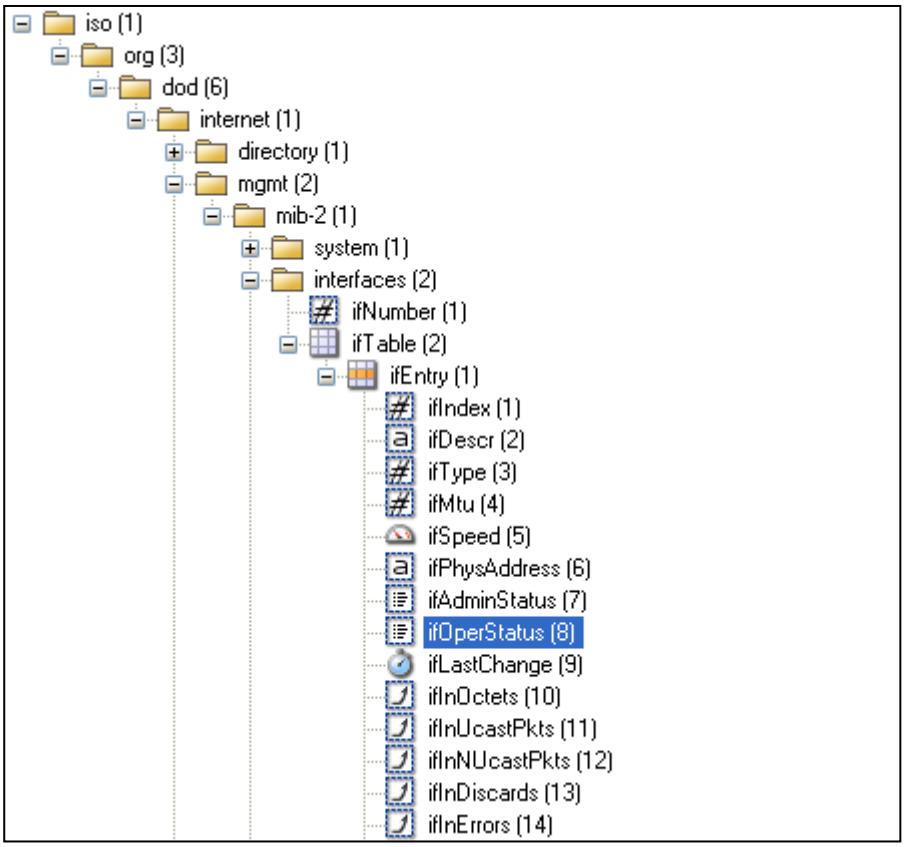
ภาพที่ 2-1 แสดงโครงสร้างของเอเจนต์

2.1.4 หมายเลข OID

SMNP Manager สามารถตั้งค่าหรือดึงค่าจากแต่ละอุปกรณ์ในที่นี่คือแต่ละตัว โดยจะใช้ OID หรือ MIB ของแต่ละอุปกรณ์เพื่อดูค่าการทำงานต่าง ๆ โดยแต่ละอุปกรณ์จะมีค่า MIB ที่แตกต่างกัน และค่า MIB แต่ละค่าจะมีค่าการทำงานต่างกันไป จะเลือกใช้ค่า MIB ที่ต้องการดูส่งไปหาตัวอุปกรณ์ก็จะได้ค่าการทำงานกลับมา และนำข้อมูลที่ได้มาวิเคราะห์และแสดงผลตามรูปแบบที่เหมาะสม ผ่านหน้าเว็บใช้ผู้ใช้สามารถตรวจดูการทำงานต่าง ๆ ของแต่ละอุปกรณ์ผ่านหน้าเว็บได้สะดวกรวดเร็วมากยิ่งขึ้นและได้นำข้อมูลที่ได้ไปวิเคราะห์และปรับปรุงแก้ไขระบบเครือข่ายให้ใช้งานได้มีประสิทธิ์ภาพมากยิ่งขึ้น ในตัวเอเยนต์ค่าพารามิเตอร์จะถูกจัดเรียงตามโครงสร้างต้นไม้ SNMP และจะใช้หมายเลข OID (Object Identifier) เพื่อเจาะจงไปยังพารามิเตอร์ที่ต้องการไม่ว่าจะเพื่อตั้งค่า หรือตรวจสอบข้อมูล ตัวหมายเลข OID จากที่กล่าวมาแล้วก็คือชุดของตัวเลขที่คั่นด้วยเครื่องหมายจุดเพื่อแยกแยะหาตำแหน่ง ในแต่ละตัวเอเยนต์จะมีฐานข้อมูลที่เป็นเสมือนกับสมุดบันทึกตำแหน่งของออบเจ็กต์ทั้งหมดรวมทั้งหมายเลขและชื่ออ้างอิงที่เรียกว่า MIB (Management Information Base) โดยที่ MIB จะจัดเรียงชื่อ, หมายเลข OID, ชนิดข้อมูล, สิทธิ์การอ่านและเขียนรวมทั้งคำอธิบายสั้น ๆ สำหรับแต่ละออบเจ็กต์ที่อยู่ในตัวเอเยนต์



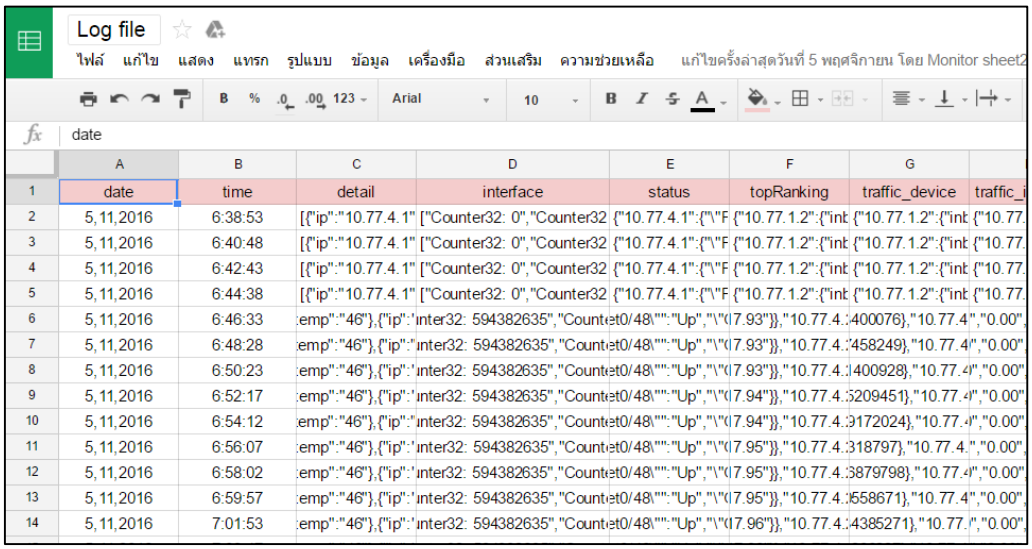
ภาพที่ 2-2 ตัวอย่าง OID Tree



ภาพที่ 2-3 ตัวอย่างข้อมูล OID

2.1.5 Google Sheets

Google Sheets เพื่อนำมาใช้สร้าง Sheet ในการเก็บข้อมูล Log แทนการจัดเก็บลง Database เพื่อลดค่าใช้จ่ายในการติดตั้งเครื่อง Server ลดค่าซ่อมบำรุง ลดความเสียหายที่อาจจะเกิดขึ้นกับเครื่อง Server และยังใช้งานสะดวกมีพื้นที่จัดเก็บเพียงพอ สามารถดูข้อมูลจากที่ไหนก็ได้ และยังสามารถแปลงข้อมูลให้เป็น API เพื่อนำออกมาแสดงผลทางหน้าเว็บเป็นกราฟ Google Sheet สามารถตอบสนองการใช้งานได้เป็นอย่างดี ผู้ใช้สามารถเข้าถึงได้จากคอมพิวเตอร์ทุกเครื่อง Web Browser

