

# การเปรียบเทียบซอฟต์แวร์โอเพนซอร์ซ สำหรับการบริหารจัดการเครือข่าย

กุลชาติ มีทรัพย์หลาก ชาวีร์ อิศริยภัทร์ กุลวดี ศรีพานิชกุลชัย  
โครงการระบบบริหารจัดการเครือข่ายอัจฉริยะ (NT5001)  
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ  
กันยายน 2551

## บทคัดย่อ

ในการบริหารจัดการเครือข่ายคอมพิวเตอร์มีความจำเป็นอย่างสูงที่จะต้องมีระบบหรือซอฟต์แวร์สำหรับช่วยในการดูแลเครือข่าย เนื่องจากความต้องการใช้งานอินเทอร์เน็ตสูงขึ้นและการเชื่อมต่อระหว่างอุปกรณ์มีจำนวนมากขึ้นตามเทคโนโลยีที่พัฒนาอย่างรวดเร็ว การดูแลเครือข่ายจำเป็นต้องใช้บุคลากรที่มีความรู้ความเชี่ยวชาญในระดับหนึ่งพร้อมกับซอฟต์แวร์ที่ใช้สำหรับดูแลระบบอย่างมีประสิทธิภาพ โดยซอฟต์แวร์ที่มีคุณลักษณะเหมาะสมกับงานดูแลเครือข่ายนอกควรมีคุณภาพเป็นที่ยอมรับกันโดยทั่วไปและใช้งานได้ง่าย ดังนั้นรายงานฉบับนี้จึงนำการวิเคราะห์ซอฟต์แวร์เพื่อที่เหมาะสมกับการดูแลเครือข่ายพร้อมทั้งเสนอแนะวิธีการปรับปรุงเพื่อให้เป็นแนวทางในการพัฒนาระบบบริหารจัดการเครือข่ายต่อไป

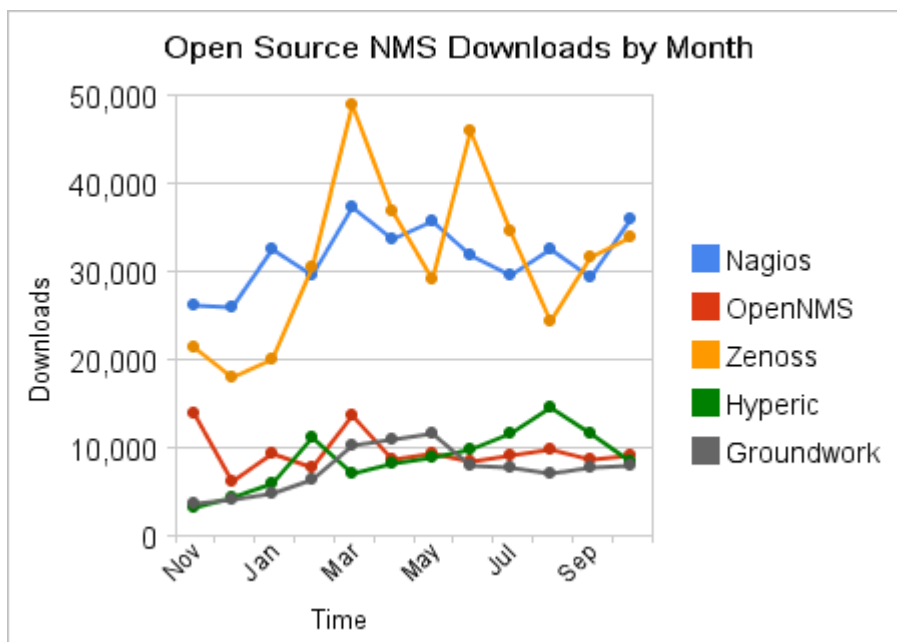
## บทนำ

เนื่องด้วยปัจจุบันความต้องการใช้งานอินเทอร์เน็ตสูงขึ้นและการเชื่อมต่อระหว่างอุปกรณ์มีจำนวนมากขึ้นตามเทคโนโลยีที่พัฒนาอย่างรวดเร็ว การดูแลเครือข่ายจำเป็นต้องใช้บุคลากรที่มีความรู้ความเชี่ยวชาญในระดับหนึ่งพร้อมกับซอฟต์แวร์ที่ใช้สำหรับช่วยดูแลระบบอย่างมีประสิทธิภาพ ดังนั้นการเปรียบเทียบซอฟต์แวร์บริหารจัดการเครือข่ายจะเป็นประโยชน์อย่างสูงสำหรับการใช้งานในองค์กร โดยเป้าหมายของการวิจัยโครงการดูแลเครือข่ายอัจฉริยะอย่างหนึ่งคือความสามารถของคุณลักษณะที่ดีของแต่ละซอฟต์แวร์มาพัฒนาต่อยอดให้เป็นระบบที่เหมาะสมกับองค์กร แต่เนื่องจากซอฟต์แวร์การค้ามีราคาสูงมาก ทำให้ผู้ใช้จำนวนมากหันมาสนใจซอฟต์แวร์โอเพนซอร์ซ ซึ่งมี Community ของตนเองในการพัฒนาอย่างต่อเนื่องและมีคุณภาพที่เป็นที่ยอมรับทั่วไป ดังนั้นทีมงานวิจัยจึงเห็นความสำคัญของการวิเคราะห์ซอฟต์แวร์โอเพนซอร์ซที่เกี่ยวข้อง เสนอแนะวิธีการปรับปรุงเพื่อให้เป็นแนวทางในการพัฒนาระบบบริหารจัดการเครือข่ายต่อไป

จากการเปรียบเทียบจำนวนการดาวน์โหลดซอฟต์แวร์โอเพนซอร์ซจาก *Sourceforge* (<http://www.sourceforge.net>) ในระหว่างเดือนพฤศจิกายน 2549 ถึงเดือนตุลาคม 2550 [1] จะเห็นได้ว่าสามอันดับแรกที่มีการดาวน์โหลดสูงสุด คือซอฟต์แวร์ชื่อว่า **Nagios** [2], **Zenoss** [3], และ **OpenNMS** [4] ดังแสดงในรูปที่ 1 ซึ่งเป็นการเปรียบเทียบจำนวนครั้งที่ดาวน์โหลดของซอฟต์แวร์ต่างๆ ดังนั้นในรายงานนี้ทีมวิจัยได้เลือกซอฟต์แวร์ Nagios Zenoss OpenNMS และซอฟต์แวร์ที่น่าสนใจอีกตัวคือ **Cacti** [5] สำหรับในการเปรียบเทียบ โดยในเบื้องต้นได้พิจารณาองค์ประกอบต่างๆที่จำเป็นดังต่อไปนี้

1. การแสดงผลการตรวจสอบสถานะภาพต่างๆของเครือข่าย
2. การค้นหาอุปกรณ์ในเครือข่าย
3. การปรับแต่งระบบ(Configuration) และการใช้ Plug-in หรือการใช้ External scripts
4. การรายงานผล การแสดงกราฟ และแผนผังการเชื่อมต่อ

ส่วนเรื่องอื่นๆ เช่น ความยากง่ายในการใช้ อาจแทรกอยู่ในหัวข้อเหล่านี้ แต่อาจแตกต่างกันไปตามความเห็นและทักษะของแต่ละบุคคล



รูป 1. เปรียบเทียบจำนวนซอฟต์แวร์ที่ดาวน์โหลด [1]

ก่อนจะทำการเปรียบเทียบนั้น ควรพิจารณาข้อมูลพื้นฐานดังนี้ ซอฟต์แวร์ส่วนใหญ่ที่ใช้ในการเปรียบเทียบนี้เป็นซอฟต์แวร์ที่ใช้งานและทดสอบโดยใช้ข้อมูลจากระบบจริงในเครือข่ายที่ใช้ในการทดสอบ เครื่อง server ที่ใช้ติดตั้งกับระบบปฏิบัติการแบบ Linux Fedora Core 7 หรือ 8 ซอฟต์แวร์ส่วนใหญ่ต้องมีการติดตั้ง package นอกเหนือจากที่มีอยู่แล้วดังนี้

### Package พื้นฐานในการติดตั้ง

1. **Nagios** (Version 3.0): ในการติดตั้งทั่วไปไม่จำเป็นต้องมีการติดตั้ง package เพิ่มเติม นอกจากที่เป็น optional เช่น net-snmp ที่จะใช้สำหรับการตรวจสอบที่ใช้ snmp
2. **Zenoss** (Version 2.2): net-snmp, mysql-server, mysql-devel, gmp, python-devel
3. **OpenNMS** (Version 1.3.8): net-snmp, postgresql, Java (>1.4.2) Tomcat (Java servlet engine), rrdtool, curl
4. **Cacti** (Version 0.8.7b): net-snmp, mysql-sever, mysql-devel, openssl-devel, php, php-mysql, php-pdo, php-snmp, rrdtool

หมายเหตุ: ผู้อ่านควรศึกษารายละเอียดการติดตั้งจาก website ของซอฟต์แวร์ในรายการอ้างอิง เนื่องจากเนื้อหาอยู่นอกขอบเขตของรายงานฉบับนี้ นอกจากนี้ความยากง่ายในการติดตั้งโปรแกรมที่เป็นสิ่งที่เปรียบเทียบกันได้โดยยาก เนื่องจากความยากง่ายนี้ขึ้นอยู่กับทักษะของแต่ละบุคคล

