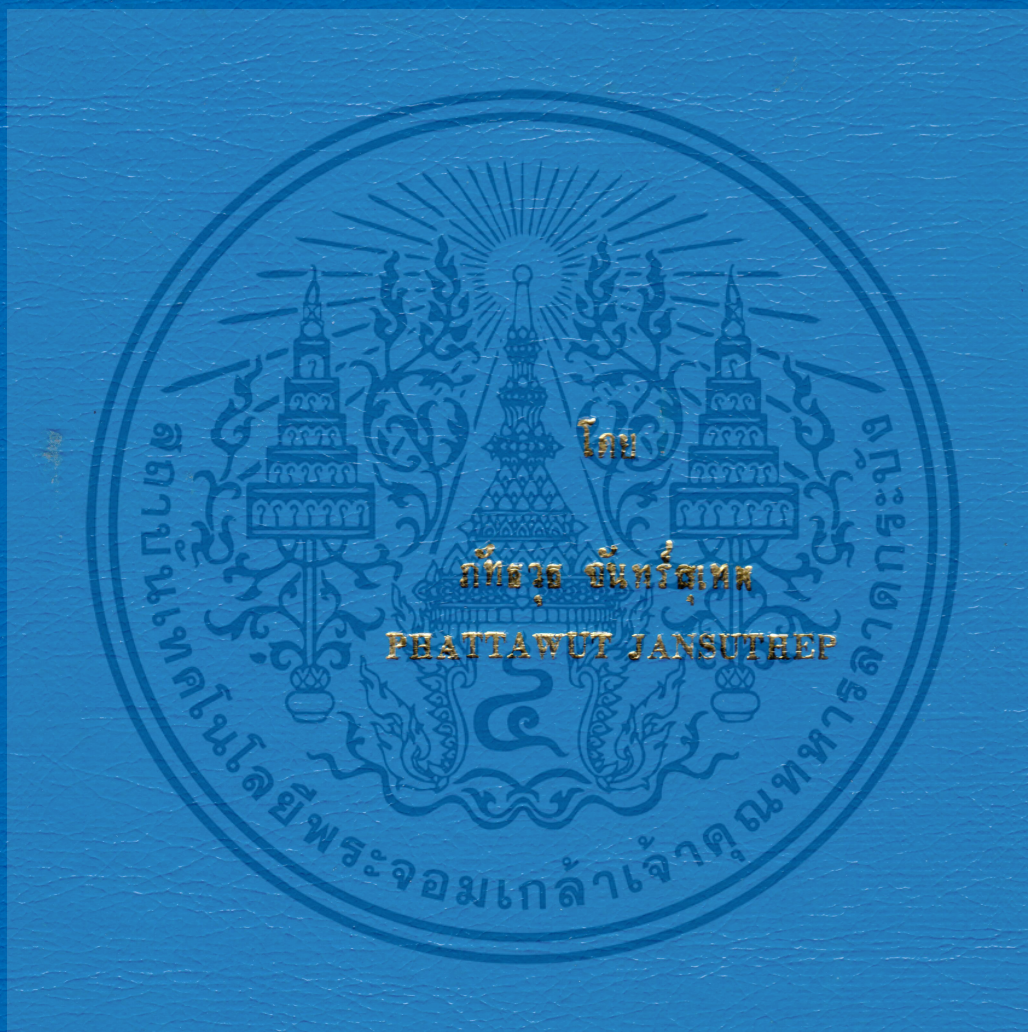


การให้ระบบบริหารจัดการเครือข่ายของซิสโก้ในการบริหารจัดการเครือข่าย
แลนและไวร์เลส

CISCO PRIME INFRASTRUCTURE NETWORK MANAGEMENT
LAN AND WIRELESS LAN



รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาดัชนี ๒
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ ๒ ปีการศึกษา ๒๕๕๘

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการศึกษา
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีความจำเป็นต้องใช้

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

การใช้ระบบบริหารจัดการเครือข่ายของซิสโก้ในการบริหารจัดการเครือข่าย
แลนและไร้สาย

CISCO PRIME INFRASTRUCTURE NETWORK MANAGEMENT
LAN AND WIRELESS LAN

โดย



ภัทรวุฑ จันทรสุเทพ

PHATTAWUT JANSUTHEP

อาจารย์ที่ปรึกษา

รศ.ดร.โชติพัชร ภรณ์ฉนวน



เลขหมู่..... 146527
เลขทะเบียน.....
วัน,เดือน,ปี. 23 มี.ค. 2560

b.....
i.....

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาระดับ 2
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับดูและใช้ศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

CISCO PRIME INFRASTRUCTURE NETWORK MANAGEMENT
LAN AND WIRELESS LAN

PHATTAWUT JANSUTHEP



A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS OF THE COURSE

INDEPENDENT STUDY 2

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อ 2/2015 เท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



COPYRIGHT 2016

FACULTY OF INFORMATION TECHNOLOGY

เอกสารนี้จัดทำขึ้นเพื่อใช้ในการเรียนการสอนในชั้นเรียนของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ใบรับรอง การศึกษาอิสระ 2 (Independent Study 2)

เรื่อง

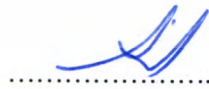
การใช้ระบบบริการจัดการเครือข่ายของซิสโก้ในการบริหารจัดการเครือข่าย
แลนและไร้สาย


**Cisco Prime Infrastructure Network Management
LAN and Wireless LAN**

**นายภักธุธ จันทรสุเทพ
รหัสประจำตัว 57606033**

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด
รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ
วิชาการศึกษาอิสระ 2 หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)
ภาคเรียนที่ 2 ปีการศึกษา 2558


.....อาจารย์ที่ปรึกษา
(รศ.ดร. โชติพัทธ์ ภรณ์วลัย)


.....กรรมการสอบ
(รศ.ดร. อาริต ธรรมโน)


.....กรรมการสอบ
(ผศ.ดร. ปานวิทย์ ชูวะนุติ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อ	การใช้ Cisco Prime Infrastructure ในการบริหารจัดการเครือข่ายแลนและไร้สาย
นักศึกษา	นายภัทรวิช จันทรสุเทพ
รหัสนักศึกษา	57606033
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีเครือข่ายและระบบ
ปีการศึกษา	2558
อาจารย์ที่ปรึกษา	รศ.ดร. โชติพัทธ์ ภรณ์วลัย