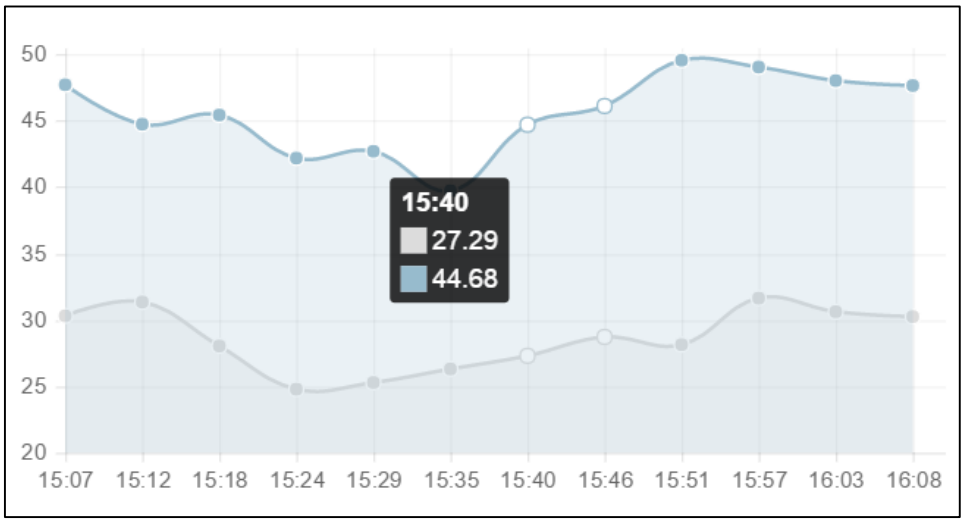


	A	B	C	D	E	F	G	
1	date	time	detail	interface	status	topRanking	traffic_device	traffic_i
2	5,11,2016	6:38:53	[{"ip":"10.77.4.1"	["Counter32: 0","Counter32	{"10.77.4.1":{"\"F	{"10.77.1.2":{"int	{"10.77.1.2":{"int	{"10.77.
3	5,11,2016	6:40:48	[{"ip":"10.77.4.1"	["Counter32: 0","Counter32	{"10.77.4.1":{"\"F	{"10.77.1.2":{"int	{"10.77.1.2":{"int	{"10.77.
4	5,11,2016	6:42:43	[{"ip":"10.77.4.1"	["Counter32: 0","Counter32	{"10.77.4.1":{"\"F	{"10.77.1.2":{"int	{"10.77.1.2":{"int	{"10.77.
5	5,11,2016	6:44:38	[{"ip":"10.77.4.1"	["Counter32: 0","Counter32	{"10.77.4.1":{"\"F	{"10.77.1.2":{"int	{"10.77.1.2":{"int	{"10.77.
6	5,11,2016	6:46:33	emp":"46"},{"ip":"	nter32: 594382635","Counte	t0/48\"":"Up","\"(7.93"}},"10.77.4.		400076},"10.77.4	"0.00",
7	5,11,2016	6:48:28	emp":"46"},{"ip":"	nter32: 594382635","Counte	t0/48\"":"Up","\"(7.93"}},"10.77.4.		458249},"10.77.4	"0.00",
8	5,11,2016	6:50:23	emp":"46"},{"ip":"	nter32: 594382635","Counte	t0/48\"":"Up","\"(7.93"}},"10.77.4.		400928},"10.77.4	"0.00",
9	5,11,2016	6:52:17	emp":"46"},{"ip":"	nter32: 594382635","Counte	t0/48\"":"Up","\"(7.94"}},"10.77.4.		5209451},"10.77.4	"0.00",
10	5,11,2016	6:54:12	emp":"46"},{"ip":"	nter32: 594382635","Counte	t0/48\"":"Up","\"(7.94"}},"10.77.4.		3172024},"10.77.4	"0.00",
11	5,11,2016	6:56:07	emp":"46"},{"ip":"	nter32: 594382635","Counte	t0/48\"":"Up","\"(7.95"}},"10.77.4.		318797},"10.77.4.	"0.00",
12	5,11,2016	6:58:02	emp":"46"},{"ip":"	nter32: 594382635","Counte	t0/48\"":"Up","\"(7.95"}},"10.77.4.		3879798},"10.77.4	"0.00",
13	5,11,2016	6:59:57	emp":"46"},{"ip":"	nter32: 594382635","Counte	t0/48\"":"Up","\"(7.95"}},"10.77.4.		558671},"10.77.4	"0.00",
14	5,11,2016	7:01:53	emp":"46"},{"ip":"	nter32: 594382635","Counte	t0/48\"":"Up","\"(7.96"}},"10.77.4.		4385271},"10.77.4	"0.00",

ภาพที่ 2-4 รูปภาพตัวอย่าง Google Sheets ที่ใช้จัดเก็บ Log

2.1.6 รายงานสรุปสถานะของอุปกรณ์ (Graph)

การนำข้อมูลที่ได้จากการวิเคราะห์มาแสดงในรูปแบบของ Report สรุปผลการทำงานทั้งหมดในแต่ละช่วงเวลาและแต่ละอุปกรณ์จะมีค่าที่นำมาใช้แสดงต่าง ๆ กันไป เพื่อช่วยในการตรวจสอบก็จะสามารถทราบถึงปัญหา และจุดที่ทำให้เกิดปัญหา ทำให้สามารถแก้ไขปัญหาได้อย่างรวดเร็ว ช่วยให้มองเห็นภาพรวมของระแบบเครือข่ายได้ง่ายขึ้น



ภาพที่ 2-5 รูปภาพตัวอย่าง Graph Traffic

2.1.7 เครื่องบริการ (Server)

เครื่องคอมพิวเตอร์เครื่องหลักในระบบเครือข่าย (network) หนึ่ง ๆ ทำหน้าที่เป็นตัวคุมคอมพิวเตอร์เครื่องอื่น ๆ ที่มาเชื่อมต่อในเครือข่ายเดียวกัน คอมพิวเตอร์ เครื่องนี้มีหน้าที่จัดการดูแลว่า คอมพิวเตอร์เครื่องใดขอใช้อุปกรณ์อะไร โปรแกรมอะไร แฟ้มข้อมูลใด เพื่อจะได้จัดการส่งต่อไปให้ในขณะเดียวกัน ก็จะเป็นที่เก็บข้อมูลและโปรแกรมที่คอมพิวเตอร์ในเครือข่ายจะมาเรียกไปใช้ได้

2.1.8 API

API (Application Programming Interface) คือช่องทางการเชื่อมต่อระหว่างเว็บไซต์หนึ่งไปยังอีกเว็บไซต์หนึ่ง หรือเป็นการเชื่อมต่อระหว่าผู้ใช้งานกับ Server หรือจาก Server เชื่อมต่อไปหา Server ซึ่ง API นี้เปรียบได้เป็นภาษาคอมพิวเตอร์ที่ทำให้คอมพิวเตอร์สามารถสื่อสารและแลกเปลี่ยนข้อมูลกันได้อย่างอิสระ โดยจะใช้ API ทำหน้าที่ช่วยในการเข้าถึงข้อมูลต่าง ๆ หรือจะเป็นการนำข้อมูลต่าง ๆ ออกจากเว็บไซต์ หรือจะเป็นการส่งข้อมูลเข้าไปก็ได้ โดยเจ้าของเว็บไซต์ที่มี API จะกำหนดขอบเขตในการเข้าถึงบริการต่าง ๆ ของทางเว็บไซต์

ประโยชน์ของ API สามารถแบ่งออกมาได้หลายอย่าง ได้แก่

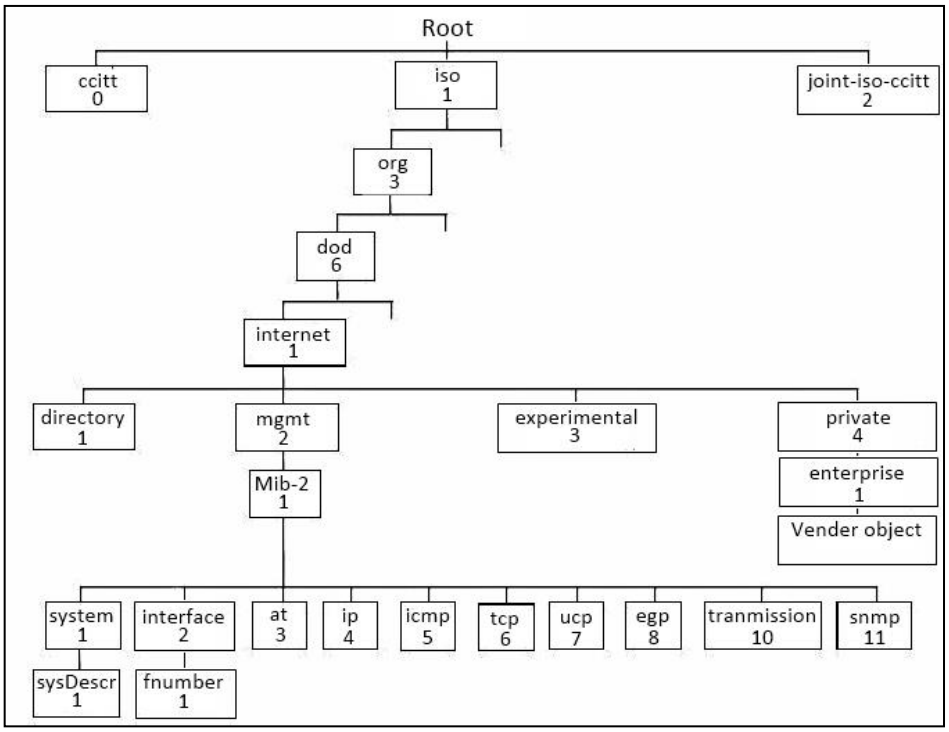
1. ช่วยในการพัฒนาเว็บไซต์หรือ Application ได้ง่ายและรวดเร็วซึ่ง API จะเป็นตัวช่วยที่นักพัฒนาไม่ต้องเข้าไปแก้ไข Code คำสั่งเลยทำให้สะดวกสบายในการใช้งาน
2. ช่วยให้นักพัฒนาเว็บไซต์หรือเจ้าของเว็บไซต์สามารถฐานผู้ชมเว็บไซต์ให้มากขึ้น
3. ทำให้ผู้ใช้งานเว็บไซต์ต่าง ๆ ที่มีการติดตั้ง API ของอีกเว็บไซต์หนึ่งไม่ต้องเข้าหน้าเว็บไซต์ที่เป็นเจ้าของ API เพียงแต่เข้ามายังเว็บไซต์ที่มีการติดตั้ง API เท่านั้น
4. API สามารถรับส่งข้อมูลข้าม Server ได้

```
{
   "one": "two",
   "key": "value"
}
```

