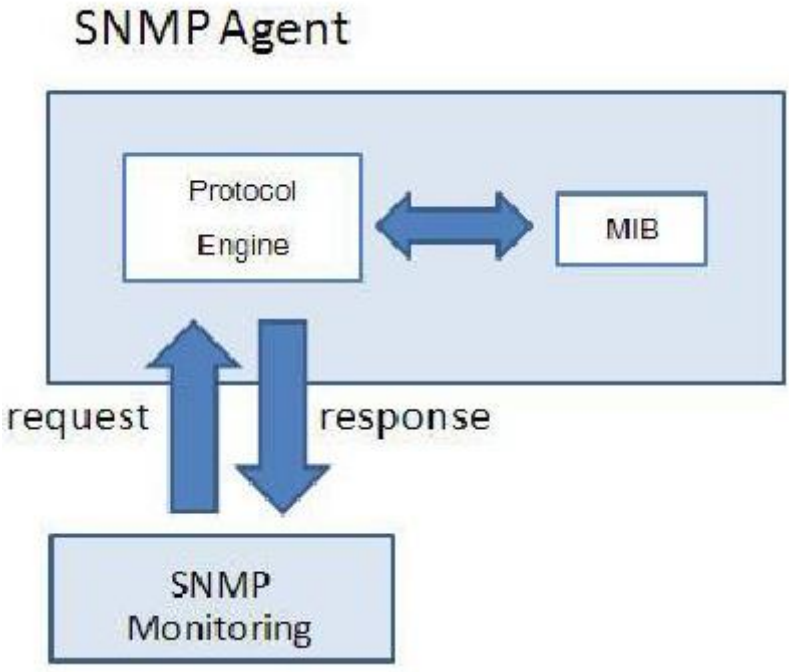
ทำงานของซอฟท์แวร์หรือฮาร์ดแวร์ เมื่อ NMS สั่งงาน โดยมีการแจ้งยืนยันสิทธิในรูปรหัสผ่านว่า NMS มีอำนาจหน้าที่ในการร้องขอและปรับค่า ปัจจุบันโปรโตคอล SNMP ได้รับความนิยมและใช้กันอย่างแพร่หลายในการจัดการอุปกรณ์ ต่าง ๆ เช่น เครื่องแม่ข่าย ไฟร์วอลล์ เราเตอร์ สวิตซ์ ในระบบเครือข่ายโปรโตคอล SNMP ช่วยให้ผู้ดูแลระบบเครือข่ายสามารถรวบรวมข้อมูล เพื่อนำไปวิเคราะห์ค้นหาปัญหาและแก้ไขปัญหาความผิดพลาดของระบบเครือข่ายที่เกิดขึ้นอีกทั้งใช้ในการจัดการประสิทธิภาพและการวางแผนการพัฒนาของระบบเครือข่ายองค์กรในอนาคต

ส่วนประกอบของโปรโตคอล SNMP ประกอบไปด้วย 3 ส่วนหลัก ๆ

2.1.3.1 ส่วนควบคุมการจัดการ (Management Console) หน้าที่รับผิดชอบ คือ ตรวจตราและควบคุมเอเจนต์ โดยตัวควบคุมจะส่งคำสั่งสอบถามหรือ คำสั่งปรับค่าการงานของเอเจนต์ในเครือข่ายหนึ่ง อาจจะมีตัวควบคุมเพียงตัวเดียวหรือหลายเครื่องดูแลจัดการเอเจนต์จำนวนมากได้

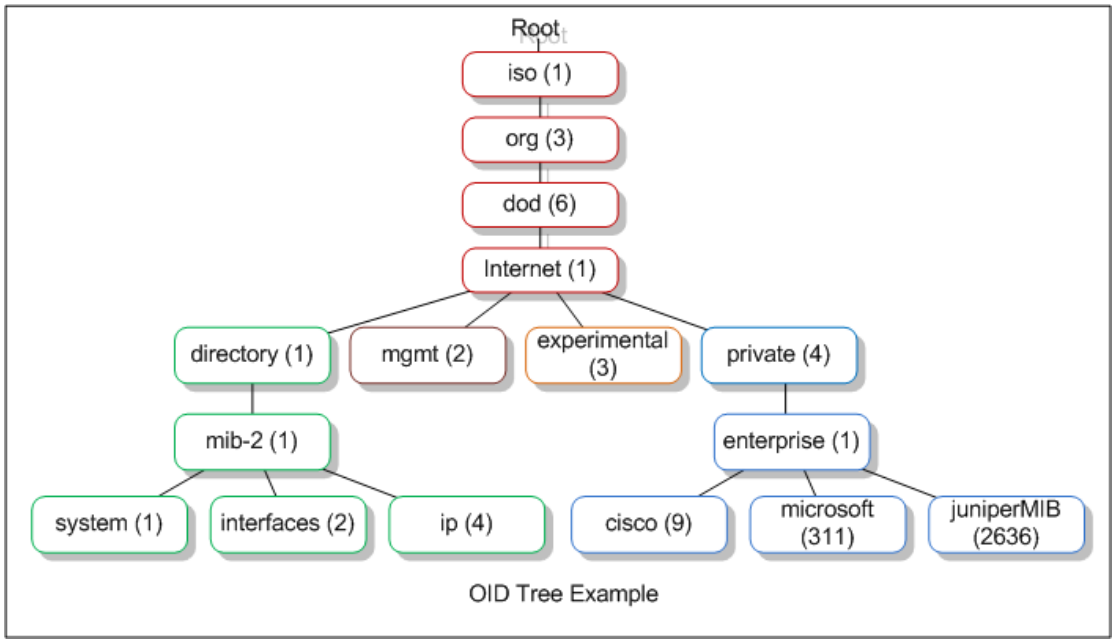
2.1.3.1 ส่วนจัดการเอเจนต์ (Management Agent) อุปกรณ์ที่เป็นเอเจนต์อาจจะเป็น พีซี สวิตซ์ เราเตอร์ และอุปกรณ์ด้านเครือข่าย ในกรณีที่ส่งข้อมูลไปยังระบบได้นั้นที่ตัวอุปกรณ์จำเป็นต้องมีโปรโตคอล SNMP Agent ฝังตัวอยู่ในอุปกรณ์ เมื่อส่วนควบคุมร้องขอข้อมูลข้อมูลก็จะถูกส่งไปยังสถานีจัดการเครือข่าย โดยก่อนจะทำการส่งข้อมูลไปยังสถานีจัดการเครือข่ายได้นั้นโดยส่วนใหญ่จะมีการตรวจสอบสิทธิในรูปแบบของค่าคอมมิวนิตี้ (Community) ว่ามีสิทธิในการร้องขอข้อมูลหรือไม่