บทคัดย่อ

โครงการงานวิจัยนี้เป็นการศึกษาคุณลักษณะและคุณสมบัติของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) มีจุดมุ่งหมายเพื่อนำเอาซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้มาใช้บริหารจัดการอุปกรณ์เครือข่าย ที่ติดตั้งใช้งานในระบบเครือข่ายขององค์กร เพื่อช่วยให้ผู้ดูแลระบบเครือข่าย สามารถบริหารจัดการเครือข่ายจากศูนย์กลาง ลดความผิดพลาดและขั้นตอนการทำงาน เพิ่มความสะดวกและรวดเร็วในการทำงาน รวมถึงเพิ่มประสิทธิภาพในการดูแลและบริหารจัดการเครือข่ายขององค์กรได้ดีขึ้น เนื่องจากซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้สามารถให้การบริหารจัดการอุปกรณ์เครือข่ายของซิสโก้แบบต่างๆ ได้หลากหลาย เช่น สวิตช์ เราเตอร์ อุปกรณ์เครือข่ายไร้สาย และอุปกรณ์เครือข่ายอื่นๆ ของซิสโก้ รวมถึงมีความสามารถในการบริหารจัดการเครือข่าย เช่น Configuration management, Net-flow analyzer and Centralize management and monitor LAN and Wireless LAN เป็นต้น

จากการศึกษาและทดสอบพบว่า ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ มีคุณสมบัติที่ตรงต่อความต้องการของผู้ดูแลระบบเครือข่าย สามารถรองรับการใช้งานในการบริหารจัดการอุปกรณ์เครือข่ายของซิสโก้และครอบคลุมอุปกรณ์เครือข่ายของซิสโก้ที่ติดตั้งใช้งานในระบบเครือข่ายขององค์กร พร้อมทั้งมีเครื่องมือที่สามารถช่วยงานของผู้ดูแลระบบเครือข่าย ให้สามารถบริหารจัดการเครือข่ายได้อย่างมีประสิทธิภาพ แต่ก็มีข้อจำกัดคือ ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) สามารถรองรับการใช้งานและจะทำงานได้เต็มประสิทธิภาพเมื่อทำงานร่วมกับอุปกรณ์เครือข่ายของซิสโก้เท่านั้น

Title	Cisco Prime Infrastructure Network Management LAN and Wireless LAN
Student	Mr. Phattawut Jansuthep
Student ID.	57606033
Degree	Master of Science
Program	Information Technology
Major	Network and Systems Technology
Academic Year	2015
Advisor	Assoc. Dr. Chotipat Pornavalai

ABSTRACT

This Independent study is to study the features and specifications of the Cisco Prime Infrastructure network management software. The purpose of this study is to bring the software Cisco Prime Infrastructure was used to manage network devices are installed and deployment in corporate network system. To help network administrators to manage the network system from centralize reduce errors and workflow increase the availability speed of work and enhance management of the corporate network can be improved. The Cisco Prime Infrastructure network management software to provide managed network equipment for Cisco product different variety such as switch router wireless and other Cisco network equipment including the ability to manage network devices such a configuration management, Netflow analyzer and centralize management and monitor LAN and Wireless LAN system etc.

After a study and test the Cisco Prime Infrastructure network management software found that the features of Cisco Prime Infrastructure network management software meet the requirement of network administrators can be support and management of Cisco network equipment and comprehensive Cisco network equipment are installed in the corporate network and there are provide tools that can help the network administrator to manage the network effectively. But there are some limitations to consider the Cisco Prime Infrastructure network management software can be support and will work to its full potential when working with Cisco network equipment only.

กิตติกรรมประกาศ

รายงานการศึกษาค้นคว้าอย่างอิสระฉบับนี้จักสำเร็จมิได้ถ้าปราศจากความอนุเคราะห์ของบุคคลเหล่านี้

ข้าพเจ้าขอขอบพระคุณ รศ.ดร. โชติพัชร ภรณวลัย อาจารย์ที่ปรึกษา ที่ช่วยสนับสนุนแนวความคิด การแนะนำแนวทางในการดำเนินโครงการ องค์ความรู้ต่างๆ ช่วยให้คำปรึกษาและให้กำลังใจ รวมถึงตรวจสอบความถูกต้อง เพื่อให้รายงานการศึกษาค้นคว้าอย่างอิสระฉบับนี้มีความถูกต้องและสมบูรณ์ที่สุด

ข้าพเจ้าขอขอบพระคุณ คณาจารย์คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกท่าน ที่ได้ประสิทธิ์ประสาทวิชาความรู้ให้กับข้าพเจ้า และขอขอบคุณรุ่นพี่และเพื่อนร่วมรุ่นทุกคน ที่คอยช่วยเหลือและให้กำลังใจมาโดยตลอด

ข้าพเจ้าขอขอบพระคุณ บริษัทพานาโซนิค ประเทศไทย ผู้บริหารหน่วยงานไอทีและผู้บังคับบัญชาเป็นอย่างสูงที่ให้โอกาสในการดำเนินโครงการ ให้คำแนะนำและทำให้การดำเนินโครงการสำเร็จลุล่วงได้เป็นอย่างดี

สุดท้ายนี้ขอกราบขอบพระคุณ คุณแม่ชีวรัตน์ และครอบครัวของข้าพเจ้าที่เป็นเบื้องหลังของความสำเร็จในการศึกษารายงานฉบับนี้ ที่คอยให้ความช่วยเหลือ สนับสนุนและให้กำลังใจกันตลอดมา

ภัทธวูจ จันทรสุเทพ

สารบัญ

	หน้า
บทคัดย่อ	I
ABSTRACT	II
กิตติกรรมประกาศ	III
สารบัญ.....	IV
สารบัญตาราง.....	VI
สารบัญรูป.....	VII
บทที่ 1 บทนำ	
1.1 ความเป็นมาและความสำคัญของปัญหา.....	1
1.2 วัตถุประสงค์ในการศึกษา.....	2
1.3 ขอบเขตของการศึกษา.....	2
1.4 ขั้นตอนและแนวทางการศึกษาและพัฒนา.....	3
1.5 ประโยชน์ที่คาดว่าจะได้รับ.....	3
บทที่ 2 ทฤษฎีและระบบงานที่เกี่ยวข้อง	
2.1 ระบบบริหารจัดการเครือข่าย (Network Management System).....	5
2.2 โพรโทคอลบริหารจัดการเครือข่าย.....	12
2.3 สถาปัตยกรรมของระบบบริการจัดการเครือข่ายซิสโก้.....	21

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ(ต่อ)

หน้า

บทที่ 3 การดำเนินงาน

3.1 ประเภทของอุปกรณ์เครือข่ายที่ใช้ในการทดลอง	26
3.2 สภาพแวดล้อมที่ใช้ในการทดสอบ	26
3.3 แผนภาพแสดงการเชื่อมต่อระบบ	27
3.4 ขั้นตอนการดำเนินงาน	29

บทที่ 4 ผลการทดลอง

4.1 การจัดการความผิดพลาด (Fault Management)	40
4.2 การจัดการค่าที่ตั้งไว้ (Configuration Management).....	46
4.3 การจัดการบัญชีผู้ใช้เครือข่าย (Account Management).....	55
4.4 การจัดการประสิทธิภาพ (Performance Management)	62
4.5 การจัดการด้านความปลอดภัย (Security Management).....	69
4.6 ความสามารถในการบริหารจัดการเครือข่ายด้านอื่นๆ.....	73