ภาพที่ 2-6 รูปภาพตัวอย่าง API

2.1.9 ฐานข้อมูล (Message Intotmation Base-MIB)

เป็นส่วนที่เก็บตัวแปรและค่ากำหนดการทำงานประจำอุปกรณ์ ข้อมูลประจำอุปกรณ์เครือข่ายชิ้นหนึ่งอาจจะมีได้หลากหลายอีกทั้งอุปกรณ์ต่าง ๆ ประเภทกันย่อมมีข้อมูลประจำอุปกรณ์ที่แตกต่างกัน ดังนั้นการสอบถามค่าหรือเปลี่ยนแปลงค่าในฐานข้อมูล จำเป็นจะต้องมีรูปแบบมาตรฐานให้กับอุปกรณ์ทุกประเภท โดยโครงสร้างแบบลำดับชั้น (Tree) ได้ถูกเลือกสำหรับใช้เป็นฐานข้อมูลเพื่อจัดเก็บตัวแปรเหล่านี้ แต่ละโหลดซึ่งแทน Object หนึ่ง ๆ มีชื่อพร้อมทั้งตัวเลขฐานสิบกำกับประจำโหนดเพื่อใช้อ้างอิงลำดับชั้นแรกจะมีโหนดหลักสามโหนดซึ่งกำหนดกลุ่มองค์กรสามกลุ่มคือ ITU-T(0), ISO(1), Joint-IOS-ITU-T (2) ภายใต้โหนด ISO มีโหนดลำดับที่สามคือ org(3) กำหนดองค์กรนานาชาติ และ ส่วนหนึ่งขององค์กรนี้คือ dod (6) Department of Defense และมีโหนด internet(1) เพื่อกำหนดกลุ่มการจัดการเครือข่ายอินเทอร์เน็ต เมื่อต้องการอ้างอิงถึงโหนดใดในโครงสร้างให้เขียนหมายเลขจากรากไปตามเส้นทางถึงโหนดนั้นและคั่นด้วยจุด ลำดับตัวเลขนี้เรียกว่า Object identifier หรือ OID Object ทุกตัวมีนิยามกำหนด ชื่อ แบบข้อมูล สิทธิ์การเข้าถึง คำอธิบายลักษณะและค่าข้อมูล การนิยาม Object มีกฎเกณฑ์ตามข้อกำหนดโครงสร้างฐานข้อมูลสารสนเทศการจัดการ



ภาพที่ 2-7 Object identifier ในโครงสร้างฐานข้อมูลสารสนเทศ

ซึ่งส่วนประกอบทั้งหมดจะทำงานร่วมกันเพื่อให้ผู้ดูแลระบบเครือข่ายสามารถตรวจสอบและควบคุมส่วนประกอบต่าง ๆ ของเครือข่าย

โพรโทคอล SNMP มี 3 เวอร์ชัน

- **SNMP V1** ได้รับการพัฒนาและอนุมัติว่ามันเป็น โพรโทคอลที่จำเป็นสำหรับการใช้งานขนาดใหญ่บนอินเทอร์เน็ต และการค้า ในช่วงเวลานั้นการตรวจสอบมาตรฐานอินเทอร์เน็ตและความปลอดภัยมุ่งเน้นไปที่ โพรโทคอลนี้ ในเวอร์ชัน 1 ยังมีระบบความปลอดภัยที่ต่ำ การยืนยันตัวตนของ clients ถูกออกแบบให้ใช้เพียง community string เท่านั้น ซึ่งมีผลเหมือนกับรหัสผ่านในการส่งผ่านข้อมูล การออกแบบ SNMPv1 สำเร็จโดยกลุ่มองค์กรที่สนับสนุนโดยOSI/IETF/NSF (National Science Foundation)

- **SNMP V2** เป็นการพัฒนามาจากเวอร์ชันที่ 1 มีการปรับปรุงประสิทธิภาพ ความปลอดภัย และการสื่อสารระหว่าง manager โครงสร้างของ MIB ยังคงยึด SNMPv1 ในการใช้งาน และถูกกำหนดไว้ใน RFC 1901, RFC 1905, RFC 1906, RFC 2578

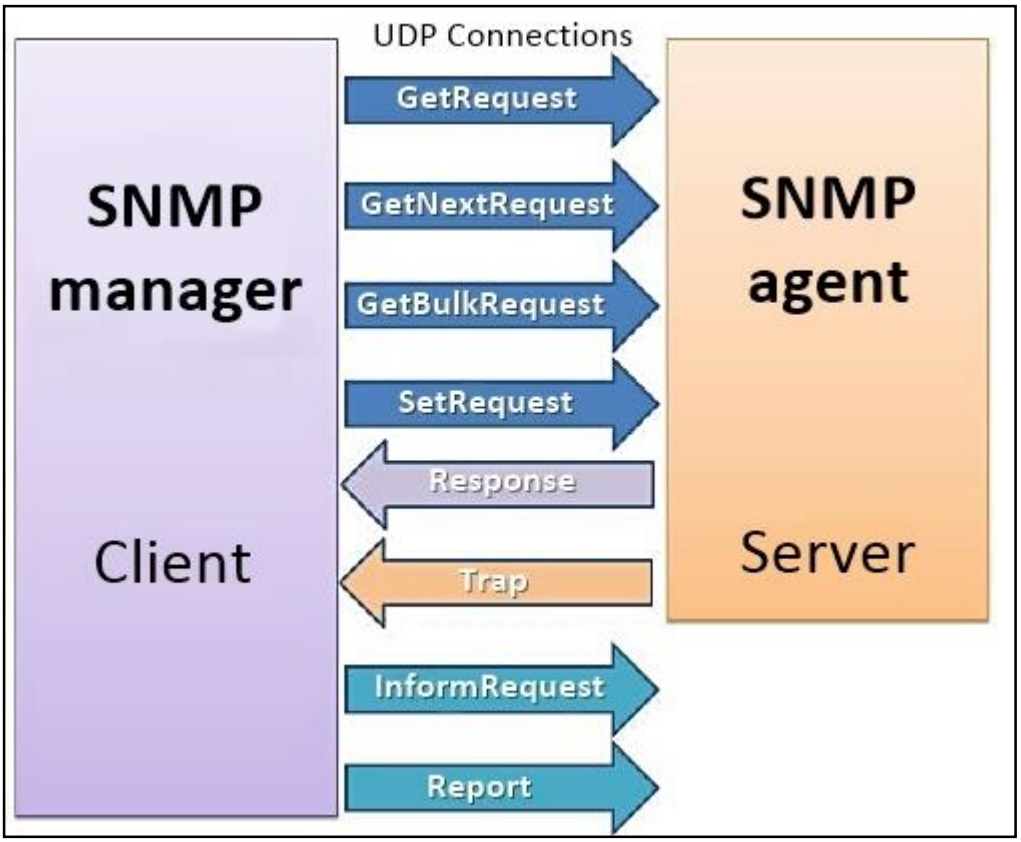
SNMPv2c อยู่ใน RFC 1901-1908 ในระยะแรกเป็นที่รู้จักอย่างไม่เป็นทางการในชื่อ SNMPv 1.5 ซึ่ง SNMPv2c ประกอบด้วย SNMPv2 ที่ปราศจากข้อถกเถียงในเรื่องของความปลอดภัยในรูปแบบใหม่ที่ใช้แทนที่ SNMPv1