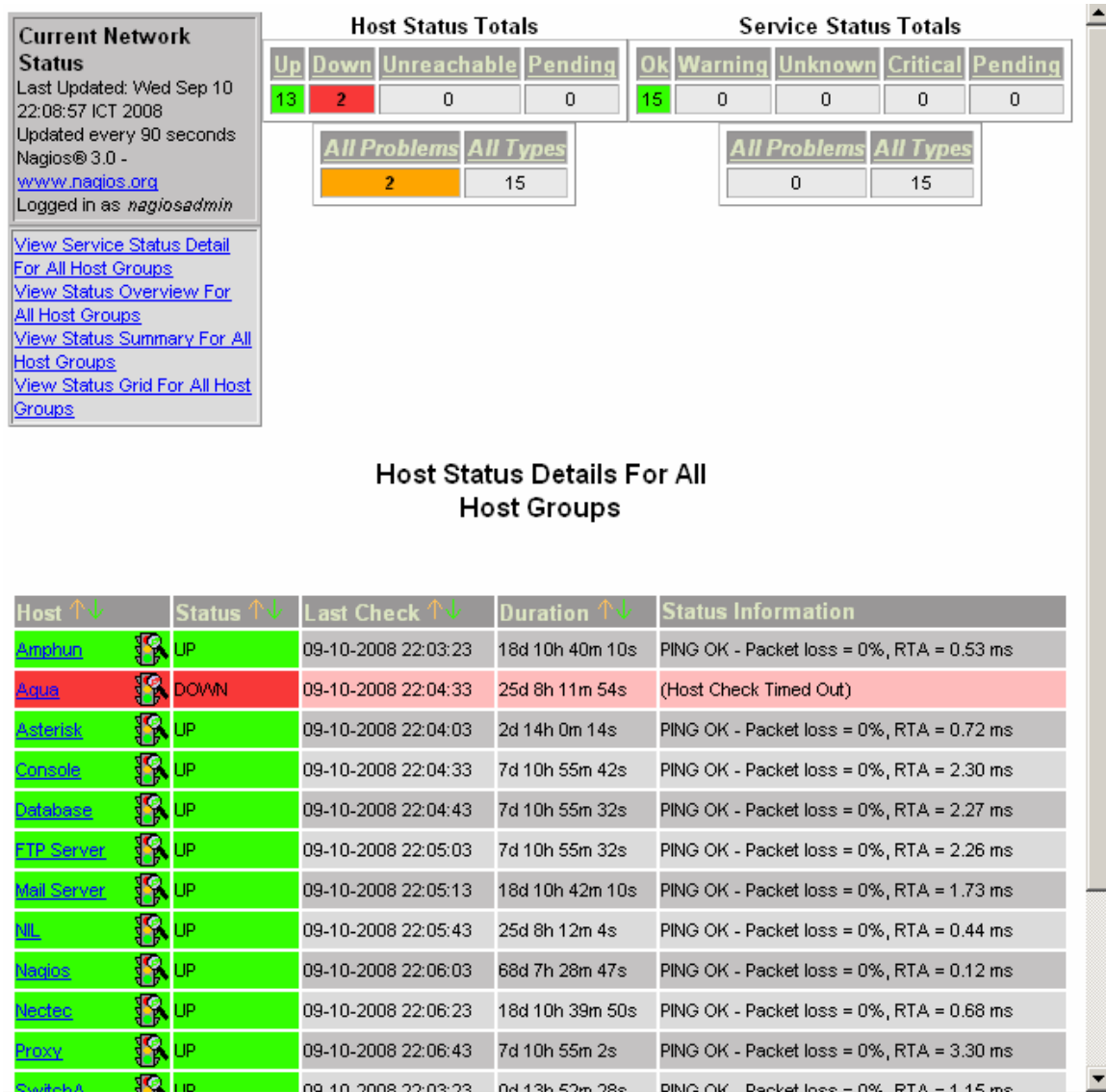
### 1. การแสดงผลการตรวจสอบสถานะภาพต่างๆของเครือข่าย

การตรวจสอบสถานะภาพเครือข่าย (monitoring) โดยรวมจะต้องมีการแสดงผลของสถานะของสิ่งที่ต้องการตรวจสอบ ซึ่งอาจจะเป็น network device เช่น router หรือ switch หรือบาง interface ที่

สำคัญของอุปกรณ์เหล่านี้ นอกจากนี้ยังเป็นการตรวจสอบสถานะภาพของ host เช่น web/mail/database/ftp servers หรือจะเป็นการ monitor service ที่runอยู่บนเครื่องต่างๆ โดยการแสดงสถานะจะบ่งบอกว่าสิ่งนั้นๆยังมีทำงานอยู่เป็นปกติหรือไม่ เช่น Up/Down แต่ถ้ามีเหตุการณ์ที่ไม่ปกติจะมีการแสดงถึงดีกรีของความผิดปกติ เช่น Warning หรือ Critical เป็นต้น พร้อมทั้งรายละเอียดของความผิดปกติตามที่ระบบตรวจเจอ นอกจากนี้องค์ประกอบที่สำคัญอีกส่วนหนึ่งคือการแจ้งเตือน (alerting) หรือระบบที่คอยส่ง notification ไปยังผู้ที่ดูแลอุปกรณ์หรือ service นั้นๆ ในที่นี้จะขอก้าวถึงการตรวจวัดสถานะภาพเครือข่ายของ Nagios ก่อน ซึ่งมี features พื้นฐานของการดูแลระบบ

## Nagios

Nagios เป็น tool ที่มี features ของการ monitoring และการ alerting ซึ่งสามารถตรวจสอบสถานะภาพทั้ง host และ service ดังแสดงในรูปที่ 2 และ 3



รูป 2. Nagios: Host monitoring

### Alert Summary Report

Last Updated: Wed Sep 10 22:14:47 ICT 2008  
Nagios® 3.0 - [www.nagios.org](http://www.nagios.org)  
Logged in as *nagiosadmin*

### Most Recent Alerts

09-03-2008 22:14:47 to 09-10-2008 22:14:47

Duration: 7d 0h 0m 0s

### Report Options Summary:

**Alert Types:** *Host & Service Alerts*

**State Types:** *Soft & Hard States*

**Host States:** *Up, Down, Unreachable*

**Service States:** *Ok, Warning, Unknown, Critical*

[Generate New Report](#)

Displaying most recent 25 of 127 total matching alerts

Time	Alert Type	Host	Service	State	State Type	Information
09-10-2008 08:24:39	Service Alert	<a href="#">Nagios</a>	<a href="#">Current Load</a>	OK	SOFT	OK - load average: 4.52, 2.81, 1.14
09-10-2008 08:23:39	Service Alert	<a href="#">Nagios</a>	<a href="#">Current Load</a>	WARNING	SOFT	WARNING - load average: 6.50, 2.66, 0.98
09-10-2008 08:22:39	Service Alert	<a href="#">Nagios</a>	<a href="#">Current Load</a>	WARNING	SOFT	WARNING - load average: 5.47, 1.47, 0.51
09-10-2008 08:16:29	Host Alert	<a href="#">SwitchA</a>	N/A	UP	SOFT	PING OK - Packet loss = 0%, RTA = 1.34 ms
09-10-2008 08:16:19	Service Alert	<a href="#">Web Server</a>	<a href="#">PING</a>	OK	SOFT	PING OK - Packet loss = 0%, RTA = 8.51 ms
09-10-2008 08:15:19	Service Alert	<a href="#">Web Server</a>	<a href="#">PING</a>	CRITICAL	SOFT	CRITICAL - Network Unreachable (10.10.10.13)
09-10-2008 08:15:19	Host Alert	<a href="#">SwitchA</a>	N/A	DOWN	SOFT	CRITICAL - Network Unreachable (203.185.129.141)
09-09-2008 16:11:26	Host Alert	<a href="#">Web Server</a>	N/A	UNREACHABLE	SOFT	CRITICAL - Network Unreachable (10.10.10.13)
09-09-2008 16:11:16	Host Alert	<a href="#">Asterisk</a>	N/A	UNREACHABLE	HARD	CRITICAL - Network Unreachable (10.10.10.10)

รูป 3. Nagios: Alert Summary

จะเห็นได้ว่าในการแสดง status เป็นการแสดงข้อมูลประมวลผลแบบง่ายๆ ทำให้รู้ว่าสิ่งที่ตรวจสอบอยู่มีสถานะเป็นเช่นไรพร้อมทั้งมี status information ซึ่งเป็นข้อมูลเพิ่มเติมในการตรวจวัด

### Cacti

เมื่อเปรียบเทียบกับ Nagios โดยทั่วไปแล้ว อาจกล่าวได้ว่า Cacti ไม่ใช่ monitoring tool 100% แต่เป็นเครื่องมือที่ใช้ดึงข้อมูลจากการทำ SNMP polling แล้วมีการแสดงผลตามแบบ RRD graphing อย่างสะดวก (ดูเรื่องการแสดงกราฟและการรายงานผลในหัวข้อต่อไป) แต่ก็อาจกล่าวได้ว่า Cacti ได้มีการทำ monitoring โดยการดูผลจากกราฟแทน ซึ่งโดยพื้นฐานแล้วคือการแสดงปริมาณของ Traffic ที่วิ่งผ่าน Interface ต่างๆ ข้อมูลปริมาณการใช้ CPU หรือ memory เป็นต้นที่ส่วนใหญ่ผู้ดูแลระบบจะคุ้นเคยกับการใช้ MRTG

Cacti สามารถดูสถานะแบบคร่าวๆได้ คือ device status (Up หรือ Down) โดยเข้าไปในหน้า Console->Devices ดังแสดงในรูปที่ 4

Devices										Add	
Type:	Any	Status:	Any	Rows:	30 Rows	Search:		go	clear		
<< Previous										Showing Rows 1 to 4 of 4 [1]	Next >>
Description**	ID	Graphs	Data Sources	Status	Event Count	Hostname	Current (ms)	Average (ms)	Availability	<input type="checkbox"/>	
Amphun	2	6	9	Up	0	10.10.10.18	3.06	5.46	99.81	<input type="checkbox"/>	
localhost	1	4	5	Up	0	127.0.0.1	0.58	0.42	100	<input type="checkbox"/>	
switch11	4	4	4	Up	0	10.10.10.11	2.17	7.84	100	<input type="checkbox"/>	
switch12	3	5	5	Up	0	10.10.10.12	2.23	2.9	100	<input type="checkbox"/>	
<< Previous										Showing Rows 1 to 4 of 4 [1]	Next >>

รูป 4. Cacti: device monitoring

สิ่งที่ Cacti ขาดคือการทำ service monitoring ซึ่งไม่ได้มี Template ที่รับรองโดยตรง (เป็น device monitoring) ส่วนการ monitor Interface ในกรณีที่ system admin ต้องการจะดูรายละเอียดของ Interface ต่างๆของ router หรือ switch นั้นจะไม่สามารถทำได้โดยตรง แต่ถ้าหากจะดู performance ในรูปของ graph ก็ต้องไประบุเป็นแต่ละ Interface ไป