บทที่ 5 บทสรุป

5.1 สรุปผลการทดลองและทดสอบระบบ	84
5.2 ปัญหาและข้อจำกัด	85
5.3 ข้อเสนอแนะและแนวทางการพัฒนาในอนาคต.....	85
บรรณานุกรม	87
ภาคผนวก.....	88
ประวัติผู้เขียน.....	98

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

ตารางที่	หน้า
2.1 แสดงการเปรียบเทียบการทำงานของโปรโตคอลเอสเอ็นเอ็มพีแต่ละรุ่น.....	16
2.2 ความต้องการใช้งานทรัพยากรขั้นต่ำในการติดตั้งบน Virtual	23
2.3 ความต้องการใช้งานทรัพยากรขั้นต่ำในการติดตั้งบน Physical	24
2.4 รายละเอียดแต่ละรุ่นของระบบบริการจัดการเครือข่ายซิสโก้	25



สารบัญรูป

รูปที่	หน้า
2.1 คุณสมบัติในแต่ละด้านของ FCAPS Model.....	6
2.2 รูปแบบตามลำดับชั้นของ FCAPS Model ในเครือข่ายซิสโก้	10
2.3 โครงสร้างของระบบบริหารจัดการเครือข่าย	11
2.4 โครงสร้างการทำงานของโปรโตคอลเอสเอ็นเอ็มพี(SNMP)	13
2.5 การทำงาน Get Request	13
2.6 การทำงาน Get Next Request	14
2.7 การทำงาน Set Request.....	15
2.8 การทำงานของ SNMP Trap.....	16
2.9 โครงสร้างของเอสเอ็นเอ็มพีแมสเซจ (SNMP Message).....	17
2.10 รายละเอียดโครงสร้างของเอสเอ็นเอ็มพีแมสเซจ (SNMP Message)	17
2.11 โครงสร้างของ Structure of Management Information หรือ (SMI)	18
2.12 การเรียกดูโครงสร้างของ MIBs Tree ผ่านโปรแกรม.....	19
2.13 โครงสร้างของ MIB-2.....	21
2.14 ภาพรวมของระบบบริการจัดการเครือข่ายซิสโก้.....	22
3.1 แผนภาพแสดงการเชื่อมต่อระบบระบบเครือข่าย	27
3.2 แสดงเครือข่ายสวิตช์.....	28
3.3 แสดงเครือข่ายไร้สาย	28
3.4 แสดงเครือข่ายเราเตอร์	29
3.5 แสดงหน้าจอ Login เข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้.....	29
3.6 แสดงหน้าจอภาพรวมของระบบบริหารจัดการเครือข่ายของซิสโก้.....	30
3.7 แสดงหน้าจอตัวเลือกหลักของระบบบริหารจัดการเครือข่ายของซิสโก้.....	30
3.8 แสดงหน้าจอตัวเลือก Dashboard ของระบบบริหารจัดการเครือข่ายของซิสโก้.....	31
3.9 แสดงหน้าจอตัวเลือก Monitor ของระบบบริหารจัดการเครือข่ายของซิสโก้.....	31

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญญรูป(ต่อ)

รูปที่	หน้า
3.10 แสดงหน้าจอตัวเลือก Configuration ของระบบบริหารจัดการเครือข่ายของซิสโก้	32
3.11 แสดงหน้าจอตัวเลือก Inventory ของระบบบริหารจัดการเครือข่ายของซิสโก้	32
3.12 แสดงหน้าจอตัวเลือก Maps ของระบบบริหารจัดการเครือข่ายของซิสโก้	33
3.13 แสดงหน้าจอตัวเลือก Services ของระบบบริหารจัดการเครือข่ายของซิสโก้	33
3.14 แสดงหน้าจอตัวเลือก Reports ของระบบบริหารจัดการเครือข่ายของซิสโก้	34
3.15 แสดงหน้าจอตัวเลือก Administration ของระบบบริหารจัดการเครือข่ายของซิสโก้.....	34
3.16 การเพิ่มอุปกรณ์เครือข่ายเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้แบบทีละตัว.....	35
3.17 แสดงการค้นหาอุปกรณ์เครือข่ายของระบบบริหารจัดการเครือข่ายของซิสโก้.....	36
3.18 การตั้งค่าค้นหาและเพิ่มอุปกรณ์เครือข่าย	37
3.19 แสดงผลการค้นหาและเพิ่มอุปกรณ์เครือข่ายตามกำหนดเวลา.....	37
3.20 แสดงรายการจำนวนอุปกรณ์เครือข่าย	38
3.21 แสดงจำนวน License อุปกรณ์เครือข่ายของระบบบริหารจัดการเครือข่ายของซิสโก้	39
4.1 แสดงหน้าจอภาพรวมของระบบเครือข่าย.....	41
4.2 แสดงหน้าจอสถานะของอุปกรณ์เครือข่ายที่เกิดปัญหา	42
4.3 แสดงหน้าจอสถานะตามชนิดของอุปกรณ์เครือข่าย.....	42
4.4 แสดงรายละเอียดของปัญหาที่เกิดขึ้นกับอุปกรณ์เครือข่าย	43
4.5 แสดงลำดับเหตุการณ์ที่เกิดขึ้นกับอุปกรณ์เครือข่าย.....	43
4.6 แสดงชนิดของอุปกรณ์เครือข่ายที่ต้องการแจ้งเตือน	45
4.7 แสดงหน้าจอการเลือกระดับความสำคัญเพื่อแจ้งเตือนผ่านอีเมล.....	45
4.8 แสดงภาพตัวอย่างอีเมลการแจ้งเตือน	46
4.9 เลือกอุปกรณ์เครือข่ายที่ต้องการปรับเปลี่ยนค่า.....	47
4.10 เลือกอินเตอร์เฟซที่ต้องการจะเปลี่ยนแปลงค่าที่ตั้งไว้.....	48
4.11 แสดงข้อมูลที่ต้องการจะเปลี่ยนแปลงค่าที่ตั้งไว้.....	48

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อ **VI** ศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญญรูป(ต่อ)