SNMPv2u ถูกกำหนดใน RFC 1909-1910 เป็นการพยายามนำเสนอความปลอดภัยที่เพิ่มขึ้นมากกว่าเดิม แต่ปราศจากความซับซ้อนสูงอย่างใน SNMPv2 ความแตกต่างนี้ถูกนำมาเป็นจุดขาย และนำไปใช้พัฒนาต่อเป็นหนึ่งในสองของความปลอดภัยของ SNMPv3

SNMPv2 ยังคงใช้คำสั่ง GET GET-NEXT SET เช่นเดียวกับในเวอร์ชัน 1 แต่อย่างไรก็ตาม เวอร์ชันที่สองได้เพิ่มฟังก์ชั่นบางอย่างเพิ่มเติม อย่างคำสั่ง TRAP ที่ถึงแม้จะมีเหมือนเวอร์ชัน 1 แต่แตกต่างกันในรูปแบบของข้อความที่ใช้และการออกแบบเพื่อแทนที่คำสั่ง TRAP ของเวอร์ชัน 1

SNMPv2 ได้ระบุสองคำสั่งใหม่คือ GET BULK และ INFORM

- **SNMPv3** ถูกออกแบบให้สามารถป้องกันการบุกรุกจากช่องทางการสื่อสารของการจัดการเครือข่ายจากผู้ที่ไม่มีอำนาจหน้าที่หรือสิทธิ์ (Unauthorized) และให้จดจำไว้ว่าการรักษาความปลอดภัยของ SNMPv3 จะปกป้องเฉพาะส่วนระบบจัดการเครือข่ายเท่านั้น ดังนั้นในระบบเครือข่ายจริง ๆ ยังต้องการระบบการรักษาความปลอดภัยอื่น ๆ ที่ป้องกันระบบเครือข่ายทั้งระบบการบุกรุกคุกคามจากช่องทางสื่อสารกับเอเจนต์โดยทั่วไปสามารถแบ่งการบุกรุกทางเทคนิคได้ดังต่อไปนี้



ภาพที่ 2-8 แสดงประเภทคำสั่งของ SNMP v3

(ที่มา : http://www.academia.edu/5383429/Monitor_System,2555)

แบ่งการบุกรุกทางเทคนิคได้ดังต่อไปนี้

- Modification of Information คือการที่ Message SNMP ถูกแก้ไขอย่างไม่พึงประสงค์ โดยผู้ไม่หวังดีระหว่างการทำ transactionทำให้ Message นั้นเสียหาย

- Masquerade คือการบุกรุกแบบการปลอมแปลงตัวจากการเป็นผู้ที่ไม่มีสิทธิ์ให้สามารถทำการจัดการระบบเครือข่ายได้ ซึ่งเป็นการบุกรุกที่ร้ายแรง เพราะสามารถทำอะไรก็ได้เหมือนผู้ดูแลระบบ

- Disclosure คือการบุกรุกจากผู้ที่ไม่มีสิทธิ์โดยการทำการดักฟังหรือดักจับเพื่อเอาข้อมูลระบบระหว่างการทำ transaction

- Message Stream Modification คือการบุกรุกที่ทำให้ Message SNMP เกิดการจัดลำดับที่ผิดพลาด หรือ ทำให้เกิดการหน่วง หรือส่งซ้ำ ส่งผลกระทบในการจัดการระบบเครือข่าย โดยอาจจะเกิดจากการบุกรุกแบบที่หนึ่งแต่กระทำการอย่างต่อเนื่อง

- Unauthorized Access คือการบุกรุกโดยผู้ไม่มีสิทธิ์โดยการผิดพลาดในการจัดการระบบ

Service ของ SNMPv3 ที่ลดการบุกรุกระบบจัดการเครือข่าย มีดังต่อไปนี้

- Data Integrity การให้ความมั่นใจว่าข้อมูลจะไม่ถูกเปลี่ยนแปลง หรือ ถูกทำลาย โดยผู้ไม่มีสิทธิ์ Data Integrity ป้องกันการแก้ไขข้อมูล โดยเฉพาะ การป้องกันการเขียนทับ การเพิ่มข้อมูลที่ไม่ต้องการ การลบ หรือ การเรียงลำดับข้อมูลใหม่โดยผู้ที่ไม่มีสิทธิ์

- Sequence Integrity ป้องกันการแก้ไขลำดับการส่งเมสเสจจากผู้ไม่พึงประสงค์

- Message Timeliness เป็นการป้องกันการตรวจสอบเมสเซจถูกหน่วงเวลา หรือส่งใหม่โดยใช้หน้าต่างเวลา (Window) เป็นเครื่องมือตรวจสอบ

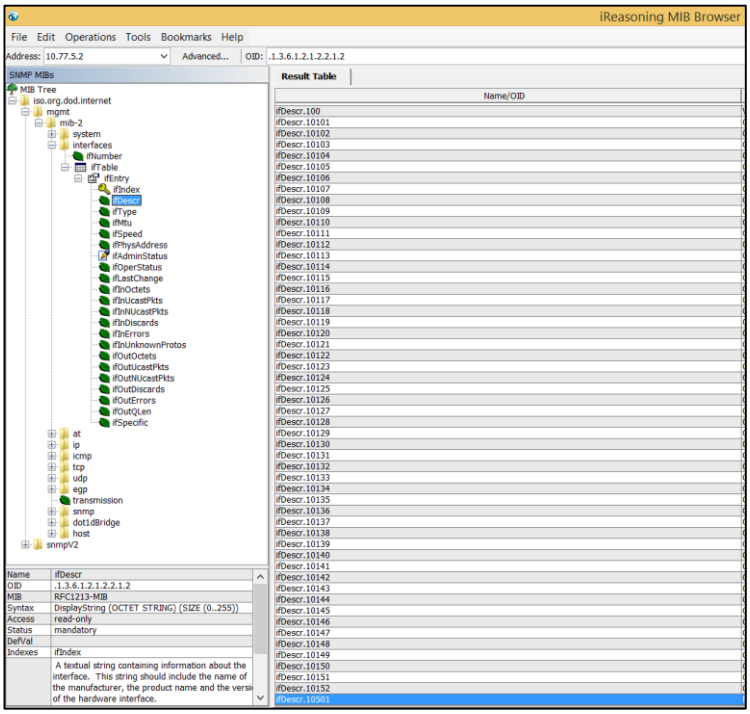
- Authentication ให้การรับรองในการตรวจสอบเอนทิตี้ที่ทำการสื่อสารแบบระหว่างกัน เช่น ระหว่าง NMS และเอเยนต์ ว่ามีตัวตนและสิทธิ์จริง

- Privacy (Confidentiality) ให้ความไว้วางใจว่าข้อมูลจะไม่ถูกเปิดเผยไปยังผู้ไม่สิทธิ์

- Access Control ให้ความมั่นใจว่าแหล่งข้อมูลไม่ถูกใช้โดยผู้ไม่มีสิทธิ์ รวมทั้งการกระทำที่ไม่สิทธิ์ ถึงแม้จะเข้าไปในระบบได้แล้วก็ตาม Access Control นั้นจะทำงานร่วมกับ Authentication เพื่อช่วยพิสูจน์ว่าเอนทิตี้ใดมีสิทธิ์เข้าถึงแหล่งข้อมูลเฉพาะหรือกลุ่มข้อมูลที่มีจุดประสงค์พิเศษ