Graph Templates											
Graph Template Name											
Create: Cisco - CPU Usage											
Create: (Select a graph type to create)											
Data Query [SNMP - Interface Statistics]											
<< Previous										Showing Rows 81 to 100 of 123 [1,2,3,4,5,6,7]	Next >>
Index	Status	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	Hardware Address	IP Address	<input type="checkbox"/>		
81	Up	Vlan9	Vl9		propVirtual(53)	1000000000	00:00:15:C7:26:B8:80		<input checked="" type="checkbox"/>		
82	Up	Vlan15	Vl15	**** Amphun to XP [ISS] ****	propVirtual(53)	1000000000	00:00:15:C7:26:B8:80	10.226.226.6	<input type="checkbox"/>		
83	Up	Vlan389	Vl389	**** Amphun [SciPark] to NIL [BTT] ****	propVirtual(53)	1000000000	00:00:15:C7:26:B8:80	203.185.127.254	<input checked="" type="checkbox"/>		
84	Up	Vlan390	Vl390	VLAN for conference at SciencePark [Phathumma FL.3]	propVirtual(53)	1000000000	00:00:15:C7:26:B8:80		<input checked="" type="checkbox"/>		
85	Up	Vlan394	Vl394	NICT FL2	propVirtual(53)	1000000000	00:00:15:C7:26:B8:80		<input type="checkbox"/>		
86	Up	Vlan395	Vl395	AIT	propVirtual(53)	1000000000	00:00:15:C7:26:B8:80		<input type="checkbox"/>		
87	Up	Vlan396	Vl396	NGI-IPv6 [BTT-SciencePark]	propVirtual(53)	1000000000	00:00:15:C7:26:B8:80		<input type="checkbox"/>		
88	Up	Vlan397	Vl397	SIIT-Osaka [Canopy]	propVirtual(53)	1000000000	00:00:15:C7:26:B8:80		<input type="checkbox"/>		

รูป 5. Cacti: List of interfaces

รูปที่ 5 แสดงรายละเอียดของ Interface ซึ่งต้อง click เข้าไปที่ device ก่อน แล้วเลือก Create Graphs for this Host ถึงจะมีตารางให้เลือก Interface ที่ต้องการจะแสดงผลในรูปภาพ

อีกสิ่งหนึ่งที่ Cacti ทำไม่ได้อย่าง Nagios คือเรื่อง Alarming ซึ่งคือการระบุว่าถ้ามีเหตุการณ์ผิดปกติจะต้องแจ้งเตือนไปที่ผู้ดูแลผู้ใด และด้วยวิธีการใด (โดย email หรือ SMS เป็นต้น)

## Zenoss

Event console ของ Zenoss เป็นแหล่งที่ตรวจดูเหตุการณ์ต่างๆที่เกิดขึ้น บ่งบอกถึงระดับความรุนแรงของเหตุการณ์ที่แตกต่างกันไปด้วยแถบสี มีระบบคัดกรองตาม menu ด้านบน และสามารถทำการ sort หรือจัดเรียงได้โดย click ที่ device, component ตามที่แสดงในรูปที่ 6

The screenshot shows the Zenoss Event Console interface. At the top, it says 'Event Console' and 'Zenoss server time: 8:48:00'. Below that, it indicates 'Last updated 2008-09-11 8:47:39.' and 'View Event History...'. The interface includes a search bar and a table of events. The table has columns for 'device', 'component', 'eventClass', 'summary', 'firstTime', 'lastTime', and 'count'. The events are color-coded by severity: orange for critical/warning and yellow for informational.

device	component	eventClass	summary	firstTime	lastTime	count
localhost.localdomain	zencommand	/Status/Heartbeat	localhost.localdomain zencommand heartbeat failure	2008/09/11 08:46:18.00	2008/09/11 08:47:18.00	2
manager.com	pagechecks	/Net	CRITICAL - Socket timeout after 10 seconds	2008/09/08 18:18:33.00	2008/09/09 00:07:10.00	3
manager.com	pagechecks	/Net	HTTP WARNING: HTTP/1.1 404 Not Found	2008/09/11 08:32:17.00	2008/09/11 08:43:17.00	12
AMPHUN.net	unrouted VLAN 2	/Perf/Interface	threshold of Utilization 75 perc exceeded: current value 9983.68	2008/09/11 08:42:20.00	2008/09/11 08:42:20.00	1
AMPHUN.net	unrouted VLAN 4	/Perf/Interface	threshold of Utilization 75 perc exceeded: current value 64.03	2008/09/11 08:42:20.00	2008/09/11 08:42:20.00	1
AMPHUN.net	unrouted VLAN 483	/Perf/Interface	threshold of Utilization 75 perc exceeded: current value 128705.55	2008/09/11 08:42:20.00	2008/09/11 08:42:20.00	1
AMPHUN.net	unrouted VLAN 399	/Perf/Interface	threshold of Utilization 75 perc exceeded: current value 557.06	2008/09/11 08:42:20.00	2008/09/11 08:42:20.00	1
AMPHUN.net	unrouted VLAN 398	/Perf/Interface	threshold of Utilization 75 perc exceeded: current value 595868.39	2008/09/11 08:42:20.00	2008/09/11 08:42:20.00	1
AMPHUN.net	unrouted VLAN 397	/Perf/Interface	threshold of Utilization 75 perc exceeded: current value 5.08	2008/09/11 08:42:20.00	2008/09/11 08:42:20.00	1

รูป 6. Zenoss: Event console

จากตารางในรูปจะเห็นได้ว่า Zenoss มีการจัด Classes หรือการแบ่งแยกหมวดหมู่ไปตามกลุ่มต่างๆ และมีปพลิเคชันย่อยลงไป (Sub-class) เช่น Events, Devices, Services, Processes และ Products ดังนั้นการอ้างอิงถึงสิ่งที่เราจะทำการตรวจวัดสามารถ click ลงไปตาม hierarchy ของ class ได้ และนับได้ว่ามีความละเอียดมากเมื่อเทียบกับซอฟต์แวร์ตัวอื่น เนื่องจากมีรายละเอียดปพลิเคชันที่มีการ define อยู่แล้ว เช่น Class: /Devices/Network/Router/Cisco เป็นต้น

เมื่อไปดูที่รายละเอียดของแต่ละ device เช่น ถ้าเป็น switch หรือ router ถ้า click ไปตาม hierarchy แล้วจะสามารถเห็นรายละเอียดพื้นฐานและสถานะของ interface ที่ SNMP polling เก็บมาได้ตามที่แสดงในรูปที่ 7

/Devices /Network /Switch /295012 Zenoss server time: 23:04:36

▼ Status OS Hardware Software Events Perf Edit

▼ Interfaces

Select: All None

Name	IP Address	Network	MAC	Descr	O	A	Lock
<input type="checkbox"/> <a href="#">FastEthernet0/1</a>			00:0C:30:EA:03:41	"to sw10.10.10.15"	●	●	
<input type="checkbox"/> <a href="#">FastEthernet0/10</a>			00:0C:30:EA:03:4A	"to sw10.10.10.16"	●	●	
<input type="checkbox"/> <a href="#">FastEthernet0/11</a>			00:0C:30:EA:03:4B	to switch 10.10.10.13 519	●	●	
<input type="checkbox"/> <a href="#">FastEthernet0/12</a>			00:0C:30:EA:03:4C	UPLINK FROM ISS to Router IPv6 Tunnel	●	●	
<input type="checkbox"/> <a href="#">FastEthernet0/2</a>			00:0C:30:EA:03:42	NGI-ISS AccessPoint	●	●	
<input type="checkbox"/> <a href="#">FastEthernet0/3</a>			00:0C:30:EA:03:43	TAFF access control	●	●	
<input type="checkbox"/> <a href="#">FastEthernet0/4</a>			00:0C:30:EA:03:44	NGI-ISS AccessPoint-spare	●	●	
<input type="checkbox"/> <a href="#">FastEthernet0/5</a>			00:0C:30:EA:03:45		●	●	
<input type="checkbox"/> <a href="#">FastEthernet0/6</a>			00:0C:30:EA:03:46		●	●	
<input type="checkbox"/> <a href="#">FastEthernet0/7</a>			00:0C:30:EA:03:47	WIFI ADSL	●	●	
<input type="checkbox"/> <a href="#">FastEthernet0/8</a>			00:0C:30:EA:03:48		●	●	
<input type="checkbox"/> <a href="#">FastEthernet0/9</a>			00:0C:30:EA:03:49		●	●	
<input type="checkbox"/> <a href="#">GigabitEthernet0/1</a>			00:0C:30:EA:03:4D		●	●	
<input type="checkbox"/> <a href="#">GigabitEthernet0/2</a>			00:0C:30:EA:03:4E		●	●	
<input type="checkbox"/> <a href="#">Null0</a>					●	●	
<input type="checkbox"/> <a href="#">Vlan1</a>			00:0C:30:EA:03:40		●	●	
<input type="checkbox"/> <a href="#">Vlan3</a>			00:0C:30:EA:03:40		●	●	
<input type="checkbox"/> <a href="#">Vlan399</a>	<a href="#">10.10.10.12/24</a>	<a href="#">10.10.10.0</a>	00:0C:30:EA:03:40		●	●	

1 of 18 < > FastEthernet0/1 > > | show all Page Size 40 ok

▼ Win Services  Monitored

รูป 7. Zenoss: Interface monitoring

## OpenNMS

OpenNMS มีรายละเอียดของ monitoring มากที่สุดเมื่อเปรียบเทียบกับโอเพนซอร์ซซอฟต์แวร์ที่กล่าวมา ถูกพัฒนาขึ้นมาเพื่อรองรับการตรวจสอบสถานะภาพสำหรับเครือข่ายขนาดใหญ่ การออกแบบได้เน้นที่สามสิ่งคือ 1) service availability 2) Data collection และ 3) Event and Notification management

OpenNMS สามารถใช้ดูแลเครือข่ายในระดับจำนวนหมื่นโหนด [6]. นอกจากนี้ใน menu bar ยังมีการ view ได้หลากหลายรูปแบบ เช่น Outages, Path Outages (การ define แบบเป็นเส้นทาง), Events, Alarms, Notification, Assets Inventory (สามารถเชื่อมโยงกับข้อมูลการซ่อมหรือการย้ายอุปกรณ์) นอกจากนี้ยังในระบบยังมีการระบุ event หรือ notification ทุกอย่างเป็นสิ่งที่มี ID หมด และสามารถสืบค้นได้ นอกจากนี้ยังมี option ให้เลือกที่จะ Acknowledge ตามแต่ละ event รูปที่ 8 แสดงตัวอย่างของ Event console ของ OpenNMS