รูปที่	หน้า
4.12 การสร้างรูปแบบคำสั่งเพื่อเพิ่มกับให้อุปกรณ์เครือข่าย.....	49
4.13 แสดงลำดับการส่งรูปแบบคำสั่งเพื่อเพิ่มกับให้อุปกรณ์เครือข่าย.....	50
4.14 แสดงการจัดเก็บค่าที่ตั้งไว้ทุกๆเดือน.....	51
4.15 แสดงข้อมูลที่ต้องการจะเปลี่ยนแปลงค่าที่ตั้งไว้.....	52
4.16 การเปรียบเทียบค่าที่ตั้งไว้.....	53
4.17 การเปรียบเทียบค่าที่ตั้งไว้ของเดิมกับปัจจุบัน.....	54
4.18 นำข้อมูลค่าที่ตั้งไว้ออกจากระบบบริหารจัดการเครือข่ายของซิสโก้.....	54
4.19 แสดงปริมาณการยืนยันตัวตนที่ใช้งานระบบเครือข่าย.....	56
4.20 แสดงแผนภูมิปริมาณโปรโตคอล 802.1X.....	56
4.21 แสดงรายละเอียดของผู้ใช้งานบนโปรโตคอล 802.1X.....	57
4.22 แสดงรายละเอียดเชิงลึกของผู้ใช้งานบนเครือข่าย.....	58
4.23 แสดงเครื่องมือที่ช่วยบริหารจัดการผู้ใช้งานบนเครือข่าย.....	58
4.24 แสดงแอปพลิเคชันที่มีการใช้งานบนอุปกรณ์เครือข่าย.....	60
4.25 แสดงอุปกรณ์ที่มีการใช้ทรัพยากรระบบเพื่อสนับสนุนการทำงานของแอปพลิเคชัน.....	61
4.26 แสดงเครื่องลูกข่ายที่มีเข้าใช้งานมากสุดบนเครือข่าย.....	61
4.27 แสดงเครื่องแม่ข่ายที่ถูกเข้าใช้งานมากสุดบนเครือข่าย.....	62
4.28 แสดงการวัดประสิทธิภาพบนอินเทอร์เน็ตเฟสของอุปกรณ์เครือข่าย.....	63
4.29 แสดงอินเทอร์เน็ตเฟสของอุปกรณ์เครือข่ายที่มีการใช้งานมาก.....	63
4.30 แสดงการละทิ้งแพคเกจและอัตราความผิดพลาดในการรับ-ส่งข้อมูล.....	64
4.31 แสดงรายการอุปกรณ์เครือข่ายที่มีการใช้งานหน่วยประมวลผลสูง.....	64
4.32 แสดงรายการอุปกรณ์เครือข่ายที่มีการใช้งานหน่วยความจำสูง.....	65
4.33 แสดงการใช้งานหน่วยประมวลผลของอุปกรณ์เครือข่ายตามช่วงเวลา.....	65
4.34 แสดงการใช้งานหน่วยความจำของอุปกรณ์เครือข่ายตามช่วงเวลา.....	66

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป(ต่อ)

รูปที่	หน้า
4.35 แสดงค่าอุณหภูมิของอุปกรณ์เครือข่ายที่มีแนวโน้มค่อนข้างสูง	66
4.36 แสดงรายละเอียดอุปกรณ์เครือข่ายสวิตช์ของซิสโก้	67
4.37 แสดงข้อมูลรายละเอียดอุปกรณ์เครือข่ายสวิตช์ของซิสโก้.....	68
4.38 แสดงรายละเอียดอุปกรณ์เครือข่ายไร้สายของซิสโก้	68
4.39 แสดงแผนภาพการทำงานร่วมกับซอฟต์แวร์ด้านความปลอดภัยของทางซิสโก้	69
4.40 แสดงแผนภูมิการเชื่อมต่อระหว่างผู้ใช้งานกับอุปกรณ์เครือข่ายไร้สาย	70
4.41 แสดงปริมาณผู้ใช้งานที่มีการยืนยันตัวตนเข้าสู่เครือข่าย	71
4.42 แสดงการจัดประเภทตามชนิดของการยืนยันตัวตนเข้าสู่เครือข่าย	71
4.43 แสดงภาพรวมเหตุการณ์ด้านความปลอดภัยที่เกิดขึ้นตามช่วงเวลา.....	72
4.44 แสดงเหตุการณ์ด้านความปลอดภัยที่เกิดขึ้นบนอุปกรณ์เครือข่าย	72
4.45 แสดงค่าการติดตั้งใช้งานที่อาจส่งผลให้เกิดความผิดพลาดด้านความปลอดภัย	73
4.46 การออกแบบจำลองเครือข่ายไร้สายจากพื้นที่ใช้งานจริง	74
4.47 การกำหนดชนิดของผนังหรือสิ่งกีดขวางสัญญาณวิทยุตามพื้นที่ใช้งานจริง.....	75
4.48 การกำหนดชนิดของตัวส่งสัญญาณวิทยุตามพื้นที่ใช้งานจริง	75
4.49 การกำหนดชนิดของเสาส่งสัญญาณวิทยุตามพื้นที่ใช้งานจริง	76
4.50 แสดงแบบจำลองการกระจายสัญญาณวิทยุตามพื้นที่ใช้งานจริง.....	76
4.51 แสดงการติดตั้งใช้งานอุปกรณ์เครือข่ายไร้สายในแต่ละพื้นที่.....	77
4.52 แสดงการใช้งานบนอุปกรณ์เครือข่ายไร้สายในแต่ละพื้นที่	77
4.53 แสดงภาพรวมในการเชื่อมต่ออุปกรณ์ต่างๆในระบบเครือข่าย	78
4.54 แสดงการเชื่อมต่อตามกลุ่มพื้นที่ที่ติดตั้งใช้งานของอุปกรณ์เครือข่าย.....	79
4.55 แสดงการเชื่อมต่อของอุปกรณ์เครือข่ายที่ใช้โปรโตคอล CDP	79
4.56 แสดงรูปแบบรายงานที่ใช้จัดทำรายงานในระบบบริหารจัดการเครือข่ายของซิสโก้	81
4.57 แสดงการสร้างรายงานให้กับผู้ดูแลระบบอัตโนมัติตามเวลาที่กำหนด	82

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป(ต่อ)

รูปที่	หน้า
4.58 แสดงสถานะการสร้างรายงานอัตโนมัติตามที่คุณเลือกระบบกำหนด.....	82
4.59 แสดงรูปแบบรายงานของระบบบริหารจัดการเครือข่ายของซิสโก้.....	83
4.60 แสดงรายละเอียดของข้อมูลในรายงาน	83



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

จากการเติบโตของธุรกิจและการพัฒนาของเทคโนโลยีสารสนเทศในปัจจุบันที่เป็นไปอย่างรวดเร็ว ทำให้ระบบเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตได้เข้ามามีบทบาทและเป็นพื้นฐานที่สำคัญในการดำเนินงานของระบบเทคโนโลยีสารสนเทศในองค์กร จากความต้องการในการใช้งานระบบเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตในองค์กรที่มีเพิ่มมากขึ้น ส่งผลทำให้จำนวนอุปกรณ์เครือข่ายและการเชื่อมต่อระหว่างอุปกรณ์เครือข่ายมีจำนวนมากขึ้น ซับซ้อนขึ้น ทำให้ระบบเครือข่ายภายในองค์กรมีการขยายตัวเพิ่มขึ้นอย่างต่อเนื่อง จากเหตุผลดังกล่าว ส่งผลทำให้ผู้ดูแลระบบต้องรับภาระและมึ่งานในการดูแลและบริหารจัดการเครือข่ายที่เพิ่มมากขึ้นตามไปด้วย