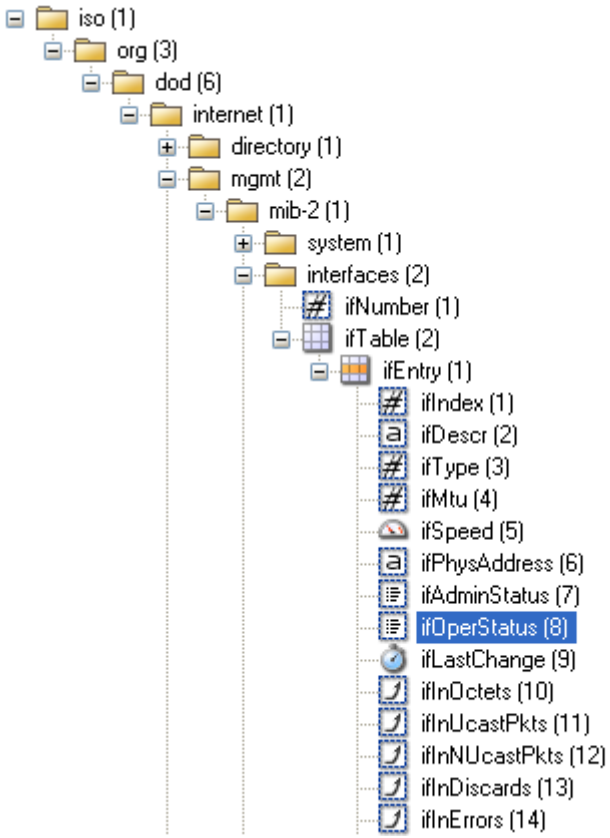
ภาพที่ 2-1 แสดงโครงสร้างของเอเจนต์

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 ของแต่ละอุปกรณ์ผ่านหน้าเว็บได้สะดวกรวดเร็วมากยิ่งขึ้นและได้นำข้อมูลที่ได้ไปวิเคราะห์และปรับปรุงแก้ไขระบบเครือข่ายให้ใช้งานได้มีประสิทธิภาพมากยิ่งขึ้น ในตัวเอเยนต์ค่าพารามิเตอร์จะถูกจัดเรียงตามโครงสร้างต้นไม้ SNMP และจะใช้หมายเลข OID (Object Identifier) เพื่อเจาะจงไปยังพารามิเตอร์ที่ต้องการไม่ว่าจะเพื่อตั้งค่า หรือตรวจสอบข้อมูล ตัวหมายเลข OID จากที่กล่าวมาแล้วก็คือชุดของตัวเลขที่คั่นด้วยเครื่องหมายจุดเพื่อแยกแยะหาตำแหน่ง ในแต่ละตัวเอเยนต์จะมีฐานข้อมูลที่เป็นเสมือนกับสมุดบันทึกตำแหน่งของออบเจ็กต์ทั้งหมดรวมทั้งหมายเลขและชื่ออ้างอิงที่เรียกว่า MIB (Management Information Base) โดยที่ MIB จะจัดเรียงชื่อ, หมายเลข OID, ชนิดข้อมูล, สิทธิการอ่านและเขียนรวมทั้งคำอธิบายสั้น ๆ สำหรับแต่ละออบเจ็กต์ที่อยู่ในตัวเอเยนต์