**Home / Events / List**  
 View all events Advanced Search Severity Legend Acknowledge entire search

Event Text:  Time:  Search

Results: (1-10 of 193473)

Search constraints:  1 2 3 4 5 Next Last

Legend

Ack	ID	Severity	Time	Node	Interface	Service	Ackd
<input type="checkbox"/>	232424	Minor [+] [-]	9/10/08 20:04:51 [<] [>]	210.32.200.210 [+] [-]	210.32.200.210 [+] [-]	HTTP	
<a href="#">uei.opennms.org/nodes/nodeLostService</a> [+] [-] Edit notifications for event HTTP outage identified on interface 210.32.200.210 with reason code: Unknown.							
<input type="checkbox"/>	232423	Minor [+] [-]	9/10/08 20:04:51 [<] [>]	210.32.200.210 [+] [-]	210.32.200.210 [+] [-]	SMTP	
<a href="#">uei.opennms.org/nodes/nodeLostService</a> [+] [-] Edit notifications for event SMTP outage identified on interface 210.32.200.210 with reason code: did not connect to host with timeout: 3000ms retry: 1 of 1.							
<input type="checkbox"/>	232422	Normal [+] [-]	9/10/08 20:04:50 [<] [>]	119.146.67.126 [+] [-]			
<a href="#">uei.opennms.org/internal/capsd/rescanCompleted</a> [+] [-] Edit notifications for event A services scan has been completed on this node.							
<input type="checkbox"/>	232421	Warning [+] [-]	9/10/08 20:04:50 [<] [>]	119.146.67.126 [+] [-]	119.146.67.126 [+] [-]	StrafePing [+] [-]	
<a href="#">uei.opennms.org/nodes/nodeGainedService</a> [+] [-] Edit notifications for event The StrafePing service has been discovered on interface 119.146.67.126.							
<input type="checkbox"/>	232420	Warning [+] [-]	9/10/08 20:04:50 [<] [>]	119.146.67.126 [+] [-]	119.146.67.126 [+] [-]	ICMP	
<a href="#">uei.opennms.org/nodes/nodeGainedService</a> [+] [-] Edit notifications for event The ICMP service has been discovered on interface 119.146.67.126.							

**รูป 8. OpenNMS: Event console**

การสืบค้นของ OpenNMS มีความสะดวกมากเมื่อเทียบกับ Zenoss และ Nagios (ไม่มีระบบ search สำหรับ event) ตัวอย่างเช่น OpenNMS มี option ให้ search event ในรูปแบบของ text หรือ drop-down menu สำหรับเลือกเวลา (Any, Last hour, Last 4 hours,..., Last month) ซึ่งนับว่ามีประโยชน์มาก ส่วน Zenoss ถึงแม้ว่าจะมีระบบ search event ในรูปแบบของ text (ดูรูปที่ 6) แต่ถ้าต้องการจะค้นหา event ในอดีตโดยการใส่วันเวลาลงไปจะไม่ค่อยได้ผล และอาจจะต้องเลื่อนตารางขึ้นลงเพื่อดูเอาเอง โดยสรุปแล้วการค้นหาใน OpenNMS นั้นทำได้ง่ายกว่าซอฟต์แวร์ตัวอื่นมาก

Home / Search / Node  
Node: 10.0.0.2  
View Events View Alarms Asset Info HTTP Resource Graphs Rescan Admin

**General (Status: Active)**

View Node Link Detailed Info

**Availability**

Availability (last 24 hours)	47.776%	
10.0.0.2	Overall	47.776%
	HTTP	47.776%
	ICMP	47.776%
	StrafePing	Not Monitored

**Interfaces**

10.0.0.2

**Surveillance Category Memberships (Edit)**

This node is not a member of any categories

**Notification**

You: **Outstanding:** (Check)  
You: **Acknowledged:** (Check)

**Recent Events**

<input type="checkbox"/>	217938	9/10/08 08:22:16	Normal	Node 10.0.0.2 is up.
<input type="checkbox"/>	217763	9/9/08 16:05:17	Normal	A services scan has been completed on this node.
<input type="checkbox"/>	215713	9/9/08 16:03:33	Major	Node 10.0.0.2 is down.
<input type="checkbox"/>	189738	9/8/08 12:53:44	Normal	A services scan has been completed on this node.
<input type="checkbox"/>	170144	9/6/08 12:56:51	Normal	A services scan has been completed on this node.

Acknowledge Reset More...

**Recent Outages**

Interface	Service	Lost	Regained	Outage ID
10.0.0.2	HTTP	9/9/08 16:03:33	9/10/08 08:22:16	107845
10.0.0.2	ICMP	9/9/08 16:03:33	9/10/08 08:22:16	107846

รูป 9. OpenNMS: Notification

รูปที่ 9 แสดงการนำเสนอ notification ที่สรุป event, availability, outage ของแต่ละ node ใน OpenNMS เนื่องจากในมีการเก็บข้อมูลจาก SNMP ในฐานข้อมูลอ้างอิงตาม "primary SNMP" ซึ่งมาจากการเลือก Interface ที่มีค่า IP address ที่ต่ำสุด ดังนั้น performance data จึงถูกเก็บเฉพาะข้อมูลนั้น ดังนั้นถ้าหากต้องการเก็บข้อมูลจากทุก Interface ของ node (router หรือ switch) ต้องไปเปลี่ยนค่าของ *snmpStorageFlag* ในไฟล์ *datacollection-confix.xml* จาก "primary" เป็น "all" แต่ผลก็คือไฟล์ RRD ที่ใช้เก็บจะมีขนาดใหญ่มาก

## 2.การค้นหาลูปกรณในเครือข่าย (Device or Service Discovery)

Nagios และ Cacti ไม่สามารถทำการค้นหาลูปกรณเพิ่มเติมได้ เป็นเพียงระบบที่ตรวจสอบลูปกรณที่ผู้ใช้ได้ระบุไว้ในตอนต้นแล้วเท่านั้น ส่วน Zenoss และ OpenNMS มีความสามารถในการค้นหาเพิ่มมากกว่านั้น

### Zenoss

Zenoss สามารถค้นหา device ที่มี IP address ในเครือข่าย โดยเฉพาะอย่างยิ่งถ้าสามารถดึงข้อมูลผ่านทาง SNMP ได้ Zenoss ก็จะเพิ่ม device นั้นไปได้  
Zenoss ใช้ daemon ที่ชื่อว่า ZenDisc ทำการค้นหา device ที่มี SNMP agent run อยู่ โดยจาก Zenoss menu ให้เลือกที่ Networks -> Subnetworks แล้วเลือก Discover Devices จาก Subnetworks menu (หากไม่มี subnetwork ที่ต้องการก็สามารถใส่เพิ่มไปได้) Zenoss ก็จะ

search หาข้อมูลจาก routing tables ของทุก router ที่สามารถหาได้และทำการ ping และ snmp device ที่เกี่ยวข้อง เมื่อเจอ device หลังจากทำการ scan แล้ว Zenoss จะทำการเพิ่ม device ที่ค้นหาเจอไปใน Class /Discovered ซึ่งผู้ใช้สามารถเลือก Move to Class หรือ Change Class จาก menu ได้ ดังนั้นผู้ดูแลเครือข่ายสามารถเห็น device เพิ่มเติมนอกเหนือจากการเพิ่ม device แบบ manual อย่างไรก็ตาม device ที่เพิ่มค้นหาเพิ่มมาเมื่อ click ตามไปดูที่รายละเอียด ส่วนใหญ่จะไม่สามารถดูข้อมูลเพิ่มเติมได้ เนื่องจากยังไม่มีการ set SNMP community ซึ่งค่า default คือ *public* แต่ผู้ดูแลไม่ได้เปิด snmp agent ด้วยค่า community= *public* อยู่แล้วเพราะไม่มีความจำเป็นให้ผู้ใช้ที่ไม่เกี่ยวข้องสามารถดูข้อมูลได้ ดังนั้นหากต้องการดูรายละเอียดเพิ่มเติมต้องไปปรับแต่งค่าของ community และมาเปลี่ยนค่าใน Zenoss ให้ตรงกัน

นอกจากนี้ถ้าต้องการให้ Zenoss ค้นหาอุปกรณ์ใน subnet ที่ define อยู่แล้วโดยอัตโนมัติ ผู้ใช้ต้องไปทำการปรับแต่งที่ menu /Network แล้วเลือกไปที่ Subnet นั้น แล้วตรวจดูที่ค่าใน zProperties ว่า zAutoDiscover ถูกเลือกให้เป็น *True*

## OpenNMS

การค้นหาอุปกรณ์ใน OpenNMS มีความละเอียดเป็นอย่างมาก โดยในการค้นหานั้นสามารถแบ่งได้เป็นสองขั้นตอน ในขั้นตอนแรกเป็นการตรวจสอบว่าสามารถติดต่ออุปกรณ์นั้นอยู่หรือไม่ โดยมีการกำหนด parameter สำหรับการ ping เช่น packets-per-second, timeout, ช่วงของ IP address ที่ต้องการหาหรือช่วงที่ไม่ต้องการ เป็นต้น ซึ่งจะอยู่ในไฟล์ *discovery-configuration.xml* ผลที่ได้หลังจากการค้นหาคือ IP address ที่สามารถ monitor ได้ หลังจากนั้นขั้นตอนต่อไปคือการค้นหา service ที่ขึ้นอยู่กับ IP address นั้นๆ ขั้นตอนที่สองนี้จะเป็นกระบวนการที่ซับซ้อนกว่าขั้นตอนแรกมาก