จากผลที่เกิดขึ้นและปัญหาที่พบในองค์กร คือ เมื่อระบบเครือข่ายมีจำนวนอุปกรณ์เครือข่ายเพิ่มมากขึ้นและระบบเครือข่ายในองค์กรมีความซับซ้อนขึ้น จะทำให้ประสิทธิภาพในการบริหารจัดการระบบเครือข่ายลดลง การจะบริหารจัดการอุปกรณ์เครือข่ายที่มีจำนวนมากให้ทั่วถึงนั้น ทำได้ยากและใช้เวลานาน แต่ด้วยเป้าหมาย หน้าที่และความรับผิดชอบที่สำคัญในการบริหารจัดการเครือข่ายขององค์กรของผู้ดูแลระบบ คือ การทำให้ระบบเครือข่ายในองค์กรสามารถให้บริการได้อย่างต่อเนื่อง มีคุณภาพและเกิดประสิทธิภาพสูงสุดให้กับผู้ใช้งานบนระบบเครือข่าย จึงมีความจำเป็นและต้องการที่จะต้องจัดการระบบหรือเครื่องมือที่มาช่วยบริหารจัดการเครือข่ายในองค์กร โดยระบบหรือเครื่องมือนั้นจะต้องสามารถบริหารจัดการเครือข่ายได้จากศูนย์กลาง รองรับปริมาณของอุปกรณ์เครือข่ายที่มีจำนวนมาก รองรับการขยายตัวของระบบเครือข่ายและเทคโนโลยีใหม่ๆ ในอนาคตได้ ช่วยอำนวยความสะดวกและรวดเร็วในการทำงานให้กับผู้ดูแลระบบ รวมถึงสามารถรวบรวมสถานะข้อมูลของอุปกรณ์เครือข่ายและการใช้งานสื่อสารข้อมูลบนระบบเครือข่ายในรูปแบบต่างๆ และนำมาแสดงผล จัดทำรายงาน ให้กับผู้ดูแลระบบ ทำให้ผู้ดูแลระบบสามารถนำข้อมูลเหล่านั้น ไปวิเคราะห์และสามารถเพิ่มประสิทธิภาพการทำงานของระบบเครือข่าย ทำให้ระบบเครือข่ายสามารถให้บริการได้ต่อเนื่องตลอดเวลา หรือถ้ามีความผิดพลาดที่เกิดขึ้นในระบบเครือข่าย ก็สามารถแจ้งเตือนให้ผู้ดูแลระบบรับทราบและสามารถแก้ไขปัญหาของระบบเครือข่ายที่เกิดขึ้นได้อย่างรวดเร็ว รวมทั้งนำข้อมูลที่ได้มาใช้ในการวางแผน เตรียมการป้องกัน รวมถึงมีแผนรองรับการเติบโตของระบบเครือข่ายขององค์กรในอนาคตได้ โดยผู้ดูแลระบบได้กำหนดความต้องการที่ระบบบริหารจัดการเครือข่ายจะต้องสามารถทำได้ไว้ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- 1.1.1 การจัดการความผิดพลาด (Fault Management)
- 1.1.2 การจัดการค่าที่ตั้งไว้ (Configuration Management)
- 1.1.3 การจัดการบัญชีผู้ใช้เครือข่าย (Account Management)
- 1.1.4 การจัดการประสิทธิภาพ (Performance Management)
- 1.1.5 การจัดการความมั่นคงปลอดภัย (Security Management)

เนื่องจากอุปกรณ์เครือข่ายที่ติดตั้งและใช้งานในองค์กรที่เป็นเครือข่ายที่ใช้สาย เครือข่ายการเชื่อมต่อระหว่างสำนักงานใหญ่ไปที่สาขาต่างๆ และเครือข่ายไร้สาย เกือบทั้งหมดเป็นของบริษัทซิสโก้ ผู้จัดทำโครงการจึงมีความประสงค์ที่จะทำการศึกษา ทดลอง และทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) เพื่อนำข้อมูลที่ได้จากการศึกษามาใช้ในการตัดสินใจและเลือกใช้ระบบบริหารจัดการเครือข่ายภายในองค์กรต่อไป

1.2 วัตถุประสงค์ในการศึกษา

- 1.2.1 เพื่อศึกษาคุณสมบัติและการใช้งานซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure)
- 1.2.2 เพื่อทดลองและทดสอบการใช้งานซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) กับอุปกรณ์เครือข่ายที่ติดตั้งและใช้งานใช้ในองค์กร
- 1.2.3 เพื่อนำข้อมูลที่ได้มาใช้ในการตัดสินใจและเลือกใช้ระบบบริหารจัดการเครือข่ายภายในองค์กรต่อไป

1.3 ขอบเขตของการศึกษา

ทำการศึกษา ทดลอง และทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) โดยมีขอบเขตดังนี้

- 1.3.1 ทำการศึกษาคู่มือและความสามารถในการบริหารจัดการเครือข่ายของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure)
- 1.3.2 ทำการติดตั้งและศึกษาวิธีการใช้งานซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure)
- 1.3.3 ทำการทดลองใช้งานและทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) กับอุปกรณ์เครือข่ายที่ติดตั้งและใช้งานในองค์กร
- 1.3.4 รวบรวมข้อมูลและผลลัพธ์ที่ได้นำมาสรุป เพื่อนำมาใช้ในการตัดสินใจและเลือกใช้ระบบบริหารจัดการเครือข่ายภายในองค์กรต่อไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.4 ขั้นตอนและแนวทางการศึกษาและพัฒนา

การศึกษา ทดลอง และทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) โดยมีขั้นตอนและแนวทางการศึกษาและพัฒนากระบวนการดังนี้

- 1.4.1 รวบรวมปัญหาที่เกิดขึ้นและความต้องการในการบริหารจัดการเครือข่ายในองค์กร
- 1.4.2 จัดทำรายการของอุปกรณ์เครือข่ายของซิสโก้ที่ติดตั้งใช้งานในองค์กรและทำการคัดเลือกอุปกรณ์เครือข่ายที่จะนำไปใช้การศึกษา ทดลอง และทดสอบกับซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure)
- 1.4.3 ทำการติดตั้งซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) และเชื่อมต่อเข้ากับระบบเครือข่ายภายในองค์กร
- 1.4.4 ทำการทดลองใช้งานซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) กับอุปกรณ์เครือข่ายที่ติดตั้งและใช้งานในองค์กร
- 1.4.5 ทำการทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) และทดลองใช้บริหารจัดการอุปกรณ์เครือข่ายภายในองค์กรดังนี้
 - 1) การตรวจสอบและจัดการความผิดพลาดของอุปกรณ์เครือข่ายจากศูนย์กลาง
 - 2) การบริหารจัดการค่าที่ตั้งไว้ การเก็บสำรองและเรียกคืนค่าที่ตั้งไว้กับอุปกรณ์เครือข่าย
 - 3) การตรวจสอบและจัดการประสิทธิภาพของอุปกรณ์เครือข่าย
 - 4) การตรวจสอบและจัดการความมั่นคงปลอดภัยของอุปกรณ์เครือข่าย
- 1.4.6 สรุปผลการทดลองและข้อเสนอแนะ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าจะได้รับจากการศึกษา ทดลอง และทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) มีดังนี้