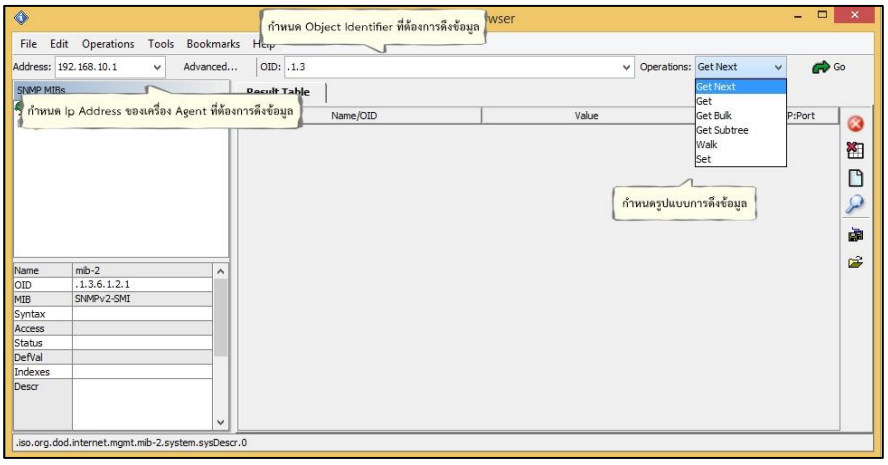
2.1.10 Mib Browser

iReasoning MIB Browser เป็นเครื่องมือที่มีประสิทธิภาพและง่ายต่อการใช้งานที่ขับเคลื่อนโดย iReasoning SNMP API Browser MIB เป็นเครื่องมือที่จำเป็นสำหรับวิศวกรในการจัดการอุปกรณ์เครือข่าย SNMP เปิดการใช้งานและการประยุกต์ใช้ จะช่วยให้ผู้ที่จะโหลดมาตรฐาน MIBs เป็นกรรมสิทธิ์และแม้กระทั่งบาง Mal - formed MIBs นอกจากนี้ยังช่วยให้พวกเขาร้องขอ SNMP ปัญหาในการดึงข้อมูลหรือทำการเปลี่ยนแปลงให้ สามารถรับ SNMP traps คุณลักษณะที่สำคัญ : ที่ใช้งานง่าย GUI เสร็จสมบูรณ์ SNMPv1, V2C และ v3 (USM และ VACM) สนับสนุนสมบูรณ์สนับสนุน SNMPv3 USM รวมทั้ง HMAC - MD5, HMAC - Sha, CBC- DES, CFB128 - AES - 128 อัลกอริทึมที่มีประสิทธิ์ภาพและมีประสิทธิภาพ SMIv1/SMIv2 MIB IPv6 parser รับการสนับสนุนผู้ส่งเข้าสู่ระบบหน้าต่างที่จะแสดงบันทึกของโปรแกรมประยุกต์และแพ็กเก็ต SNMP แลกเปลี่ยนระหว่าง Browser และมุมมองของพอร์ต (การใช้แบนด์วิดท์เปอร์เซ็นต์ข้อผิดพลาด) สำหรับเครือข่ายอินเตอร์เฟซ ที่ดูพอร์ตสวิตช์สำหรับการทำแผนที่สลับมุมมองตารางพอร์ตสำหรับ MIB ตารางผลการดำเนินงานภาพรวมอุปกรณ์ของซิสโก้ภาพรวมอุปกรณ์ เครื่องมือกราฟสำหรับการตรวจสอบจากตัวเลขค่าปิง OID และเครื่องมือ traceroute เครือข่าย SNMP เปรียบเทียบการค้นพบเครื่องมือที่ทำงานบน Windows, Mac OS X, Linux และแพลตฟอร์มยูนิกซ์อื่น ๆ



ภาพที่ 2-9 หน้าจอโปรแกรม iReasoning MIB-Browser

การกำหนดค่าสำหรับการติดต่อกับเครื่อง Agent



ภาพที่ 2-10 การทำงานของโปรแกรม iReasoning MIB-Browser

Address : ผู้ใช้จะต้องระบุหมายเลขเครื่องของ Agent ที่โปรแกรมต้องการเข้าไปอ่านข้อมูล เมื่อผู้ใช้ต้องการอ่านค่าจากเครื่องอื่นจะต้องทำการเปลี่ยนหมายเลข IP ที่ช่องนี้

OID : ทำหน้าที่กำหนดหมายเลข OID ของ Object ที่ต้องการติดต่อใน MIB

Operations : ทำหน้าที่กำหนดการกระทำของของโปรแกรมในการติดต่อกับ Object ภายใน MIB ซึ่งสามารถเลือกรูปแบบการดึงข้อมูลจาก Agent ได้ 5 รูปแบบ ได้แก่

- Get Next ดึงข้อมูลจากเครื่อง Agent ทีละบรรทัด เมื่อกดซ้ำจะดึงข้อมูลในบรรทัดถัดไปมาแสดง
- Get ดึงข้อมูลจากเครื่อง Agent ทีละบรรทัด (จะดึงข้อมูลชุดเดิมออกมาแสดง)
- Get Bulk ดึงข้อมูลจากเครื่อง Agent ทีละชุดออกมาแสดง
- Walk ดึงข้อมูลจากเครื่อง Agent แบบเวลาจริง จนกว่าจะ Stop Operation.
- Set ดึงข้อมูลจากเครื่อง Agent โดยจะมีการกำหนดชนิดของข้อมูลที่ต้องการดึง

ถ้า Agent รองรับการทำงาน SNMP V1 สามารถเลือกget get-next Set Walk ถ้า Agent รองรับการทำงาน SNMP V2 ขึ้นไป สามารถใช้ได้ทั้งหมด

2.1.11 Jquery

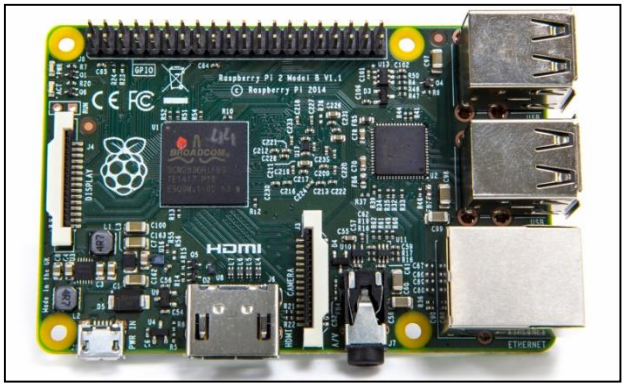
jQuery เป็น JavaScript Library ที่มีการรวบรวม function ของ JavaScript ต่าง ๆ ให้อยู่ในรูปแบบ Patterns Framework ที่สะดวกและง่ายต่อการใช้งาน มีความยืดหยุ่นรองรับต่อการใช้งาน Cross Browser คือไม่ว่าจะใช้งานบน Web Browser ใด ใน Library ของ jQuery จะมีการเลือกใช้ function ที่ เหมาะสมต่อการทำงานและแสดงผลใน Web Browser ที่กำลังทำงานอยู่ ซึ่งช่วยลดปัญหาการทำงานที่ผิดพลาดในฝั่งของ Client ได้ JQuery ถูกพัฒนาให้สามารถเรียกใช้ได้ง่าย เช่นเดียวกับการเขียน Javascript แบบดั้งเดิม ซึ่งสามารถใช้งานร่วมกับ Ajax หรือ DIV ได้ด้วย และที่สำคัญที่สุด Jquery ได้ถูกทดสอบว่าสามารถรองรับ Browser ได้ทุก Broswer ไม่ว่าจะเป็น IE Firefox Safari และอื่น ๆ อีกมากมาย

```
<div id="text"></div>  <div id="get_text"></div>
$(document).ready(function(){
var str = $("#text").text();     // สั่งให้ ตัวแปร "str" เก็บค่า text จาก id="text" เข้ามาเก็บไว้
$("#get_text").text(str); // ใส่ตัวแปร "str" เข้าไปใน id="get_text" ด้วยคำสั่ง .text();
```