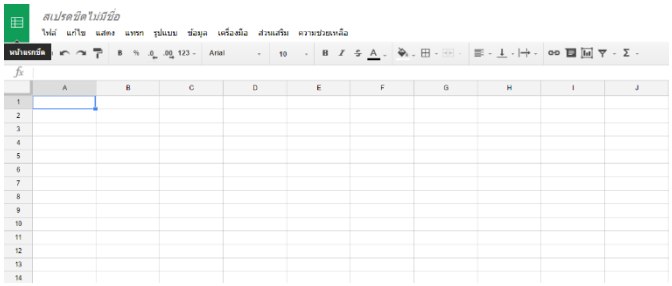
ภาพที่ 2-2 ตัวอย่าง OID Tree

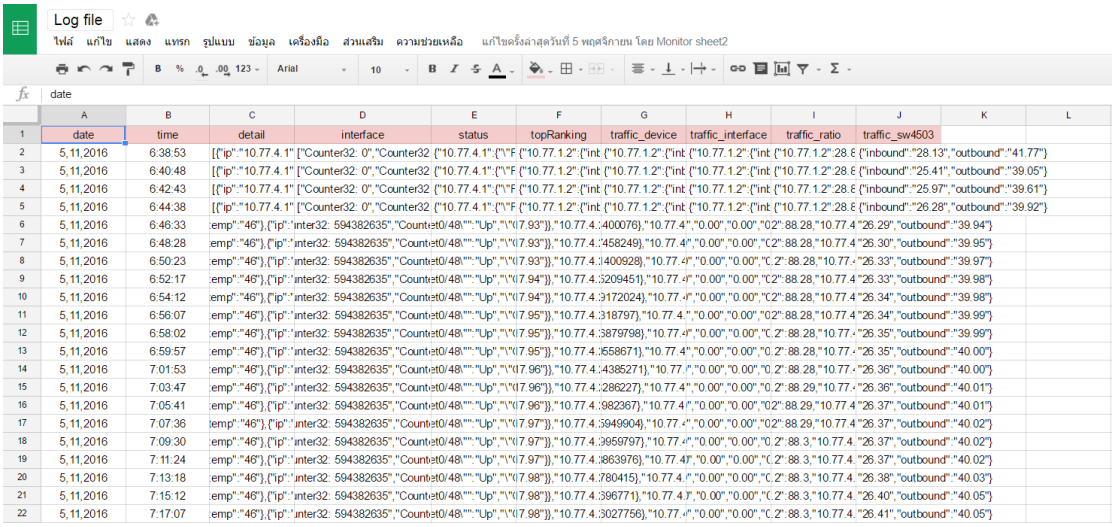


ภาพที่ 2-3 ตัวอย่างข้อมูล OID

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 ผ่านเว็บบราวเซอร์





Log file

ไฟล์ แก้ไข แสดง แทรก รูปแบบ ข้อมูล เครื่องมือ ส่วนเสริม ความช่วยเหลือ แก้ไขครั้งล่าสุดวันที่ 5 พฤศจิกายน โดย Monitor sheet2

Arial 10

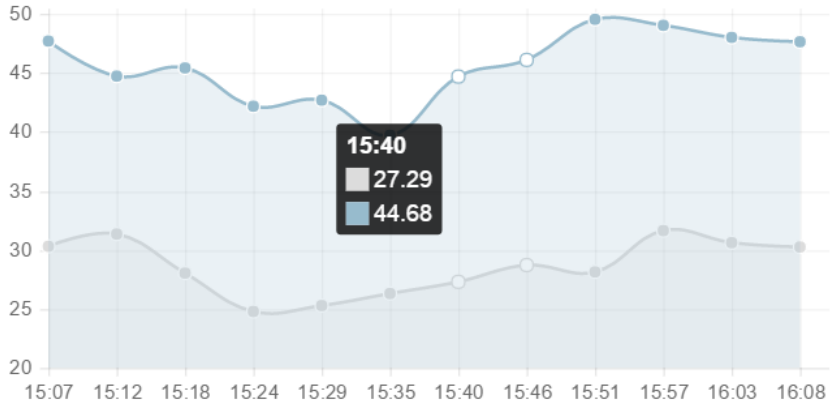
date

	A	B	C	D	E	F	G	H	I	J	K	L
1	date	time	detail	interface	status	topRanking	traffic_device	traffic_interface	traffic_ratio	traffic_sw4503		
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	{"10.77.1.2":{"int	{"10.77.1.2":28.8	{"inbound":"28.13","outbound":"41.77"}		
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	{"10.77.1.2":{"int	{"10.77.1.2":28.8	{"inbound":"25.41","outbound":"39.05"}		
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	{"10.77.1.2":{"int	{"10.77.1.2":28.8	{"inbound":"25.97","outbound":"39.61"}		
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	{"10.77.1.2":{"int	{"10.77.1.2":28.8	{"inbound":"26.28","outbound":"39.92"}		
6	5,11,2016	6:46:33	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.93"}},"10.77.4.:400076},"10.77.4","0.00","0.00","02":88.28,"10.77.4							"26.29","outbound":"39.94"}		
7	5,11,2016	6:48:28	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.93"}},"10.77.4.:458249},"10.77.4","0.00","0.00","02":88.28,"10.77.4							"26.30","outbound":"39.95"}		
8	5,11,2016	6:50:23	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.93"}},"10.77.4.:400928},"10.77.4","0.00","0.00","0.2":88.28,"10.77.4							"26.33","outbound":"39.97"}		
9	5,11,2016	6:52:17	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.94"}},"10.77.4.:3209451},"10.77.4","0.00","0.00","02":88.28,"10.77.4							"26.33","outbound":"39.98"}		
10	5,11,2016	6:54:12	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.94"}},"10.77.4.:3172024},"10.77.4","0.00","0.00","02":88.28,"10.77.4							"26.34","outbound":"39.98"}		
11	5,11,2016	6:56:07	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.95"}},"10.77.4.:318797},"10.77.4.","0.00","0.00","02":88.28,"10.77.4							"26.34","outbound":"39.99"}		
12	5,11,2016	6:58:02	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.95"}},"10.77.4.:3879798},"10.77.4","0.00","0.00","0.2":88.28,"10.77.4							"26.35","outbound":"39.99"}		
13	5,11,2016	6:59:57	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.95"}},"10.77.4.:658671},"10.77.4","0.00","0.00","0.2":88.28,"10.77.4							"26.35","outbound":"40.00"}		
14	5,11,2016	7:01:53	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.96"}},"10.77.4.:4385271},"10.77.4","0.00","0.00","0.2":88.28,"10.77.4							"26.36","outbound":"40.00"}		
15	5,11,2016	7:03:47	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.96"}},"10.77.4.:286227},"10.77.4","0.00","0.00","0.2":88.29,"10.77.4							"26.36","outbound":"40.01"}		
16	5,11,2016	7:05:41	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.96"}},"10.77.4.:982367},"10.77.4","0.00","0.00","02":88.29,"10.77.4							"26.37","outbound":"40.01"}		
17	5,11,2016	7:07:36	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.97"}},"10.77.4.:3949904},"10.77.4","0.00","0.00","02":88.29,"10.77.4							"26.37","outbound":"40.02"}		
18	5,11,2016	7:09:30	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.97"}},"10.77.4.:3959797},"10.77.4","0.00","0.00","0.2":88.3,"10.77.4.							"26.37","outbound":"40.02"}		
19	5,11,2016	7:11:24	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.97"}},"10.77.4.:863976},"10.77.4","0.00","0.00","0.2":88.3,"10.77.4.							"26.37","outbound":"40.02"}		
20	5,11,2016	7:13:18	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.98"}},"10.77.4.:780415},"10.77.4.","0.00","0.00","0.2":88.3,"10.77.4.							"26.38","outbound":"40.03"}		
21	5,11,2016	7:15:12	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.98"}},"10.77.4.:396771},"10.77.4.","0.00","0.00","0.2":88.3,"10.77.4.							"26.40","outbound":"40.05"}		
22	5,11,2016	7:17:07	emp":"46"},{"ip":"inter32: 594382635","Counter0/48\"":"Up","\"(7.98"}},"10.77.4.:3027756},"10.77.4","0.00","0.00","0.2":88.3,"10.77.4.							"26.41","outbound":"40.05"}		