- 1.5.1 ได้ทดลองและทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) ว่าเป็นเครื่องมือที่มีคุณสมบัติเหมาะสมหรือไม่ ก่อนที่จะตัดสินใจเลือกซื้อและเลือกนำมาใช้ช่วยงานผู้ดูแลระบบและเพิ่มประสิทธิภาพในการบริหารจัดการระบบเครือข่ายภายในองค์กร
- 1.5.2 สามารถนำข้อมูลและผลลัพธ์ที่ได้นำมาสรุป เพื่อนำมาใช้ในการตัดสินใจและเลือกใช้

เอกสารนี้เป็นระบบบริหารจัดการเครือข่ายภายในองค์กรต่อไป ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- 1.5.3 เพื่อหาเครื่องมือที่ช่วยลดภาระในการทำงานของผู้ดูแลระบบเครือข่าย สามารถทำให้การทำงานสะดวกและรวดเร็วขึ้น
- 1.5.4 เพื่อช่วยลดค่าใช้จ่ายให้กับองค์กร ในการจ้างบุคคลากรผู้ดูแลระบบเครือข่ายในแผนกเพิ่ม
- 1.5.5 เพื่อช่วยในการบริหารจัดการเครือข่ายภายในองค์กรให้มีประสิทธิภาพ สามารถวางแผนและป้องกันปัญหาที่จะเกิดขึ้น ทำให้การทำงานของระบบเครือข่ายเป็นไปอย่างต่อเนื่อง



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2

ทฤษฎีและระบบงานที่เกี่ยวข้อง

การจัดทำโครงการฉบับนี้มีวัตถุประสงค์ เพื่อศึกษาและทดสอบคุณสมบัติของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายซิสโก้ (Cisco Prime Infrastructure) ดังนั้นเพื่อให้เกิดองค์ความรู้ในการศึกษาและทดสอบคุณสมบัติของซอฟต์แวร์ดังกล่าว ผู้จัดทำจึงได้ศึกษาทฤษฎีและเทคโนโลยีที่เกี่ยวข้องโดยครอบคลุมหัวข้อต่างๆ ดังนี้

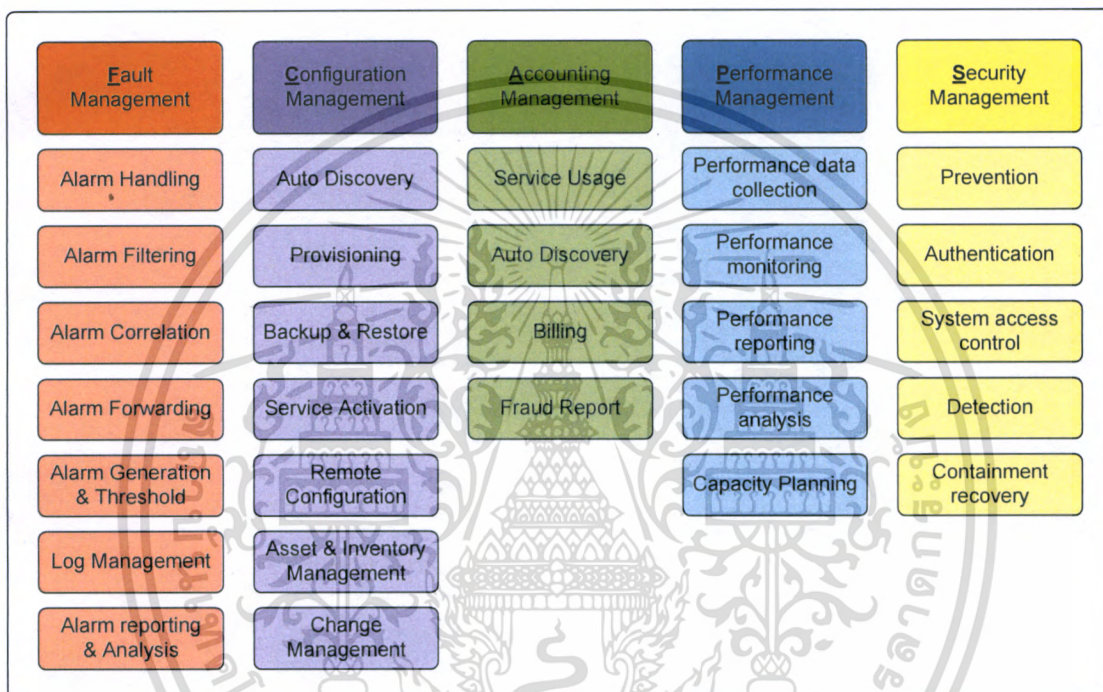
- 2.1 ระบบบริหารจัดการเครือข่าย
- 2.2 โพรโตคอลบริหารจัดการเครือข่าย
- 2.3 สถาปัตยกรรมของระบบบริหารจัดการเครือข่ายซิสโก้ (Cisco Prime Infrastructure)

2.1 ระบบบริหารจัดการเครือข่าย (Network Management System)

ระบบบริหารจัดการเครือข่าย คือ ระบบที่ทำหน้าที่เป็นศูนย์กลางการควบคุม ดูแล บริหารจัดการและตรวจสอบสถานะอุปกรณ์ในเครือข่ายได้ตลอดเวลา ทำให้ผู้ดูแลระบบมีความมั่นใจว่าระบบเครือข่ายสามารถทำงานได้อย่างต่อเนื่องและเต็มประสิทธิภาพ พร้อมทั้งมีเครื่องมือที่สามารถช่วยงานผู้ดูแลระบบในด้านต่างๆ เพื่อให้สามารถบริหารจัดการเครือข่ายจากศูนย์กลางได้ ตัวระบบต้องมีการใช้งานที่ง่าย สะดวกรวดเร็วและครอบคลุมทั้งอุปกรณ์ในระบบเครือข่าย มีระบบแจ้งเตือนให้ผู้ดูแลระบบรับทราบ เมื่อมีส่วนหนึ่งส่วนใดของระบบเครือข่ายเกิดการดำเนินงานที่ผิดพลาด หรือเกิดข้อขัดข้องขึ้นจากฮาร์ดแวร์หรือซอฟต์แวร์ ทำให้ผู้ดูแลระบบสามารถเข้าไปตรวจสอบและทำการแก้ไขได้อย่างรวดเร็ว โดยการทำงานของระบบบริหารจัดการเครือข่ายนั้นจะต้องทำการเก็บรวบรวมข้อมูลของอุปกรณ์เครือข่าย เช่น สถานะของอุปกรณ์ ปริมาณการรับ-ส่งข้อมูล ปริมาณผู้ใช้ที่มีอยู่ในระบบเครือข่ายและนำมาแสดงผลไว้ เพื่อให้ผู้ดูแลระบบสามารถนำข้อมูลนั้นมาวิเคราะห์และตัดสินใจ เพื่อใช้ในการวางแผน ป้องกันและแก้ปัญหาในระบบเครือข่ายได้อย่างมีประสิทธิภาพ จากแนวคิดและความต้องการในการบริหารจัดการเครือข่าย จึงได้มีการจัดตั้งเป็นมาตรฐานของระบบบริหารจัดการเครือข่ายขึ้นมา โดยกลุ่ม International Organization for Standards Network Management (OSI) ของสถาบัน International Organization for Standardization (ISO) ได้จัดทำรูปแบบเพื่อแบ่งหน้าที่ของระบบบริหารเครือข่ายที่ใช้ชื่อว่า FCAPS Model ดังรูปที่ 2.1 [1] ซึ่ง FCAPS มาจากอักษรตัวหน้าของหัวข้อการทำงานในระบบบริหารเครือข่าย โดยหน้าที่การทำงานของระบบบริหารเครือข่าย สามารถแบ่งออกเป็นส่วนต่าง ๆ ได้ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1. การจัดการความผิดพลาด (Fault Management)
2. การจัดการค่าที่ตั้งไว้ (Configuration Management)
3. การจัดการบัญชีผู้ใช้เครือข่าย (Account Management)
4. การจัดการประสิทธิภาพ (Performance Management)
5. การจัดการความมั่นคงปลอดภัย (Security Management)