ภาพที่ 2-11 ตัวอย่างการใช้งาน jquery

2.1.12 Raspberry Pi 3

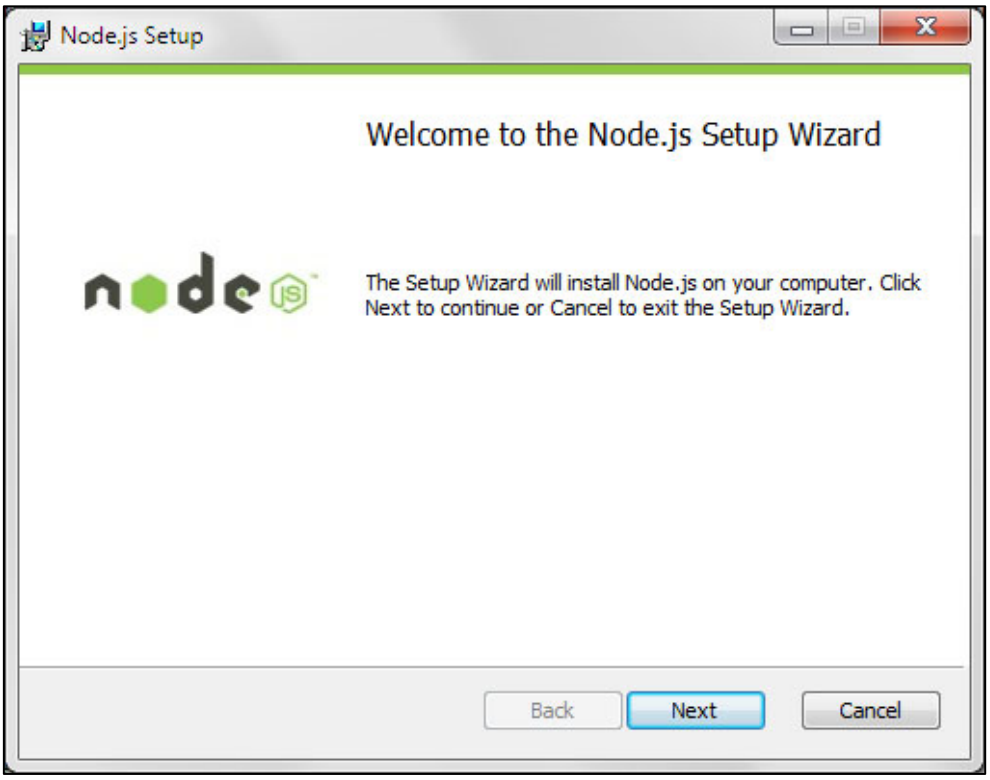
Raspberry pi 3 เป็นคอมพิวเตอร์ขนาดเล็ก สามารถใช้งานกับทีวีหรือหน้าจอคอมพิวเตอร์ในราคาถูก ด้วยขนาดและคุณสมบัติของ raspberry pi เหมาะกับการนำมาทดลองใช้แทนเครื่อง Server ที่ใช้ทำการดึงข้อมูลจากอุปกรณ์ภายในเครือข่าย ช่วยลดต้นทุนในการติดตั้งเครื่อง Server ลดค่าใช้จ่ายลง และลดพื้นที่ในการวางเครื่อง server ลง คุณสมบัติของ Raspberry pi 3 คือ โมดูลคอมพิวเตอร์ Raspberry Pi 3 (CM3) ความแรงเร็วยิ่งกว่า version ก่อนหน้านี้ รุ่น CM3 ประกอบด้วย RAM ขนาด 1GB และระบบประมวลผล BCN2837 ขนาด 64 บิต แบบเดียวกับที่ใช้ใน Raspberry Pi 3 แต่พื้นที่ติดตั้งน้อยลง CM3 เหมาะอย่างยิ่งสำหรับผู้ที่ต้องการใช้ Raspberry Pi กับการออกแบบที่ครบวงจร อุปกรณ์มาตรฐานนี้มาพร้อมกับ eMMC ขนาด 4GB และช่องเสียบการ์ด SD อุปกรณ์รุ่น lite มีคุณสมบัติเดียวกัน แต่ไม่มี eMMC ขนาด 4GB และช่องเสียบการ์ด SD บอร์ด CMOI V3 รุ่นใหม่ จัดจำหน่ายพร้อมช่องเสียบการ์ด SD เพื่อรองรับอุปกรณ์รุ่น lite



ภาพที่ 2-12 Raspberry Pi

2.1.13 NodeJs

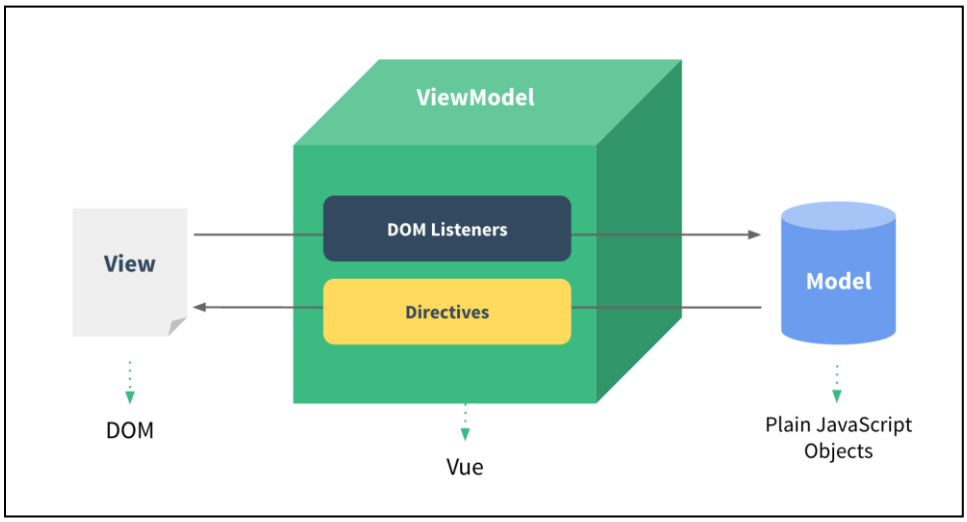
NodeJs เป็น platform ที่มีความสามารถทางด้านความเร็วในการประมวลผล จึงถูกนำมาใช้แทน PHP ที่เคยใช้ในการดึงข้อมูลการทำงานจากอุปกรณ์เครือข่าย ใช้ร่วมกับ npm ที่ช่วยจัดการ package เสริมต่าง ๆ หรือการติดตั้ง module ต่าง ๆ ที่เป็น dependency ของ application ที่ต้องการใช้ ทำให้การทำงานของ backend ทำงานได้ดียิ่งขึ้น Node.js เป็น Cross Platform Runtime Environment สำหรับฝั่ง Server และเป็น Open Source ซึ่งเขียนด้วยภาษา JavaScript Platform ตัวหนึ่งที่ใช้เขียนสำหรับเป็น Web Server ที่ช่วยให้เราทำงานได้ง่ายยิ่งขึ้น และรวดเร็วพร้อมมีตัวช่วยต่าง ๆ ที่เหมาะสม



ภาพที่ 2-13 Nodejs platform

2.1.14 VueJS

VueJs คือ framework ที่ใช้ง่ายและเรียนรู้ได้ไว vue ช่วยจัดการเรื่อง User Interface เพื่อช่วยเรื่องการจัดการหน้าการแสดงผล โดยจะแยก logic การตัดสินใจออกจากการแสดงผล เช่น การซ่อนหรือแสดงซ้ำ ๆ ช่วยแยกหน้าเว็บออกเป็น component ทำให้จัดการง่ายขึ้น ช่วยจัดการเรื่อง Dynamic data ให้ง่ายขึ้น ซึ่งช่วยให้เว็บสามารถทำง่ายได้ไวขึ้น จัดการ data ได้ง่ายและโปรแกรมมีประสิทธิภาพดียิ่งขึ้น สิ่งที่ vue ทำได้ดีคือ การทำ data binding (Data binding คือการผูกข้อมูลในฝั่งของ Code JavaScript เบื้องหลัง เข้ากับ View ที่ Render แล้วเข้าด้วยกัน นั่นคือเมื่อมีการเปลี่ยนแปลงข้อมูลที่ view ก็จะมีการเปลี่ยนแปลงของข้อมูลที่ Code JavaScript เบื้องหลัง และในทำนองเดียวกัน เมื่อมีการเปลี่ยนแปลงข้อมูลที่ Code JavaScript เบื้องหลัง ก็จะมีการเปลี่ยนแปลงของข้อมูลที่ view ด้วย) และการทำ UI Template ซึ่ง 2 อย่างนี้เป็นสิ่งที่จำเป็นในการทำ web แบบ one page app



ภาพที่ 2-14 Concepts Vue

2.1.15 Materiallize

Materialize เป็น front-end framework มีการออกแบบให้รองรับบน เดสก์ท็อป แท็บเล็ต มือถือ เพื่อความสะดวกสะบายในยุคปัจจุบันเน้นไปที่ สีสันสดใส รูปทรงเรขาคณิต หลักการออกแบบ (Design Principle) ของ Material Design ใช้หลักการเลียนแบบ "วัสดุ" (material) เน้นการใช้พื้นผิว (surface) และ ขอบ (edge) ใช้แสงเงาภาพเคลื่อนไหวเหมือนกับแสงเงาการเคลื่อนไหวของวัตถุเชิงกายภาพ เป็นการออกแบบที่ "ตั้งใจนำเสนอ" (intentional) ใช้วิธีการนำเสนอแบบเดียวกับสิ่งพิมพ์กระดาษ เช่น ฟอนต์ ที่ว่าง สีสัน ภาพประกอบแสดงการเคลื่อนไหว (motion) เพื่อบอกความหมาย (meaning) ของการกระทำ