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 เพื่อจะได้จัดการส่งต่อไปให้ ในขณะเดียวกัน ก็จะเป็นที่เก็บข้อมูลและโปรแกรมที่คอมพิวเตอร์ในเครือข่ายจะมาเรียกไปใช้ได้

2.1.8 API คืออะไร

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

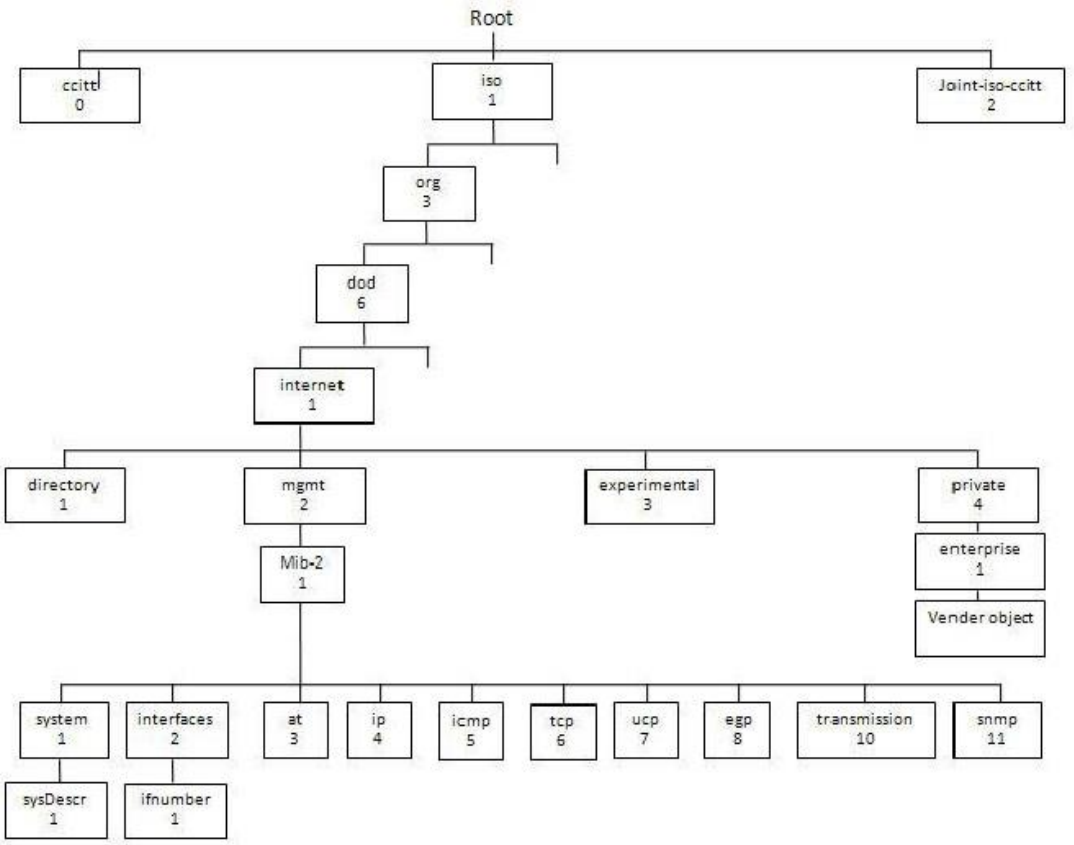
1. ช่วยในการพัฒนาเว็บไซต์หรือ Application ได้ง่ายและรวดเร็วซึ่ง API จะเป็นตัวช่วยที่นักพัฒนาไม่ต้องเข้าไปแก้ไข Code คำสั่งเลยทำให้สะดวกสบายในการใช้งาน
2. ช่วยให้นักพัฒนาเว็บไซต์หรือเจ้าของเว็บไซต์สามารถฐานผู้ชมเว็บไซต์ให้มากขึ้น
3. ทำให้ผู้ใช้งานเว็บไซต์ต่าง ๆ ที่มีการติดตั้ง API ของอีกเว็บไซต์หนึ่งไม่ต้องเข้าหน้าเว็บไซต์ที่เป็นเจ้าของAPIเพียงแต่เข้ามายังเว็บไซต์ที่มีการติดตั้งAPIเท่านั้นทำให้การรับรู้ข่าวสารต่าง ๆ ทั่วถึงกัน
4. API สามารถรับส่งข้อมูลข้าม Server ได้

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

ภาพที่ 2-6 รูปภาพตัวอย่าง Graph Traffic

2.1.9 ฐานข้อมูล (Message Intotmation Base-MIB)