รูปที่ 2.1 คุณสมบัติในแต่ละด้านของ FCAPS Model

2.1.1 การจัดการความผิดพลาด (Fault Management)

ระบบเครือข่ายที่ดีจะต้องอยู่ในสภาพพร้อมใช้งานตลอดเวลา (Availability) เมื่อระบบเกิดปัญหาหรือความผิดพลาดขึ้น จะอาจส่งผลทำให้เครือข่ายหยุดการให้บริการ หรือให้การบริการไม่ต่อเนื่องและไม่เต็มประสิทธิภาพ ซึ่งส่งผลต่อความน่าเชื่อถือของระบบเครือข่าย ดังนั้นผู้ดูแลระบบจะต้องมีวิธีการป้องกันและบริหารจัดการความผิดพลาดที่เกิดขึ้นในระบบเครือข่ายให้มีประสิทธิภาพ เพื่อตอบสนองความต้องการของผู้ใช้ และสร้างความน่าเชื่อถือให้กับระบบเครือข่าย ระบบบริหารจัดการเครือข่ายที่ดีจะต้องมีเครื่องมือที่คอยดูแล ตรวจสอบ เฝ้าระวังและเก็บรวบรวมข้อมูลความผิดพลาดที่เกิดขึ้นในระบบเครือข่ายได้อย่างมีประสิทธิภาพ เพื่อให้ผู้ดูแลระบบสามารถนำข้อมูลเหล่านั้นมาใช้วิเคราะห์และตัดสินใจ ในการแก้ปัญหาได้อย่างรวดเร็วที่สุด รวมถึงนำมาเอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่นอนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประเมินความเสี่ยงและหาวิธีการป้องกันปัญหาที่จะขึ้นในอนาคต การจัดการความผิดพลาด มีขั้นตอนการดำเนินงานดังนี้

2.1.1.1 การตรวจสอบและระบุความผิดพลาดภายในเครือข่าย มี 2 วิธี คือ

1. การตรวจจับเหตุการณ์ที่เกิดขึ้น – เป็นการกำหนดให้อุปกรณ์เครือข่ายเป็นผู้ส่งข้อมูลความผิดพลาดมายังระบบบริหารจัดการเครือข่าย เมื่อมีความผิดพลาดเกิดขึ้นในอุปกรณ์เครือข่ายนั้น เช่น การเชื่อมต่อล้มเหลว, อุปกรณ์มีการเริ่มต้นการทำงานใหม่, ฮาร์ดแวร์หรือซอฟต์แวร์เกิดการดำเนินงานที่ผิดพลาดขึ้น แต่วิธีนี้มีข้อจำกัดคือ ในกรณีที่การทำงานของระบบโดยรวมล้มเหลวทั้งระบบ ทำให้อุปกรณ์เครือข่ายในระบบไม่สามารถส่งสัญญาณติดต่อกับระบบบริหารจัดการเครือข่ายได้ จะทำให้ระบบบริหารจัดการเครือข่ายไม่สามารถทำการตรวจจับและเก็บข้อมูลความผิดพลาดจากเหตุการณ์ที่เกิดขึ้นได้

2. การส่งข้อความสอบถาม (Polling) – ระบบบริหารจัดการเครือข่ายจะทำการส่งสัญญาณผ่านโปรโตคอลทางค่านเครือข่าย ออกไปสอบถามสถานะของอุปกรณ์เครือข่ายตามช่วงเวลาที่กำหนด วิธีนี้ช่วยให้ระบบจัดการเครือข่ายสามารถตรวจสอบสถานะและหาความผิดพลาดในอุปกรณ์เครือข่ายได้ แต่สิ่งที่จะต้องคำนึงคือ การกำหนดช่วงเวลาในการส่งสัญญาณออกไปสอบถาม เพราะถ้าส่งในช่วงเวลาที่บ่อยครั้งและเร็วเกินไปจะทำให้ปริมาณข้อมูลในระบบเครือข่ายเพิ่มมากขึ้น

2.1.1.2 หลังจากระบบตรวจสอบพบความผิดพลาดแล้ว ระบบบริหารจัดการเครือข่ายจะต้องนำข้อมูลที่เก็บรวบรวมได้ มาแยกจัดประเภทและระดับความสำคัญของปัญหา เพื่อให้ผู้ดูแลเครือข่ายสามารถนำข้อมูลที่ได้ ไปวิเคราะห์และระบุสาเหตุของปัญหาที่แท้จริง ทำให้สามารถดำเนินการแก้ไขได้รวดเร็วและมีประสิทธิภาพ

2.1.1.3 ทำการแจ้งเตือนไปยังผู้ดูแลเครือข่ายหรือผู้เกี่ยวข้องให้ทราบเมื่ออุปกรณ์เครือข่ายหรือระบบเกิดความผิดพลาดขึ้น เช่น การส่งอีเมล การแสดงสถานะหรือข้อความเตือนที่หน้าจอคอมพิวเตอร์ และการส่งข้อความทางมือถือ เป็นต้น

2.1.2 การจัดการค่าที่ตั้งไว้ (Configuration Management)