ขั้นตอนต่อไปหลังจากพบว่ามีอุปกรณ์นี้แล้วคือการค้นหา service (เช่น httpd, DNS, DHCP) ที่เราจะทำการ monitor โดยการใช้ process ที่ชื่อว่า *caspsd* ที่ define parameter ต่างๆไว้ในไฟล์ *caspsd-configuration.xml* ซึ่ง ขั้นตอนที่สองนี้เรียกว่า *Capabilities check* ก่อนอื่น caspsd จะทำการตรวจดูแต่ละ interface ถ้าหากมี service ใหม่เพิ่มขึ้นมา OpenNMS ทดสอบเครือข่ายในการค้นหาด้วย protocol ต่างๆ ดังแสดงในเอกสารอ้างอิง [7] ซึ่งเป็น protocol plugin ที่สามารถนำไปใช้ทดสอบว่า service นั้นๆมีอยู่จริง แล้วก็สามารถปรับแต่งให้ scan IP address แคบลงช่วงก็ได้ หรือจะระบุให้ใช้ protocol นั้นๆสำหรับการตรวจสอบสถานะเลยก็ได้ (ไม่ใช่แค่ test ตอน scan ตอนแรก)

ส่วน SNMP protocol plugin จะต่างกับชนิดอื่นเพราะเป็นเรื่องของการเก็บข้อมูล และต้องไปปรับแต่งเพิ่มเติมในไฟล์ *snmp-config.xml* ถ้าสามารถเข้าถึงข้อมูล ipAddrTable และ ifTable ของอุปกรณ์ได้ ก็จะนำ IP address ใน ipAddrTable ไปทำการ scan ต่อ ขอให้อ่านรายละเอียดเพิ่มเติมโดยละเอียดใน [7]

ค่า default ของการ update Discovery จะมีการทำทุกๆ 24 ชั่วโมง ตัวอย่าง UI ที่ทำการ configure Discovery service ซึ่งมีการเพิ่มเข้าหรือนำออก IP address หรือช่วงของ IP address แสดงในรูปแบบที่ 10

Home / Admin / Discovery / Modify Configuration

Save and Restart Discovery

**General settings**

Initial sleep time (sec.):  Restart sleep time (hours):  Threads:  Retries:  Timeout (ms.):

**Specifics**

No Specifics found.

**Include Ranges**

<input type="button" value="Add New"/>	Begin Address	End Address	Timeout (ms.)	Retries	Action
	10.10.10.10	10.10.10.19	800	3	<input type="button" value="Delete"/>
	10.226.2.17	10.226.2.22	800	3	<input type="button" value="Delete"/>
	10.226.0.42	10.226.0.42	800	3	<input type="button" value="Delete"/>

**Exclude Ranges**

No exclude range defined.

Save and Restart Discovery

รูป 10. OpenNMS: Configuration of Discovery service

### 3.การปรับแต่งระบบ (Configuration) และการใช้ Plug-in หรือการใช้ External scripts

ความยากง่ายในการปรับแต่งระบบหรือ Configuration นับว่ามีความจำเป็นอย่างสูงสำหรับ system admin ด้วยเหตุที่ว่าหาก configuration ทำได้ยากแล้ว การเพิ่มอุปกรณ์เข้าไปใหม่ การเพิ่มการตรวจสอบโดยเปลี่ยนแปลง parameter หรือ threshold ต่างๆ การจัดการกับจำนวนอุปกรณ์หรือ Interface จำนวนมากจะมีเป็นปัญหาใหญ่

#### Cacti

เนื่องจากการ configure ระบบของ Cacti ส่วนใหญ่จะเป็น graph management ซึ่งประกอบด้วย การเพิ่ม device ที่จะ monitor การ set parameter สำหรับ SNMP polling และ การเพิ่มและการปรับแต่งกราฟสำหรับอุปกรณ์ หรือ interface ของอุปกรณ์ โดยทั่วไปแล้วการปรับแต่งทำได้ง่ายและมีรายละเอียดที่เพียงพอ Cacti ยังมี Template ต่างๆสำหรับ Graph Templates (เช่น Interface Traffic, Linux Memory Usage, Cisco CPU Usage) Host Templates (เช่น Cisco Router, Generic SNMP-enabled Host, Windows Host) และ Data Templates (สำหรับการ define data source สำหรับการเก็บด้วย SNMP) Template เหล่านี้สามารถแก้ไขเพิ่มเติมได้ตามความต้องการ

#### Nagios

Nagios ไม่สามารถ configure ผ่านหน้า Web UI แต่จะต้องไปแก้ไข configuration ไฟล์ต่างๆ เช่น Main configuration file, Resource files, Object definition files และ CGI configuration files

(กรุณาอ่านรายละเอียดใน [2] และรายงาน [8]) ส่วนเรื่องการควบคุม บน UI นั้น Nagios สามารถ turn on/off service checks และการ schedule queues สำหรับการตรวจสอบต่างๆ

ถึงแม้ว่าการ configure ใน Nagios จะดูยุ่งยากกว่าซอฟต์แวร์อื่นที่สามารถปรับแต่งผ่านทาง UI แต่ Nagios มีความยืดหยุ่นสูงในการในการแก้ไขดัดแปลงหรือเพิ่มเติมเพื่อให้เหมาะกับสิ่งที่ต้องการ monitor โดยเฉพาะอย่างยิ่งการใช้ Plugin หรือ external script เนื่องจากการทำงานใน core ของ Nagios เองไม่ได้มีโปรแกรมสำหรับตรวจสอบสถานะของ host หรือ service ต่างๆโดยเบ็ดเสร็จจ้อยู่ภายในตัวเหมือน monitoring tool ตัวอื่นๆ ดังนั้น Nagios จึงต้องใช้ external program หรือ plugin ในการตรวจสอบและส่งค่าที่ตรวจสอบกลับมาเพื่อแสดงผล โดยผู้ใช้สามารถพัฒนา plugin ขึ้นมาเองได้หรือใช้ plugin ที่มีอยู่ก็ได้ โดยทั่วไปแล้ว plugin ที่ใช้งานตามปกติของ Nagios (อยู่ใน *libexec* directory) จะเป็นโปรแกรมสำหรับตรวจวัดสถานะทั่วไปหรือวัด performance เช่น *check\_ping*, *check\_http* หรือ *check\_load* เป็นต้น แต่หากผู้ใช้ต้องการ plugin ที่ specific สำหรับงานบางอย่างก็สามารถใช้ plugin พิเศษที่มีผู้พัฒนาขึ้นมาได้ ตัวอย่างเช่น plugin สำหรับตรวจสอบอุณหภูมิของเครื่อง server บางรุ่น

นอกจาก plugin แล้ว Nagios ยังมี Addon ที่ช่วยทำงานเสริมกับระบบหลักอีก เช่น NRPE สำหรับการ ใช้ plugin บน Unix/Linux remote machine หรือ NSClient++ ที่ใช้เป็น agent สำหรับ Windows

## Zenoss

การเพิ่มอุปกรณ์ใน Zenoss สามารถทำได้โดยสะดวก นอกจากนี้ยังทำการ configure หลักๆได้หลายอย่าง เช่น ใน menu *Settings* สามารถ define commands ที่ใช้ ส่วนเรื่อง user management สามารถ define use's level of access และการ view event และตั้งค่า alert โดยการ define alerting rule และการ สำหรับ SNMP สามารถเพิ่ม MIB ได้จาก UI ในเรื่องการควบคุมผ่าน UI Zenoss สามารถ เปิดหรือปิด daemon ทุกตัวที่ใช้อยู่ นอกจากนี้การ Browse ในทุก category ถ้าไม่มี list ของสิ่งที่ต้องการอยู่จะสามารถเพิ่มไปใน list ได้โดยสะดวกโดยผ่านทาง *Add New Organizer*

ในการใช้ plugin นั้น Zenoss ใช้ *ZenPack* ซึ่งก็คือ package ที่เพิ่ม functionality ให้กับ Zenoss โดยอาจไปเพิ่ม action rules, commands, data sources, class หรือ templates ต่างๆ ตัว Core ZenPacks เช่น *HttpMonitor*, *FTP Monitor*, *DNSMonitor* ไม่ได้มากับ Zenoss Core ตอนติดตั้ง ผู้ใช้ต้องdownload มาติดตั้งเพิ่มเติมเอง นอกจากนี้ยังมี plugin เพิ่มเติมอื่นๆที่ถูกพัฒนาให้เหมาะกับ Manufacturer บางอย่าง

Plugin ใน ZenPack บางอย่างคล้ายกับที่ Nagios ใช้ เช่น *HttpMonitor* ที่ใช้ command *check\_http* ซึ่งอยู่ใน *libexec* directory นอกจากนี้ Zenoss ได้นำ plugin บางอันของ Nagios มาใช้ด้วย การลง plugin อาจลงผ่านทาง command หรือ *ZenPacks* manager ซึ่งผู้ใช้สามารถสร้าง Zenoss plugin package ได้ด้วย (โดยเลือก *Create a ZenPack*)