เป็นส่วนที่เก็บตัวแปรและค่ากำหนดการทำงานประจำอุปกรณ์ ข้อมูลประจำอุปกรณ์เครือข่ายชิ้นหนึ่งอาจจะมีได้หลากหลายอีกทั้งอุปกรณ์ต่าง ๆ ประเภทกันย่อมมีข้อมูลประจำอุปกรณ์ที่แตกต่างกัน ดังนั้นการสอถามค่าหรือเปลี่ยนแปลงค่าในฐานข้อมูล จำเป้นจะต้องมีรูปแบบมาตรฐานให้กับอุปกรณ์ทุกประเภท โดยโครงสร้างแบบลำดับชั้น (Tree) ได้ถูกเลือกสำหรับใช้เป็นฐานข้อมูลเพื่อจัดเก็บตัวแปรเหล่านี้ แต่ละโหลดซึ่งแทนอ็อบเจ็กหนึ่ง 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) เพื่อกำหนดกลุ่มการจัดการเครือข่ายอินเตอร์เน็ต เมื่อต้องการอ้างอิงถึงโหนดใดในโครงสร้างให้เขียนหมายเลขจากรากไปตามเส้นทางถึงโหนดนั้นและคั่นด้วยจุด ลำดับตัวเลขนี้เรียกว่า Object identifier หรือ OID อ็อบเจ็กทุกตัวมีนิยามกำหนด ชื่อ แบบข้อมูล สิทธิการเข้าถึง คำอธิบายลักษณะและค่าข้อมูล การนิยาม อ็อบเจ็กมีกฎเกณฑ์ตามข้อกำหนดโครงสร้างฐานข้อมูลสารสนเทศการจัดการ



ภาพที่ 2-7 Object identifier ในโครงสร้างฐานข้อมูลสารสนเทศ

ซึ่งส่วนประกอบทั้งหมดจะทำงานร่วมกันเพื่อให้ผู้ดูแลระบบเครือข่ายสามารถตรวจสอบและควบคุมส่วนประกอบต่าง ๆ ของเครือข่าย

โปรโตคอล SNMP มี 3 เวอร์ชั่น

- **SNMP V1** ได้รับการพัฒนาและอนุมัติว่ามันเป็นโปรโตคอลที่จำเป็นสำหรับการใช้งานขนาดใหญ่บนอินเตอร์เน็ต และการค้า ในช่วงเวลานั้นการตรวจสอบมาตรฐานอินเตอร์เน็ตและความปลอดภัยมุ่งเน้นไปที่โปรโตคอลนี้ ในเวอร์ชั่น 1 ยังมีระบบความปลอดภัยที่ต่ำ การยืนยันตัวตนของ clients ถูกออกแบบให้ใช้เพียง community string เท่านั้น ซึ่งมีผลเหมือนกับรหัสผ่านในการส่งผ่านข้อมูล การออกแบบ SNMPv1 สำเร็จโดยกลุ่มองค์กรที่สนับสนุนโดยOSI/IETF/NSF (National Science Foundation)

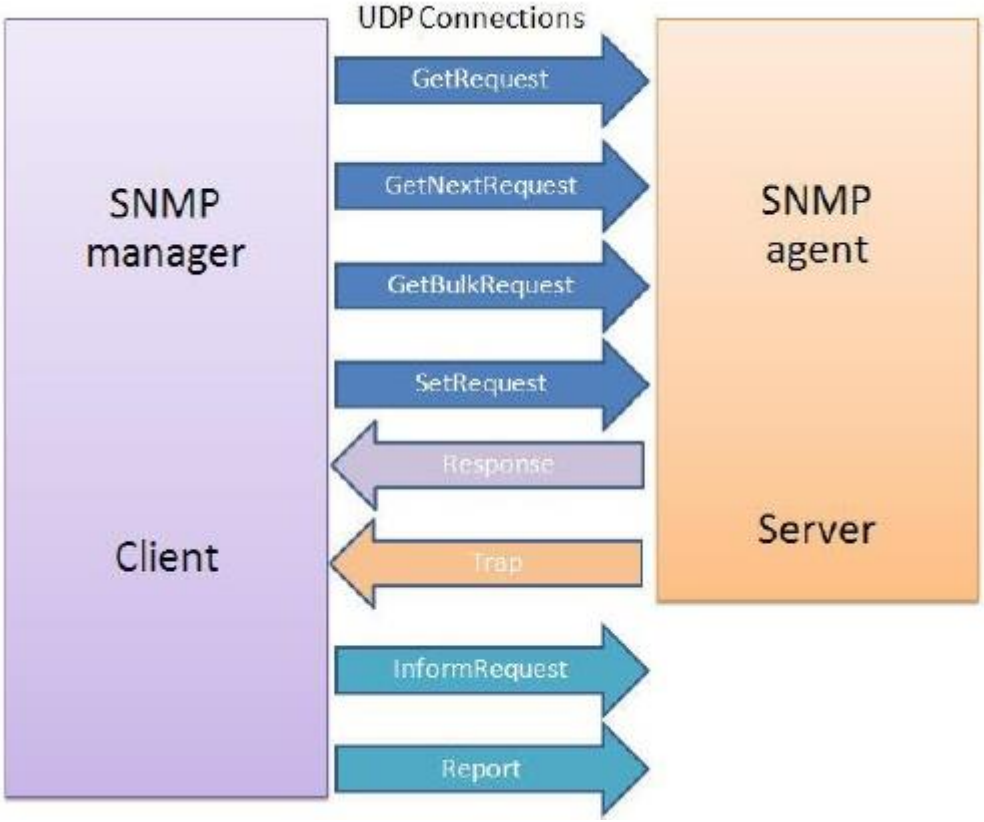
- **SNMP V2** เป็นการพัฒนามาจากเวอร์ชั่นที่ 1 มีการปรับปรุงประสิทธิภาพ ความปลอดภัย และการสื่อสารระหว่าง manager โครงสร้างของ MIB ยังคงยึด SNMPv1 ในการใช้งาน และถูกกำหนดไว้ใน RFC 1901, RFC 1905, RFC 1906, RFC 2578

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 เช่นเดียวกับในเวอร์ชั่น 1 แต่อย่างไรก็ตามเวอร์ชั่นที่สองได้เพิ่มฟังก์ชั่นบางอย่างเพิ่มเติม อย่างคำสั่ง TRAP ที่ถึงแม้จะมีเหมือนเวอร์ชั่น 1 แต่แตกต่างกันในรูปแบบของข้อความที่ใช้และการออกแบบเพื่อแทนที่คำสั่ง TRAP ของเวอร์ชั่น 1 SNMPv2 ได้ระบุสองคำสั่งใหม่คือ GET BULK และ INFORM