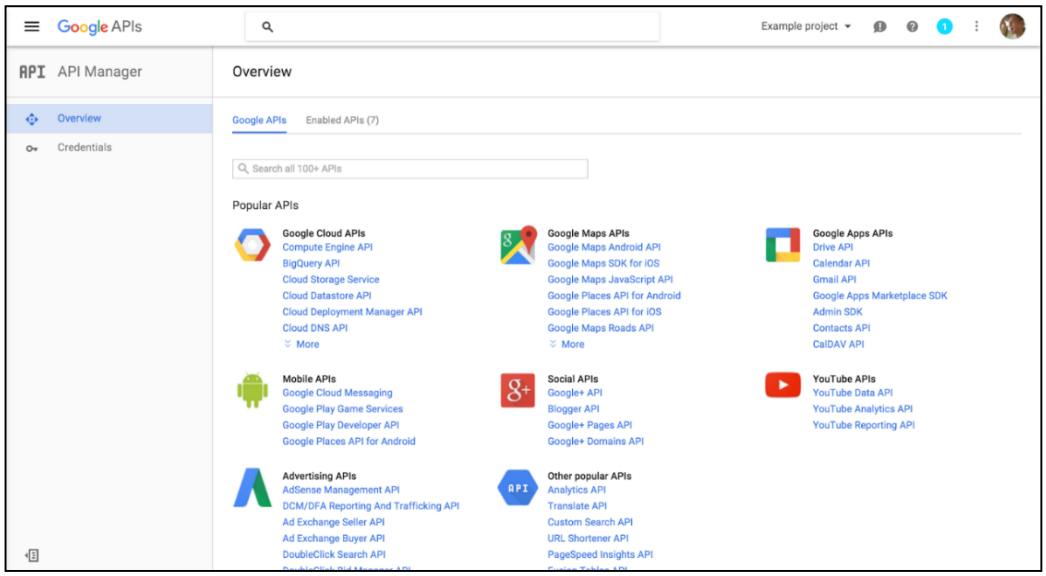
ภาพที่ 2-15 Materialize css framework

2.1.16 Google Developer

Google Developer คือ ระบบที่ทางทีม Google เปิดให้นักพัฒนาระบบเรียกใช้งาน Api ในการเข้าถึงข้อมูลต่าง ๆ ของทาง Google เช่น ดึงข้อมูลผู้ใช้งาน Google ทำ Google login เชื่อมต่อ Google map หรืออื่นๆ อีกมากมายหลายอย่าง Google ทั้งยังรองรับหลายภาษาอีกด้วย เช่น php, java, JavaScript และอื่น ๆ

2.1.17 Google api Console

Google api Console เป็นตัวช่วยจัดการ api ในเรื่องของการดึงและสร้าง api เพื่อนำไปใช้งานต่อ Google api จะช่วยให้เข้าถึง api ได้ง่ายแก้ไขปัญหาเรื่อง require ที่ให้ใช้ได้เหมาะสมกับระบบที่พัฒนาขึ้น มีขั้นตอนการทำ Athen เพื่อป้องกันการเข้าถึงข้อมูลโดยผู้ที่ไม่มีสิทธิ์ในการเข้าถึง ทำให้ api มีความปลอดภัยมากขึ้น

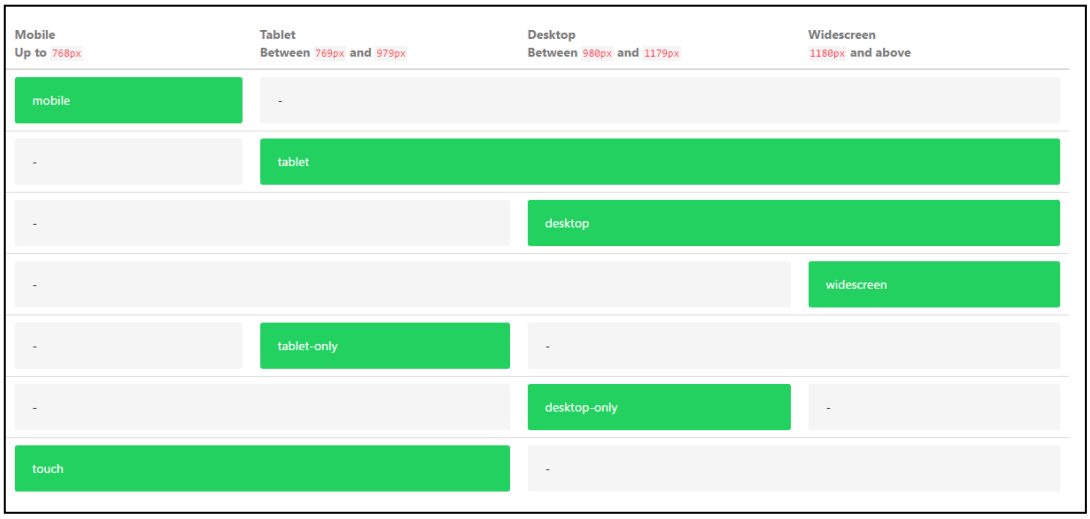


ภาพที่ 2-16 Google api Console

2.1.18 Bulma css framework

Bulma เป็น css framework ตัวนึงที่มีขนาดเล็กเพียง 118 kb โดยตัวมันจะเป็นแค่ css ไม่มี JavaScript บรรจุมาให้จึงทำให้มีขนาดที่เล็ก Bulma จะช่วยจัดการ css ให้เราสามารถเรียกใช้งานโดยไม่ต้องไปสร้าง css เองให้ยุ่งยาก ช่วยให้ผู้พัฒนาเว็บสามารถทำงานได้ง่ายและเร็วยิ่งขึ้นด้วยความที่ Bulma เป็น CSS ไฟล์เดียวจบ ไม่มี JavaScript / รูปภาพอะไรทั้งสิ้น ก็สามารถ Download มาใช้ได้เลยจากเว็บ Bulma CSS Framework หรือ Bulma Github หรือใช้ CDN ก็ได้ ความสามารถหนึ่งของ Flexbox คือ มันสามารถยืดหดตามพื้นที่แบบไม่จำเป็นต้องกำหนด class แบบ .col-md-6 เหมือนใน Bootstrap / Foundation แบบเก่า ๆ หรือจะกำหนดก็ Fix ความกว้างให้ได้ bulma สามารถใช้งานได้ง่ายลองรับการทำงานได้หลายขนาดหน้าจอ โดย Bulma จะรองรับการย่อขยาย หน้าจอ กันได้ 4 แบบคือ

1. mobile จะมีขนาดถึง 768px
2. tablet จะเริ่มที่ขนาด 769px
3. desktop จะเริ่มที่ขนาด 769px
4. widescreen จะเริ่มที่ขนาด 1180px