## OpenNMS

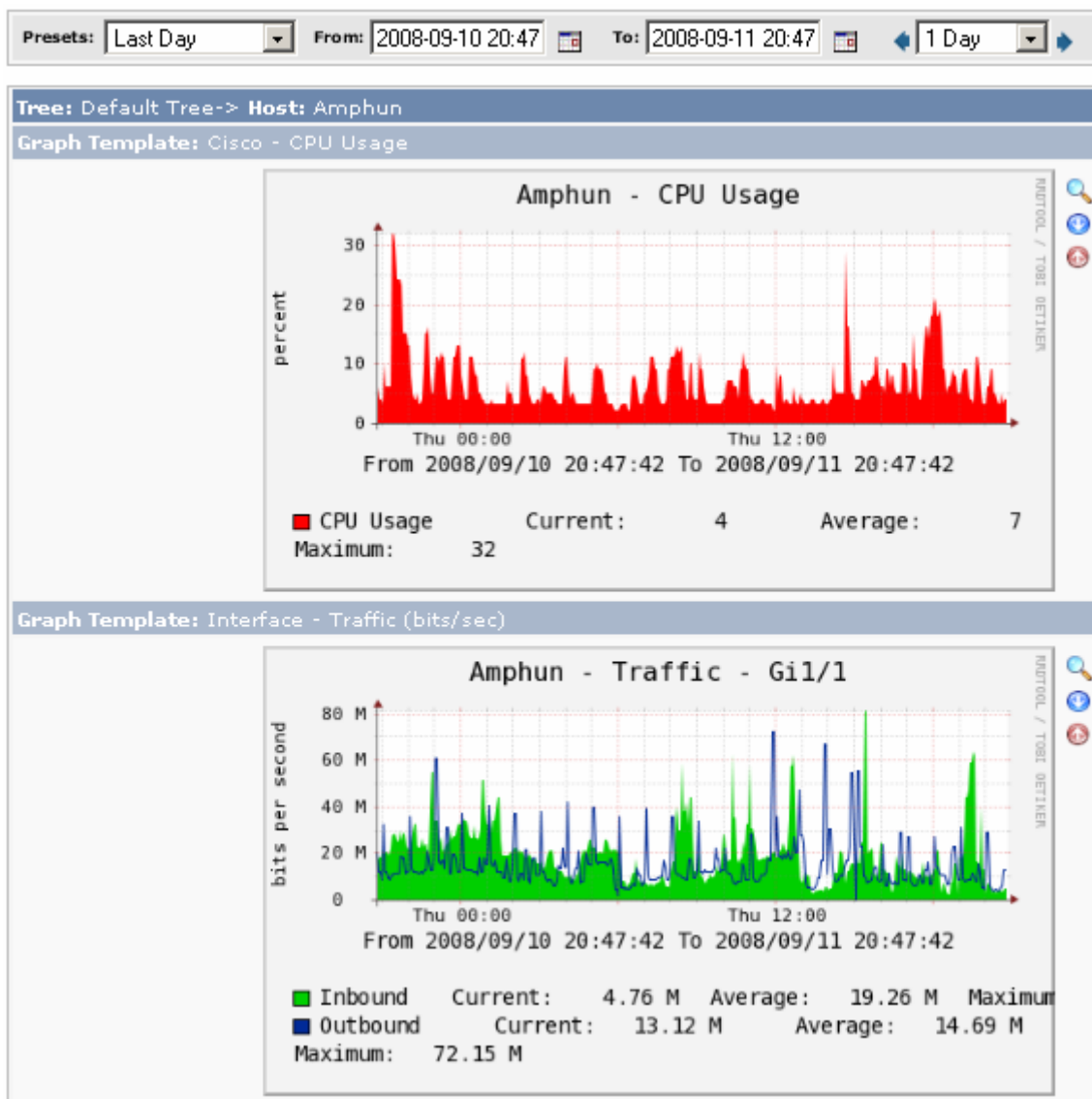
การ configure ใน OpenNMS สามารถทำได้หลากหลายและละเอียดมาก เนื่องจากถูกพัฒนามาให้ปรับแต่งได้โดยง่ายผ่านทาง UI ตัวอย่างเช่น ใน menu *Home/Admin* มีการ configure สำหรับ Discovery, Users and Groups, Notifications, Manage SNMP Data Collection per Interface, Add Interface และ Manage Thresholds เป็นต้น

OpenNMS มี plugin สำหรับการ monitor เบ็ดเสร็จอยู่แล้วในตัว ตามที่กล่าวแล้วใน [7] ส่วน plugin เพิ่มเติมอื่นๆก็สามารถเพิ่มได้ การแก้ไขไฟล์ *poller-configuration.xml* และ *capsd-configuration.xml* นอกจากนี้ OpenNMS ได้ออกแบบให้สามารถใช้งานกับ NRPE ของ Nagios สำหรับการตรวจสอบ remote machine ได้

#### 4.การรายงานผล การแสดงกราฟ และแผนที่การเชื่อมต่อ

##### Cacti

ดังที่กล่าวมาแล้วในหัวข้อที่ 3 จุดเด่นของ Cacti คือการแสดงผลผ่านทางกราฟ ผู้ใช้สามารถเลือก options และ Template ต่างๆในการแสดงผล และสามารถเพิ่มหรือลดจำนวนกราฟได้อย่างสะดวก เนื่องจาก UI ได้ถูกออกแบบให้ผู้ใช้ปรับแต่งได้ง่าย แต่ Cacti จะไม่มีแผนที่แสดงการเชื่อมต่อเหมือน tool อื่น



รูป 11. Cacti: Graph Display

## Nagios

Nagios ไม่มีรูปแบบการแสดงผลที่ละเอียดเหมือน Cacti และกราฟของ Nagios ก็ไม่ใช่ performance graph (เช่น Throughput, CPU load, Response time) แต่จะเป็น Event history แทน ซึ่งเป็นการแสดงผลของจำนวนเหตุการณ์ที่เกิดขึ้นสำหรับ Host (Recovery (Up), Down, Unreachable) หรือสำหรับ Service (Recovery (OK), Warning, Unknown, Critical) ตามช่วงเวลาที่เราเลือก

ในส่วนของ Availability report มีการสรุปผลดังแสดงในรูปที่ 12

**Host Availability Report**  
Last Updated: Sat Sep 27 21:11:56 ICT 2008  
Nagios@ 3.0 - [www.nagios.org](http://www.nagios.org)  
Logged in as *nagiosadmin*

**All Hosts**

First assumed host state: Unspecified  
First assumed service state: Unspecified

09-01-2008 00:00:00 to 09-27-2008 21:11:56  
Duration: 26d 21h 11m 56s

Report period: This Month  
Backtracked archives: 4

[ Update ]

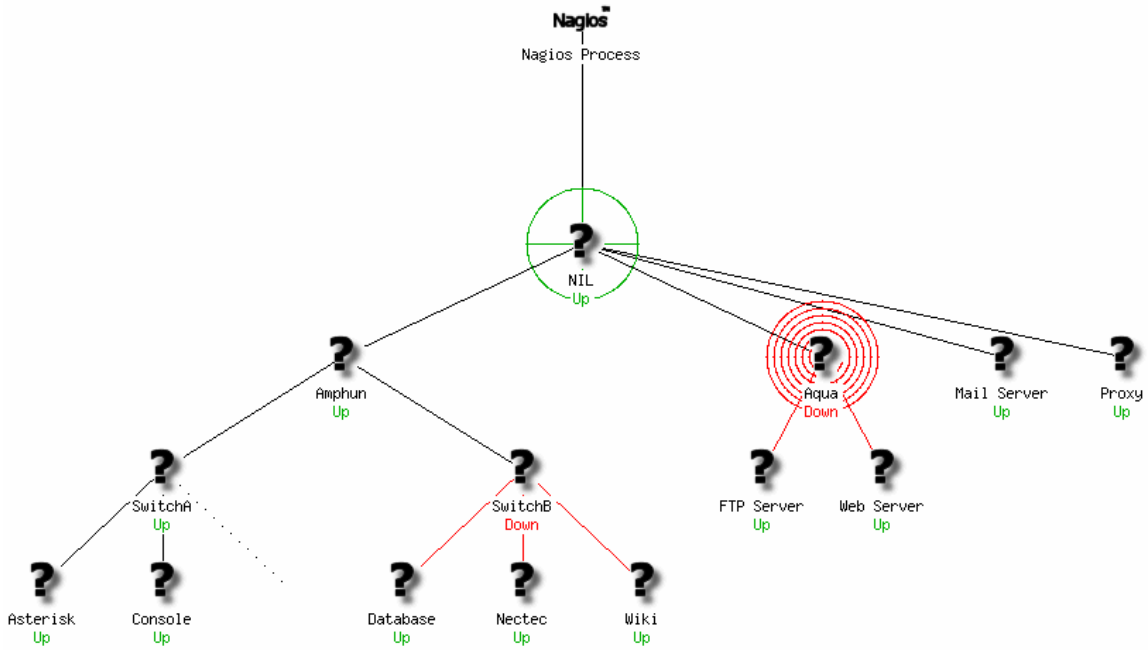
[ Availability report completed in 0 min 0 sec ]

**Host State Breakdowns:**

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
<a href="#">Amphun</a>	98.787% (98.787%)	0.000% (0.000%)	1.213% (1.213%)	0.000%
<a href="#">Aqua</a>	0.000% (0.000%)	98.764% (98.764%)	1.236% (1.236%)	0.000%
<a href="#">Asterisk</a>	98.789% (98.789%)	0.000% (0.000%)	1.211% (1.211%)	0.000%
<a href="#">Console</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Database</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">FTP Server</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Mail Server</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">NIL</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Nagios</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Nectec</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Proxy</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">SwitchA</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">SwitchB</a>	0.000% (0.000%)	98.750% (98.750%)	1.250% (1.250%)	0.000%
<a href="#">Web Server</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Wiki</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	86.505% (86.505%)	13.168% (13.168%)	0.327% (0.327%)	0.000%

รูป 12. Nagios: Availability Report

นอกจากนี้ Nagios ยังสามารถแสดงแผนที่การเชื่อมต่อระหว่างอุปกรณ์ต่างๆแบบเป็น hierarchy ของ node ตามที่แสดงในรูปที่ 13 แต่ต้องมีการ define ความสัมพันธ์ระหว่างคู่ node (เป็น parent-child relationship) ในไฟล์ configuration ก่อน เนื่องจาก Nagios ไม่ได้มี snmp built-in feature ที่สามารถทำ auto-discovery ได้เอง



ຮູບ 13. Nagios: Map

## Zenoss

/Reports /Performance Reports /Availability Report Zenoss server time: 16:48:5

Device:  Component:

Start Date: 09/15/2008  End Date: 09/22/2008

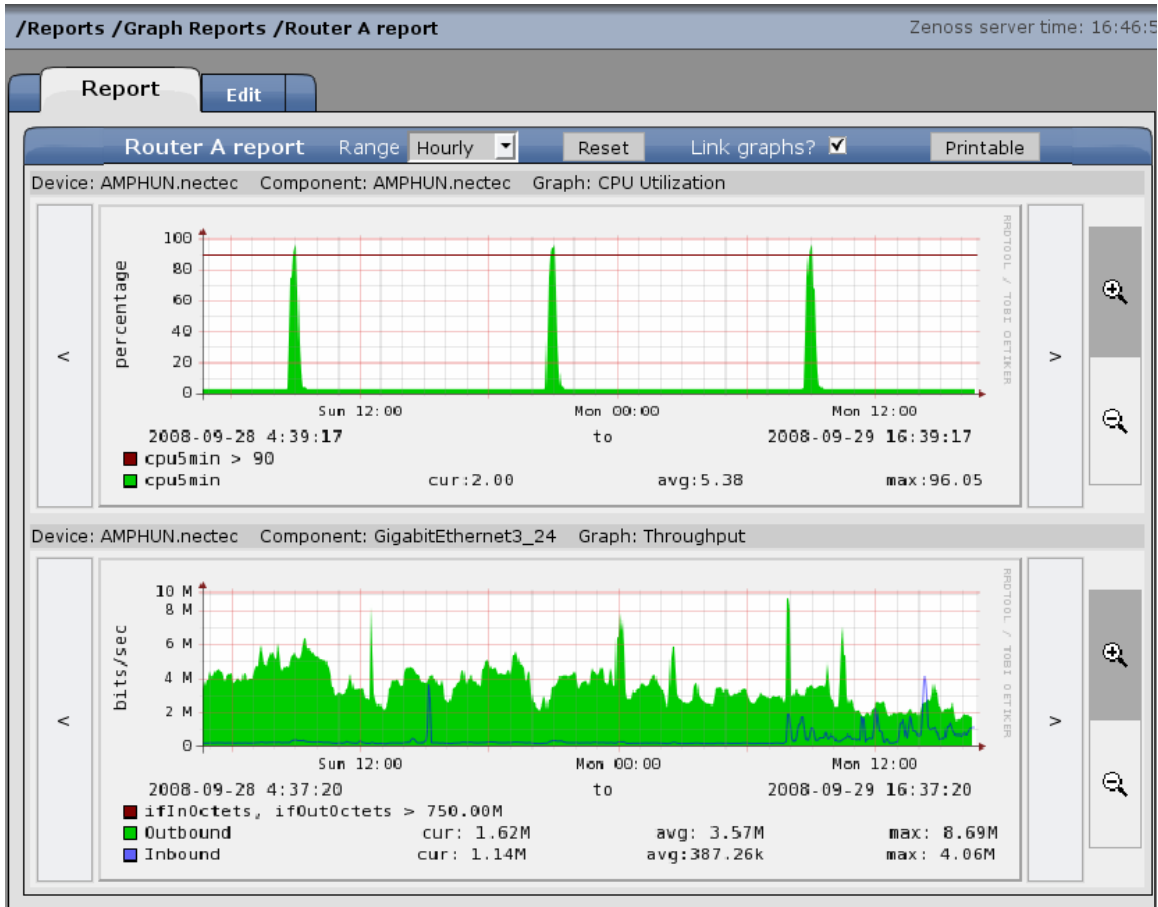
Event Class: /Status/Ping  Severity: Error

Device	Component	Systems	Availability
<a href="#">10.10.10.36</a>			99.822%
<a href="#">10.10.10.102</a>			99.891%
<a href="#">Aqua.nectec.or.th</a>			99.891%
<a href="#">netmon</a>			99.941%
<a href="#">NIL.nectec.or.th</a>			99.941%
<a href="#">10.10.10.14</a>			99.941%
<a href="#">10.10.10.35</a>			99.941%
<a href="#">295012</a>			99.941%
<a href="#">295013</a>			99.941%
<a href="#">290011</a>			99.941%
<a href="#">295016</a>			99.941%
<a href="#">AMPHUN.nectec</a>			99.941%
<a href="#">295015</a>			99.941%
<a href="#">375010</a>			99.941%
<a href="#">manager.co.th</a>			100.000%
<a href="#">google.com</a>			100.000%

1 of 16   0.998219995039   show all export all Page Size 40

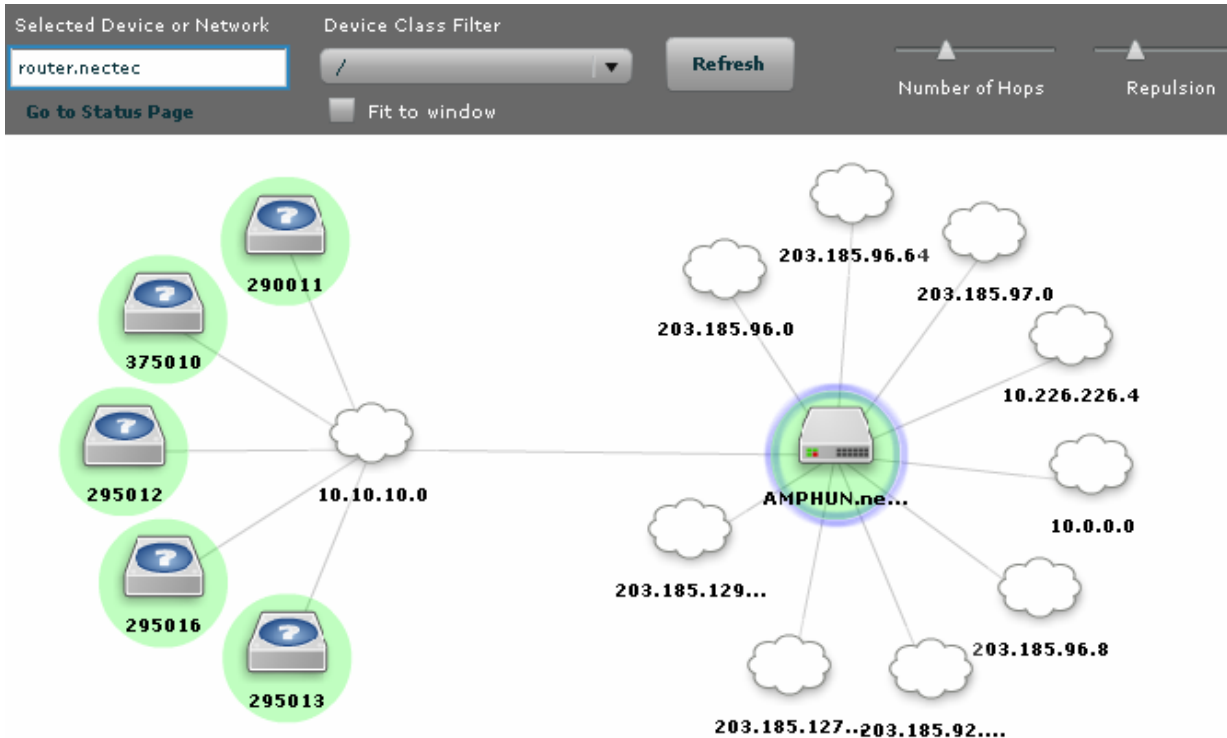
ຮູບ 14. Zenoss: Availability Report

Zenoss มีการแสดงผลเป็นรายงานในหลากหลายรูปแบบทำให้สามารถสื่อให้เห็นมุมมองตามอุปกรณ์ต่างๆหรือหมวดหมู่ (Class) ต่างๆ เช่น Device reports (ซึ่งมีรายงานย่อยอีกหลายแบบ เช่น All devices, All monitored devices, Device changes เป็นต้น) Event reports Graph report (สำหรับการเลือกแสดง performance graph ที่มีอยู่ในรูปแบบของรายงาน) Performance report (ซึ่งมีรายงานย่อยๆ เช่น Availability report, CPU/Interface/Memory Utilization, Threshold summary เป็นต้น) รูปที่ 14 แสดงตัวอย่างของ Availability report ส่วนรูปที่ 15 แสดง Graph report ซึ่งผู้ใช้สามารถเลือกกราฟมาแสดงและปรับแต่งรูปแบบได้โดยสะดวก แต่ถ้าต้องการจะแสดงผลนอกเหนือจาก performance graph ที่มีอยู่หรือต้องการบางรูปแบบพิเศษเช่นการแสดงผลของกราฟหลายอันบนแกนเดียวกันก็สามารถปรับแต่งได้ใน menu Multi-graph report



รูป 15. Zenoss: Graph report

ส่วนการแสดงผลการเชื่อมต่อ (Map) นั้น Zenoss จะไม่แสดงการเชื่อมต่อให้โดยอัตโนมัติ แต่ผู้ใช้ต้องไปกรอกข้อมูลลงในช่อง Device หรือ Network ก่อนแล้วถึงจะดูได้ ซึ่งสิ่งนี้ควรจะมีการปรับปรุงให้ดูได้โดยอัตโนมัติ นอกจากนี้ความถูกต้องของ Topology ที่แสดงใน map ยังไม่ถูกต้องนักและอุปกรณ์บางตัวที่มีการ monitor ก็ไม่ได้แสดงใน map ซึ่งโดยทั่วไปแล้ว map ของ OpenNMS จะแสดงผลได้ดีกว่า (ดูในหัวข้อถัดไป)



รูป 16. Zenoss: Map

## OpenNMS

การรายงานผลของ OpenNMS มีรายงานที่หลากหลายคล้ายกับ Zenoss ซึ่งส่วนใหญ่เป็นรายงานชนิดที่แสดงผลซึ่งเป็นตัวชี้วัด SLA เช่น Availability หรือ Outage report เป็นต้น เช่น การสรุปผล availability โดยรวมดังแสดงในรูปที่ 17 นอกจากนี้ยังมีการแสดงผลในรูปแบบของกราฟ ซึ่งก็ใช้รูปแบบการปรับแต่งในคล้ายๆกับ Cacti และ Zenoss แต่ OpenNMS จะไม่มี graph template ให้เลือกใน UI เหมือน Cacti และ Zenoss ส่วนใหญ่การปรับแต่งใน OpenNMS จะไม่ซับซ้อนมากนัก เช่น ตัวอย่างแสดงในรูปที่ 18 ส่วนรูปที่ 19 เป็นหน้ารายงานกราฟซึ่งสามารถระบุช่วงเวลาที่ต้องการแสดงได้

Home / SLM / Category

Overall Service Availability

Show interfaces:  All  With outages  With availability < 100%

This category reflects availability of all services currently being monitored by OpenNMS.