- **SNMPv3** ถูกออกแบบให้สามารถป้องกันการบุกรุกจากช่องทางการสื่อสารของการจัดการเครือข่ายจากผู้ที่ไม่มีอำนาจหน้าที่หรือสิทธิ (Unauthorized) และให้จดจำไว้ว่าการรักษาความปลอดภัยของ SNMPv3 จะปกป้องเฉพาะส่วนระบบจัดการเครือข่ายเท่านั้น ดังนั้นในระบบเครือข่ายจริง ๆ ยังต้องการระบบการรักษาความปลอดภัยอื่น ๆ ที่ปกป้องเครือข่ายทั้งระบบ การบุกรุกคุกคามจากช่องทางสื่อสารกับเอเจนต์โดยทั่วไปสามารถแบ่งการบุกรุกทางเทคนิคได้ดังต่อไปนี้



ภาพที่ 2-8 แสดงประเภทคำสั่งของ SNMP v3

แบ่งการบุกรุกทางเทคนิคได้ดังต่อไปนี้

- Modification of Information คือการที่เมสเสจ SNMP ถูกแก้ไขอย่างไม่พึงประสงค์โดยผู้ไม่หวังดีระหว่างการทำ transactionทำให้เมสเซจนั้นเสียหาย

- Masquerade คือการบุกรุกแบบการปลอมแปลงตัวจากการเป็นผู้ที่ไม่มีสิทธิให้สามารถทำการจัดการระบบเครือข่ายได้ ซึ่งเป็นการบุกรุกที่ร้ายแรง เพราะสามารถทำอะไรก็ได้เหมือนผู้ดูแลระบบ

- Disclosure คือการบุกรุกจากผู้ที่ไม่มีสิทธิ์โดยการทำการดักฟังหรือดักจับเพื่อเอาข้อมูลระบบระหว่างการทำ transaction

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

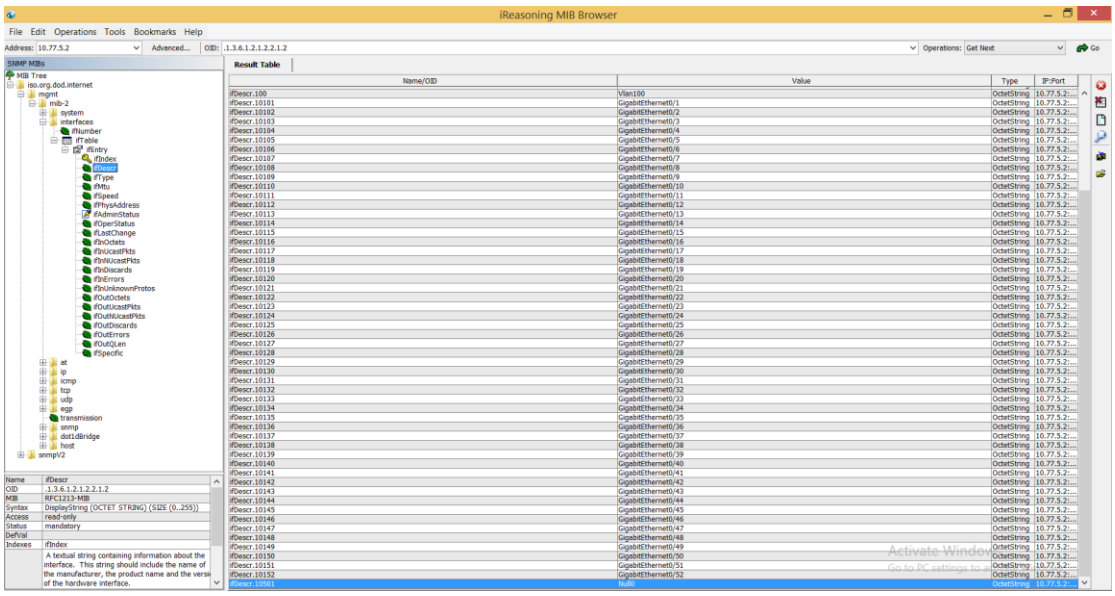
- Unauthorized Access คือการบุกรุกโดยผู้ไม่มีสิทธิโดยการผิดพลาดในการจัดการระบบ

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 หรือส่งใหม่ โดยใช้หน้าต่างเวลา (Window) เป็นเครื่องมือตรวจสอบ
- Authentication ให้การรับรองในการตรวจสอบเอนทิตี้ที่ทำการสื่อสารแบบระหว่างกัน เช่น ระหว่าง NMS และเอเยนต์ ว่ามีตัวตนและสิทธิ์จริง
- Privacy (Confidentiality) ให้ความไว้วางใจว่าข้อมูลจะไม่ถูกเปิดเผยไปยังผู้ไม่สิทธิ์
- Access Control ให้ความมั่นใจว่าแหล่งข้อมูลไม่ถูกใช้โดยผู้ไม่มีสิทธิ์ รวมทั้งการกระทำที่ไม่สิทธิ์ ถึงแม้จะเข้าไปในระบบได้แล้วก็ตาม Access Control นั้นจะทำงานร่วมกับ Authentication เพื่อช่วยพิสูจน์ว่าเอนทิตี้ใดมีสิทธิเข้าถึงแหล่งข้อมูลเฉพาะหรือกลุ่มข้อมูลที่มีจุดประสงค์พิเศษ