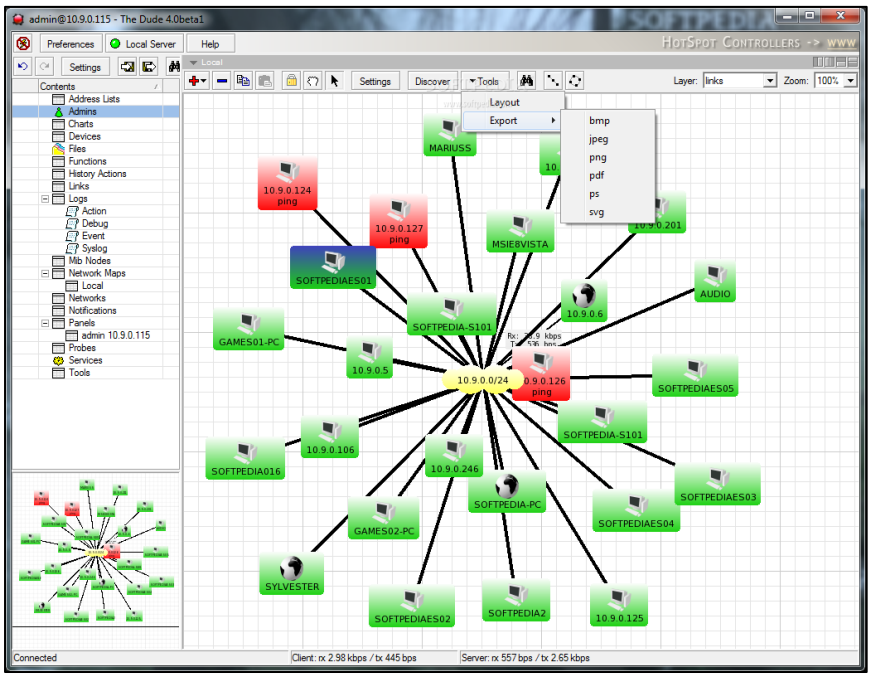


ภาพที่ 2-17 การจัดการ grid Bulma

2.1.19 งานวิจัยที่เกี่ยวข้อง

ตัวอย่างระบบ Network Monitoring

The Dude Network Monitoring เป็นโปรแกรมเป็นฟรีแวร์จากบริษัท MikroTik The Dude จัดอยู่ในโปรแกรมประเภท Network Monitoring จะช่วยจัดการสภาพแวดล้อมของระบบเครือข่ายให้มีประสิทธิภาพ The Dude สามารถดูสถานะของระบบเครือข่ายได้ว่ามีจุดไหนหรือว่าอุปกรณ์ตัวใดทำงานผิดปกติหรือไม่ โดยระบบสามารถสแกนค้นหาอุปกรณ์ Network ในเครือข่ายได้เองและยังมีข้อดีอื่น ๆ อีกมากมาย ยกตัวอย่างเช่น มีระบบ Scan หาอุปกรณ์ในเครือข่ายได้เอง ความสามารถในการค้นหายี่ห้ออุปกรณ์ได้ สามารถตรวจสอบได้ทั้งอุปกรณ์ว่ายังทำงานอยู่หรือไม่ พร้อมแจ้งเตือน สามารถวาดผังของเครือข่ายเองได้ สามารถ Import และ Export ค่าที่ Setting เอาไว้เพื่อ Backup/Restore ได้มี Report รวมให้อุปกรณ์แต่ละตัวด้วยเพื่อสรุปค่าความเสถียรเป็นรายงาน ตรวจสอบ Service บน อุปกรณ์ก็ได้ เช่น HTTP, SMTP, SNMP วาดผังเองก็ได้ รองรับ SNMP v1 และ SNMP v2 สามารถรองรับระบบ Syslog สำหรับอุปกรณ์ Network เป็นต้น สามารถ Monitor อุปกรณ์พร้อม ๆ กันได้หลายเครื่อง ยกตัวอย่างอุปกรณ์เช่น AD Server, Print Server, Router, Firewall, Wireless, File Server เป็นต้น



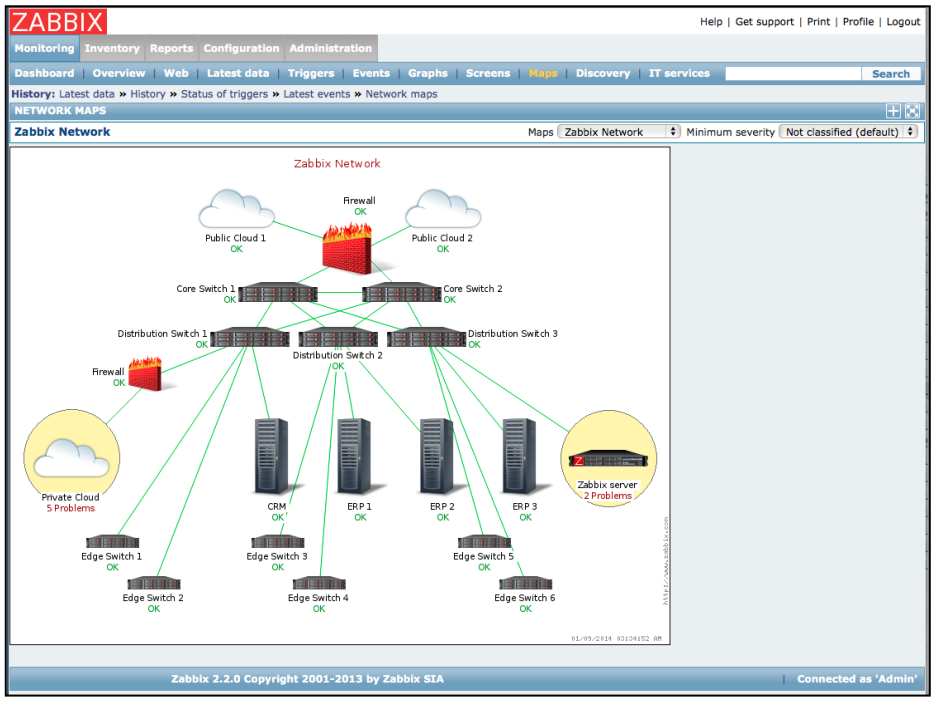
ภาพที่ 2-18 รูปภาพตัวอย่าง The Dude Network Monitoring

Nagios เป็น application ที่ใช้ในการตรวจสอบระบบผ่าน web-application เพื่อใช้การดูทำงานของ Host และ Service ที่เราต้องการ เช่น Disk space, Ram, CPU, Application เมื่อเกิดปัญหาขึ้นจะมีการส่ง alert มายัง administrative เพื่อทำการตรวจสอบ เพื่อใช้ในการบริหารในส่วนของ Fault Management Nagios ได้รับการออกแบบโดย rock solid framework เพื่อใช้ในการ Monitor, scheduling และ alerting ในระบบเครือข่าย และมีความสามารถที่จะเพิ่มศักยภาพในการทำงานอีกได้ตามที่ผู้ใช้ต้องการ ระบบนี้สามารถใช้งานง่าย ผู้ใช้งานไม่จำเป็นที่จะต้องมีความรู้มากมายเพียงแต่จะต้องเข้าใจว่าระบบที่ เราต้องการ Monitor นั้นมีอะไรบ้าง เพื่อที่จะนำข้อมูลเหล่านี้ไปทำการตั้งค่าระบบต่อไป โปรแกรมนี้เหมาะสำหรับ admin ทั่วไปที่ต้องการงานการ Monitoring Network System ในส่วนของ system และ service ต่าง ๆ ที่เราต้องการและที่สำคัญโปรแกรมนี้เป็น free-ware และยังสามารถทำการพัฒนาระบบให้เหมาะสมกับองค์กรได้ ข้อดี คือ ตรวจสอบสถานะ การทำงานของ Server ว่า UP - Down สามารถทำการแจ้งเตือนเมื่อเครื่อง Server down โดย mail หรือ SMS แสดงการให้บริการของ Service เช่น MySQL, HTTP, Application สามารถพัฒนา Plug-in ได้เพื่อให้สอดคล้องกับระบบ สามารถกำหนด Event ได้เพื่อใช้ในการตรวจสอบ สามารถทำการมอนิเตอร์ได้หลาย ๆ เครื่อง เป็นต้น

ภาพที่ 2-19 รูปภาพตัวอย่าง Nagios Network Monitoring

ZABBIX เป็นระบบ Monitoring ที่เป็น Open Source สามารถติดตามการใช้งานของ Server และระบบเครือข่ายผ่านทาง Zabbix Agent ซึ่งรองรับการทำงานบนระบบปฏิบัติการที่

หลากหลาย หรือใช้วิธีตรวจสอบปกติที่ไม่ต้องติดตั้ง Agent ก็ได้เช่นกัน เช่น SNMP เป็นต้น Zabbix ยังรองรับการแจ้งเตือนเมื่อตรวจพบเหตุการณ์ที่สนใจ รวมทั้งสามารถปรับแต่ง Web UI ตามความต้องการได้ นอกจากนี้ Zabbix ยังมีเครื่องมือที่ใช้มอนิเตอร์ Web Application และ Hypervisor ได้ด้วยเช่นกัน อีกจุดเด่นที่สำคัญ คือ Zabbix สามารถแสดงแผนภาพการเชื่อมต่อระหว่างอุปกรณ์ที่สนใจ พร้อมระบุรายละเอียดของอุปกรณ์ดังกล่าวได้ Zabbix รองรับการตรวจสอบและรายงานผลปริมาณการใช้งานของ System Resource ต่าง ๆ ของ Server ทุก OS เช่น CPU, RAM, Disk Space, Traffic รวมไปถึงข้อมูล Inventory Management ของอุปกรณ์ โดยรายงานผลในรูปแบบของกราฟ มีวิธีการตรวจสอบที่ยืดหยุ่นในการตรวจสอบการทำงานของ Server หรืออุปกรณ์เครือข่ายชนิดต่าง ๆ เพื่อให้ทราบถึงสถานะ การทำงานล่าสุด และหากไม่ทำงาน ระบบจะ Alert ไปแจ้งยังผู้ดูแลระบบทันที สามารถตรวจจับความเปลี่ยนแปลงของ File หรือ Configuration เช่น Configure file ของ Server มีการเปลี่ยนแปลง หรือมีการเพิ่มค่าลงไปในไฟล์ ระบบจะทำการบันทึกและกำหนดให้ Alert แจ้งได้ หรือ การนำไปประยุกต์เพื่อตรวจสอบ Mail Server เพื่อตรวจจำนวนเมลที่ตกค้างที่ Queue Server มากจนเกินไป ซึ่งจะส่งผลให้ Mail Server ส่ง email ออกช้าเป็นต้น



ภาพที่ 2-20 รูปภาพตัวอย่าง ZABBIX Network Monitoring