Nodes	Outages	24hr Availability
087231080223.chello.fr	0 of 1	62.467%
10.0.0.2	0 of 2	62.589%
10.10.10.100	0 of 4	62.590%
10.10.10.102	0 of 2	62.520%
10.10.10.104	1 of 1	0.000%
10.10.10.14	0 of 2	62.589%
10.10.10.17	0 of 2	62.596%
10.10.10.19	0 of 1	62.590%
10.10.10.20	0 of 1	62.586%
10.10.10.35	0 of 2	62.586%
10.10.10.9	0 of 4	62.004%

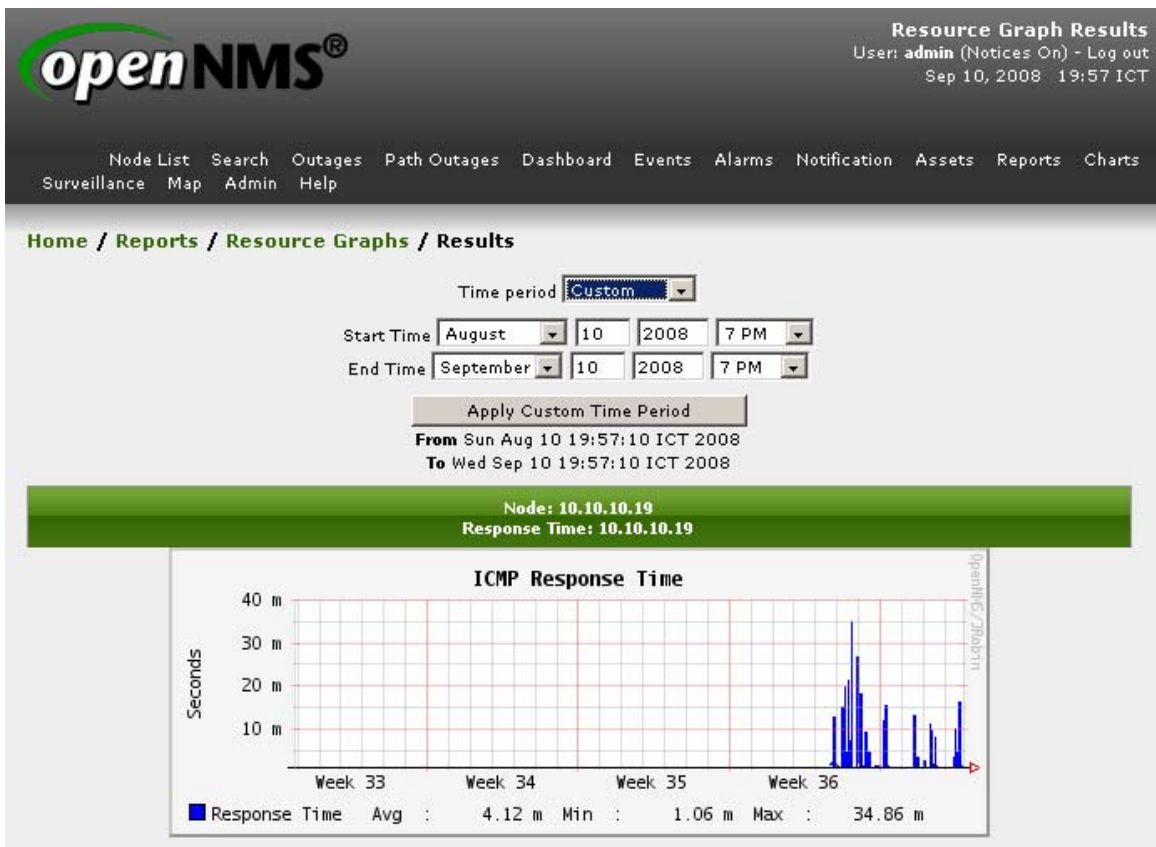
រូប 17. OpenNMS: Availability Report

Home / Reports / Resource Graphs / Custom  
 Step 2: Choose Data Sources

Node: 202.44.204.44  
 Response Time: 202.44.204.44

<b>Data Source 1 (required):</b> <input type="checkbox"/> icmp <input checked="" type="checkbox"/> ssh <input type="checkbox"/> http	Title: <input type="text" value="Data Source 1"/> Color: <input type="text" value="Red"/> Style: <input type="text" value="Medium Line"/> Value Type: <input type="text" value="Average"/>
<b>Data Source 2 (optional):</b> <input type="checkbox"/> icmp <input checked="" type="checkbox"/> ssh <input type="checkbox"/> http	Title: <input type="text" value="Data Source 2"/> Color: <input type="text" value="Green"/> Style: <input type="text" value="Medium Line"/> Value Type: <input type="text" value="Average"/> <input type="text" value="Average"/> <input type="text" value="Minimum"/> <input type="text" value="Maximum"/>
<b>Data Source 3 (optional):</b> <input type="checkbox"/> icmp <input checked="" type="checkbox"/> ssh <input type="checkbox"/> http	Title: <input type="text" value="Data Source 3"/> Color: <input type="text" value="Blue"/> Style: <input type="text" value="Medium Line"/> Value Type: <input type="text" value="Average"/>
<b>Data Source 4 (optional):</b> <input type="checkbox"/> icmp <input type="checkbox"/> ssh <input type="checkbox"/> http	Title: <input type="text" value="Data Source 4"/>

រូប 18. OpenNMS: Graph Management



รูป 19. OpenNMS: Graph Display

จุดเด่นของ OpenNMS อีกอย่างหนึ่งคือการแสดงผลการเชื่อมต่อของอุปกรณ์ รูปที่ 20 แสดงการเชื่อมต่อของอุปกรณ์ที่ดูแล โดยมีการแสดงสถานะของอุปกรณ์ด้วยสัญลักษณ์ที่ดูง่าย นอกจากนี้ หาก right-click ไปที่ node นั้นๆ จะสามารถทำการ execute command *ping* หรือ *traceroute* และสามารถเข้าไปดู event หรือ resource graph ที่เกี่ยวข้องกับอุปกรณ์นั้นๆด้วย

จากการทดสอบการแสดงผลการเชื่อมต่อภายในองค์กรพบว่า OpenNMS มีความถูกต้องสูงกว่า 80% การที่ OpenNMS มีประสิทธิภาพมากกว่า Zenoss ในด้านนี้คาดว่ามาจากที่ OpenNMS ใช้ process ที่ซับซ้อนกว่า Zenoss ในการทำ Discovery ซึ่งประกอบด้วยการทดสอบ protocol จำนวนมาก รวมทั้งการได้ข้อมูลโดยละเอียด เช่น จาก routing table ของ router แต่อีกปัญหาหนึ่ง ซึ่งเป็นปัญหาของ tool ตัวอื่นด้วยคือ ไม่สามารถเห็นการเชื่อมต่อของอุปกรณ์ที่มาจาก Manufacturer ต่างกัน ซึ่งเป็นโจทย์ที่น่าสนใจที่ควรพัฒนาต่อไป แต่ทั้งนี้ขึ้นอยู่กับว่าอุปกรณ์นั้นมี MIP สำหรับรองรับการเข้าถึงข้อมูลที่จำเป็นได้หรือไม่

The screenshot shows the OpenNMS web interface. At the top left is the OpenNMS logo. To the right, it says 'Display Map' and 'User: admin (Notices On) - Log out' with the date 'Sep 10, 2008 19:09 ICT'. Below this is a navigation menu with items: Node List, Search, Outages, Path Outages, Dashboard, Events, Alarms, Notification, Assets, Reports, Charts, Surveillance, Map, Admin, Help. The main content area has a breadcrumb trail: 'Home / Map / View Network Map'. The network map shows several nodes connected by lines. Nodes are labeled with IP addresses: 10.10.10.17, 295016, 295012, 295013, 10.10.10.101, 290011, 10.10.10.10, 203.185.97.42, 203.185.97.40, 10.10.10.18, 203.185.97.41, 10.10.10.1, 203.185.97.43, 203.185.97.44, and 10.10.10.1. A context menu is open over the node 10.10.10.1, showing options: Ping, Traceroute, Events, and Resource Graphs.

รูป 20. OpenNMS: Map

## บทสรุป

เนื่องจากซอฟต์แวร์ที่มีคุณลักษณะเหมาะสมกับงานดูแลเครือข่ายจำเป็นต้องมีประสิทธิภาพสูงและสามารถปรับแต่งและใช้งานได้ง่าย รายงานนี้จึงเปรียบเทียบและวิเคราะห์ซอฟต์แวร์ที่เกี่ยวข้องเพื่อเป็นประโยชน์ต่อการเลือกใช้ในองค์กรและเพื่อเป็นแนวทางในการพัฒนาต่อไป

จากการวิเคราะห์พบว่าซอฟต์แวร์แต่ละชนิดมีความสามารถพิเศษแตกต่างกันไปตามลักษณะการใช้งาน หากเน้นการแสดงผลในรูปแบบของกราฟที่สามารถเลือก Template ต่างๆ ได้มากมาย Cacti อาจเป็นทางเลือกที่ดี แต่ถ้าต้องการซอฟต์แวร์ที่ทำการตรวจสอบและดูแลเครือข่ายได้โดยละเอียดและมีการปรับแต่งผ่าน UI ได้หลายรูปแบบ ก็อาจเลือกใช้ OpenNMS หรือ Zenoss แต่ทั้งนี้ขึ้นอยู่กับความจำเป็นในการใช้ ตัวอย่างเช่น OpenNMS อาจเกินความจำเป็นในการดูแลเครือข่ายขนาดเล็ก ส่วนซอฟต์แวร์ Nagios มีความยืดหยุ่นในการใช้งานสูงถึงแม้จะไม่มี UI สำหรับทำ configuration แต่การที่มี Plugin หลากหลายและมี developer community ที่แข็งแกร่งจึงมีแนวโน้มที่ดีสำหรับการนำไปพัฒนาต่อยอดเพื่อใช้กับระบบบริหารจัดการเครือข่ายได้

## รายการอ้างอิง

- [1] Jack Hughes, *Open Source network management download comparison*, <http://www.openextra.co.uk/blog/open-source-network-management-download-comparison/>
- [2] Nagios, <http://www.nagios.org>
- [3] Zenoss, <http://www.zenoss.com>
- [4] OpenNMS, <http://www.opennms.org>
- [5] Cacti, <http://www.cacti.net>
- [6] FAQ-About OpenNMS, <http://www.opennms.org/index.php/FAQ-About>
- [7] Discovery, [http://www.opennms.org/index.php/Discovery\\_Configuration\\_How-To](http://www.opennms.org/index.php/Discovery_Configuration_How-To)
- [8] ชาวีร์ อีสริยภัทร์, กุลวดี ศรีพานิชกุลชัย, กุลชาติ มีทรัพย์หลาก, การพัฒนาโมดูลในการตัดเก็บข้อมูลเชิงสถิติของอุปกรณ์เครือข่ายสำหรับ Nagios, รายงานวิจัยฉบับสมบูรณ์, NECTEC, ส.ค. 2550
- [9] UCD-SNMP (NET-SNMP) Integration  
[http://nagios.sourceforge.net/docs/1\\_0/int-snmpttrap.html](http://nagios.sourceforge.net/docs/1_0/int-snmpttrap.html)