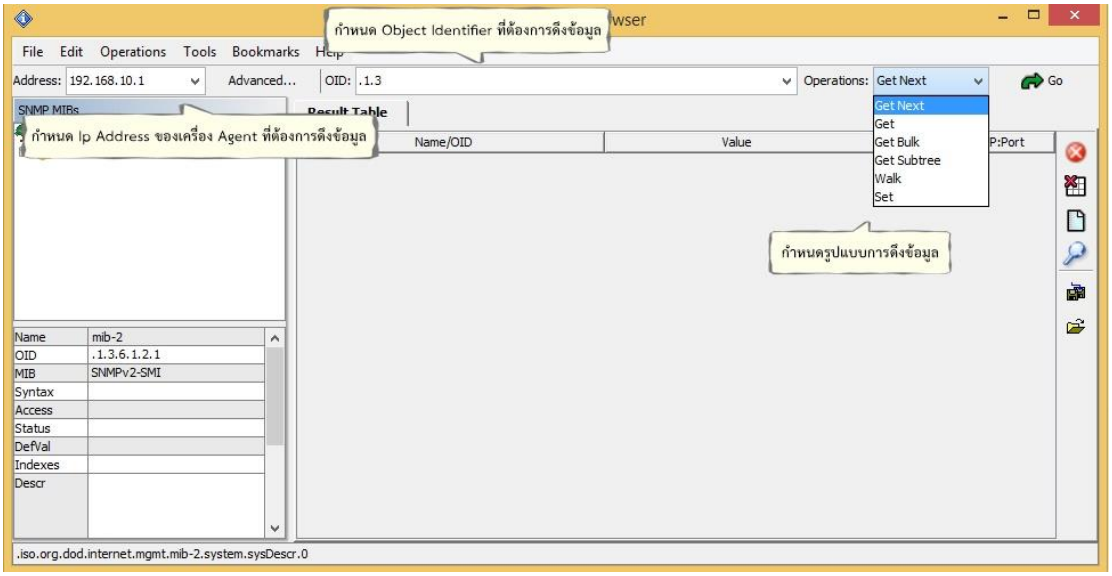
2.1.9 Mib Browser

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 อัลกอริทึมที่มีประสิทธิภาพและมีประสิทธิภาพ SMIv1/SMIv2 MIB IPv6 parser รับการสนับสนุนผู้ส่งเข้าสู่ระบบหน้าต่างที่จะแสดงบันทึกของโปรแกรมประยุกต์และแพ็กเก็ต SNMP แลกเปลี่ยนระหว่าง Browser และมุมมองของพอร์ต (การใช้แบนด์วิธเปอร์เซ็นต์ข้อผิดพลาด) 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: ทำหน้าที่กำหนดการกระทำของของโปรแกรม ในการติดต่อกับ 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

2.1.10 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 ที่กำลังรันอยู่ 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

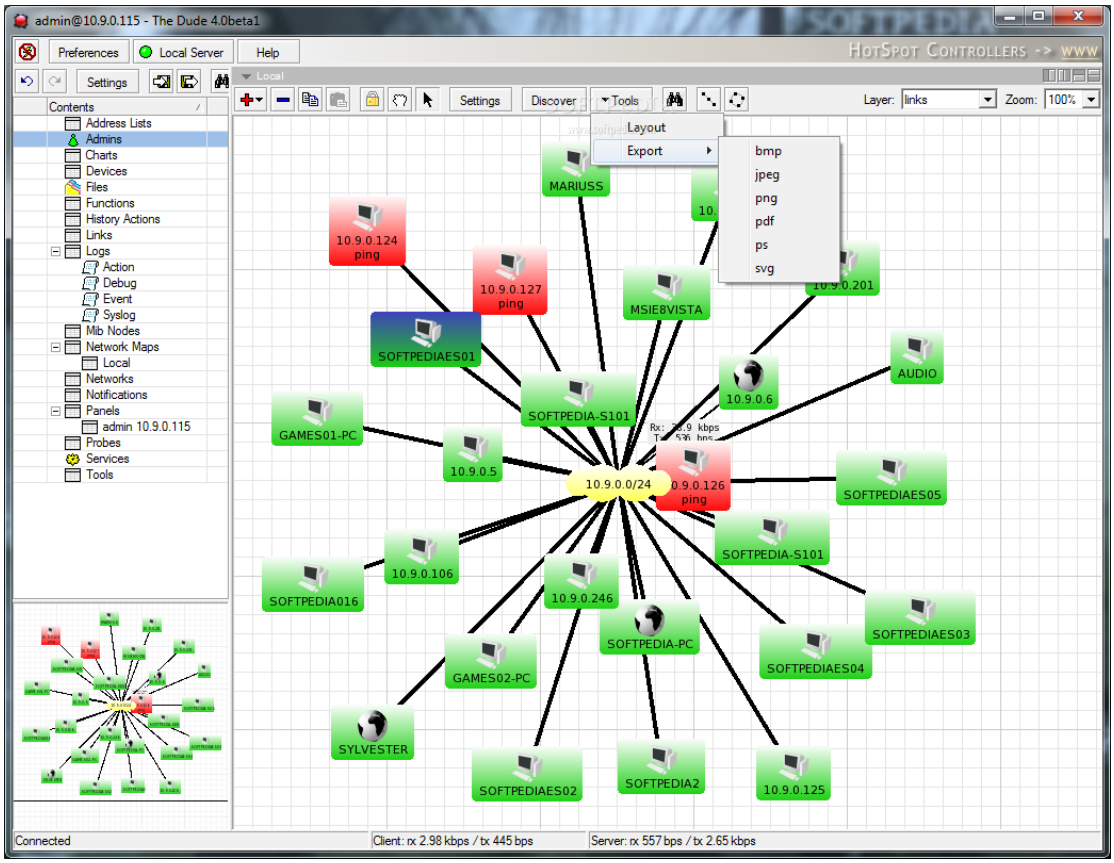
```
<div id="text"></div>
<div id="get_text"></div>
<script>
$(document).ready(function(){
var str = $("#text").text();     // สั่งให้ ตัวแปร "str" เก็บค่า text จาก id="text" เข้ามาเก็บไว้
$("#get_text").text(str);       // ใส่ตัวแปร "str" เข้าไปใน id="get_text" ด้วยคำสั่ง .text();
});
</script>
```

ภาพที่ 2-11 ตัวอย่างการใช้งาน jquery

2.1.11 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 ความสามรถในการค้นหายี่ห้ออุปกรณ์ได้ สามารถตรวจสอบได้ทั้งอุปกรณ์ว่ายังทำงานอยู่หรือไม่พร้อมแจ้งเตือน สามารถวาดผังของเครือข่ายเน็ตเวิร์กเองได้ สามารถ Import และ Export ค่าที่ Setting เอาไว้เพื่อ Backup/Restore ได้มี Report รวมให้อุปกรณ์แต่ละตัวด้วยเพื่อสรุปค่าความเสถียรเป็นรายงานตรวจสอบ Service บน อุปกรณ์ก็ได้ เช่น HTTP ,SMTP ,SNMP วาดผังเองก็ได้ รองรับ SNMP v1 และ SNMP v2 สามารถรองรับระบบ Syslog สำหรับอุปกรณ์ Network เป็นต้น The Dude สามารถ Monitor อุปกรณ์พร้อม ๆ กันได้หลายเครื่อง ยกตัวอย่างอุปกรณ์เช่น AD Server, Print Server , Router ,Firewall, Wireless (ตามจุด), File Server เป็นต้น

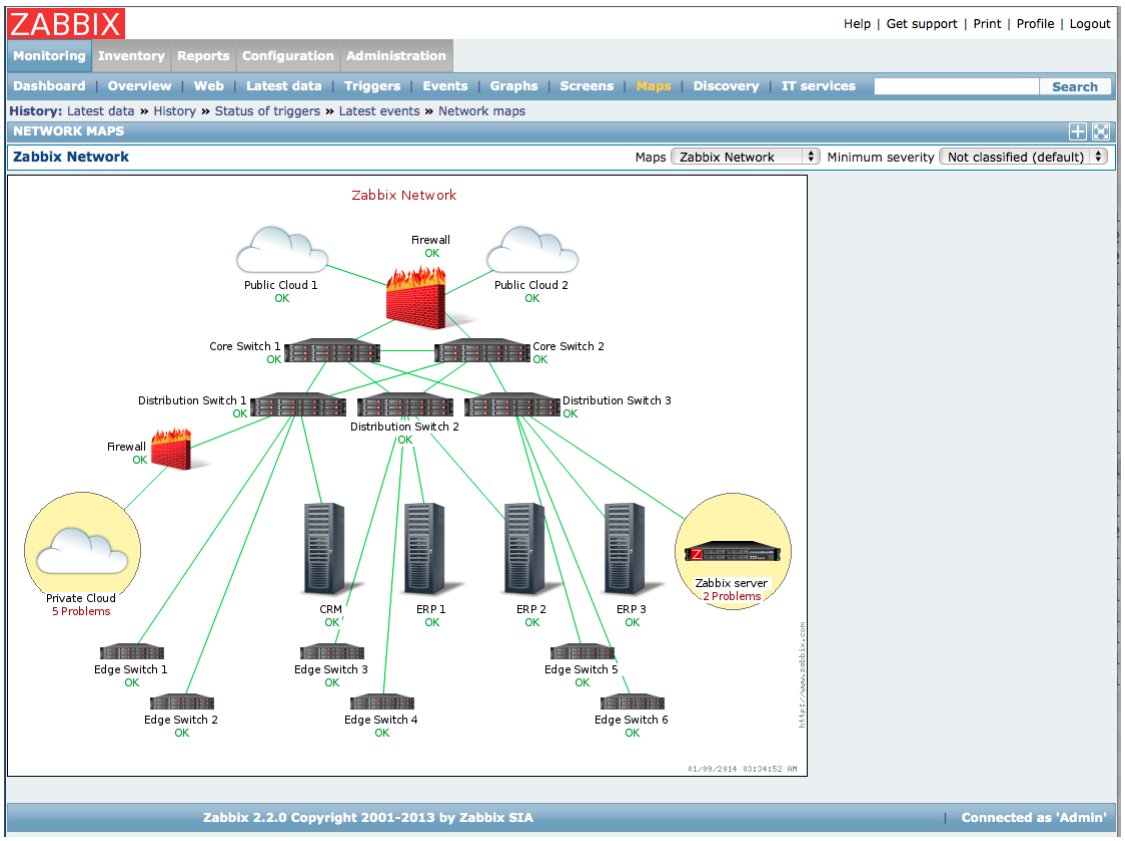


ภาพที่ 2-12 รูปภาพตัวอย่าง The Dude Network Monitoring

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 สามารถทำการแจ้งเตือนเมื่อ Server down โดย mail หรือ SMS แสดงการให้บริการของ Service เช่น , MySQL, HTTP, Application สามารถพัฒนา Plug-in ได้เพื่อให้สอดคล้องกับระบบ สามารถกำหนด Eventได้เพื่อใช้ในการตรวจสอบ สามารถทำการมอนิเตอร์ได้หลาย ๆ เครื่อง เป็นต้น

ภาพที่ 2-13 รูปภาพตัวอย่าง Nagios Network Monitoring

ZABBIX เป็นระบบ Monitoring ที่เป็น Open Source สามารถติดตามการใช้งานของเซิฟเวอร์และระบบเครือข่ายผ่านทาง Zabbix Agent ซึ่งรองรับการทำงานบนระบบปฏิบัติการที่หลากหลาย 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 เพื่อตรวจจำนวนเมล์ที่ตกค้างที่ Queue Server มากจนเกินไป ซึ่งจะส่งผลให้ Mail Server ส่งเมล์ออกช้าเป็นต้น



ภาพที่ 2-14 รูปภาพตัวอย่าง ZABBIX Network Monitoring