ค่าการติดตั้งบนอุปกรณ์เครือข่าย เป็นข้อมูลที่สำคัญที่ผู้ดูแลเครือข่ายต้องมีเก็บรักษาและสำรองไว้ เพื่อความสะดวกในการปรับแต่ง เปลี่ยนแปลงค่าการทำงานของอุปกรณ์เครือข่าย ให้ถูกต้องเหมาะสม สอดคล้องกับหน้าที่ของแต่ละอุปกรณ์ในระบบเครือข่าย หรือมีไว้เพื่อกู้คืนค่าการติดตั้ง เมื่อมีการเปลี่ยนอุปกรณ์ใหม่ กู้คืนทั้งระบบเครือข่ายเมื่อระบบเกิดปัญหาขึ้น โดยระบบบริหารจัดการเครือข่ายจะต้องมีเครื่องมือที่ช่วยผู้ดูแลเครือข่ายสามารถจัดเก็บและกู้คืนค่าการติดตั้งให้กับอุปกรณ์เครือข่าย ได้สะดวกรวดเร็ว ระบบควรจะสามารถทำการจัดเก็บค่าที่ตั้งไว้ได้เองตามช่วงของวัน เวลาที่ทางผู้ดูแลเครือข่ายได้กำหนดไว้ รวมถึงสามารถเข้าถึงอุปกรณ์จากระยะไกล

(Remote Access) เพื่อให้สามารถบริหารจัดการค่าที่ตั้งไว้จากศูนย์กลางและครอบคลุมทุกอุปกรณ์ในระบบเครือข่าย

2.1.2.1 การรวบรวมข้อมูลค่าที่ตั้งไว้ในระบบเครือข่าย มีลักษณะการดำเนินงาน 2 รูปแบบ

1. การรวบรวมข้อมูลค่าที่ตั้งไว้แบบทำเอง โดยผู้ดูแลเครือข่ายเป็นผู้ดำเนินการเอง อาจเป็นการเข้าไปเชื่อมต่อโดยตรงหรือเข้าถึงอุปกรณ์จากระยะไกลและทำการเก็บข้อมูลการติดตั้งจากอุปกรณ์ที่ละตัว แล้วบันทึกในรูปแบบไฟล์ข้อมูลการติดตั้งไว้ในคอมพิวเตอร์ แต่วิธีนี้มีข้อเสีย คือ ถ้าในระบบเครือข่ายมีจำนวนอุปกรณ์เครือข่ายในปริมาณมาก จะทำให้ผู้ดูแลเครือข่ายใช้เวลาในการดำเนินงานมากและอาจเกิดความผิดพลาดขึ้นได้ง่าย

2. การรวบรวมข้อมูลแบบอัตโนมัติ โดยการให้ระบบบริหารจัดการเครือข่ายใช้โปรโตคอลการจัดการเครือข่าย ทำการรวบรวมข้อมูลและเก็บบันทึกไฟล์ข้อมูลการติดตั้งของอุปกรณ์เครือข่ายจากศูนย์กลางโดยอัตโนมัติ ตามช่วงวันและเวลาที่ผู้ดูแลเครือข่ายเป็นผู้กำหนด ซึ่งสามารถช่วยลดงานให้กับผู้ดูแลเครือข่ายได้อีกด้วย

2.1.2.2 การปรับแต่งค่าของอุปกรณ์ ระบบจัดการเครือข่ายจะสามารถช่วยอำนวยความสะดวกในการทำงานของผู้ดูแลระบบ เช่น การเรียกดูข้อมูลค่าปรับแต่งเดิมของอุปกรณ์ที่กำลังทำงานอยู่ เพื่อเปรียบเทียบข้อมูลการติดตั้งใช้งานอยู่และกับข้อมูลการติดตั้งที่จะทำการแก้ไขปรับปรุง ช่วยลดความผิดพลาดและสามารถปรับแต่งข้อมูลการติดตั้งให้กับอุปกรณ์เครือข่ายได้อย่างมีประสิทธิภาพ

2.1.2.3 การสั่งบันทึกค่าการปรับแต่งที่เปลี่ยนแปลงแล้วลงในอุปกรณ์เครือข่ายพร้อมทั้งทำรายงานการบันทึกการเปลี่ยนแปลง โดยข้อมูลจะถูกเก็บบันทึกลงในระบบฐานข้อมูล เพื่อให้ผู้ดูแลสามารถนำมาเรียกดูได้ภายหลัง ทำให้ทราบถึงการเปลี่ยนแปลงของข้อมูลการติดตั้งตามลำดับ รวมถึงสามารถตรวจสอบจุดที่ทำการแก้ไขที่เกิดขึ้นได้อีกด้วย

2.1.3 การจัดการบัญชีผู้ใช้เครือข่าย (Account Management)

ระบบบริหารจัดการเครือข่ายต้องสามารถเก็บรวบรวมข้อมูล ที่เกี่ยวกับการใช้งาน โดยแยกรายละเอียดเป็นกลุ่มของผู้ใช้หรือรายบุคคล เพื่อนำไปใช้ประโยชน์ เช่น การจัดสรรทรัพยากรของเครือข่ายให้แก่ผู้ใช้งานแต่ละราย, การจัดทำใบแจ้งค่าใช้จ่าย, การจัดทำรายงานจำนวนข้อมูลเกิดขึ้นจากผู้ใช้งาน และสามารถนำข้อมูลเกี่ยวกับบัญชีผู้ใช้ทรัพยากรเครือข่าย ให้ผู้ดูแลเครือข่ายสามารถวิเคราะห์และวางแผนเพื่อหาแนวทางกำหนดสิทธิในการใช้งานเครือข่าย และกำหนดปริมาณการใช้งานให้กับผู้ใช้ ให้ตรงกับวัตถุประสงค์และความจำเป็นในการใช้งานของผู้ใช้แต่ละราย และมีความสามารถในการออกรายงานหรือใบแจ้งค่าใช้จ่ายให้กับผู้ใช้งานระบบเครือข่าย เพื่อนำมา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คำนวณค่าใช้จ่ายในการจัดเก็บเงินโดยอ้างอิงตามปริมาณการใช้ทรัพยากรในเครือข่ายของผู้ใช้งานแต่ละราย

2.1.4 การจัดการประสิทธิภาพ (Performance Management)

ในระบบบริหารจัดการเครือข่ายที่ดีจะต้องมีเครื่องมือที่ช่วยบริหารจัดการเกี่ยวกับประสิทธิภาพของเครือข่าย สามารถตรวจวัดข้อมูลการจราจรในระบบเครือข่าย มาแสดงผลให้ผู้ดูแลเครือข่ายทราบ เพื่อนำข้อมูลที่ได้ไปใช้ในการตัดสินใจ วางแผน และจัดเตรียมความพร้อมของทรัพยากรในระบบเครือข่ายให้สอดคล้องกับความต้องการใช้งานเครือข่ายในปัจจุบัน โดยมีวิธีการ ดังนี้

2.1.4.1 การรวบรวมข้อมูลการทำงาน การเชื่อมต่อและการส่งผ่านข้อมูลของอุปกรณ์เครือข่าย ในทุกช่วงเวลา ตัวอย่าง การวัดประสิทธิภาพการให้บริการของเครือข่าย เช่น เวลาการตอบสนอง (Response Time), การละทิ้งแพ็คเกจ (Package Drop), การสูญหายของแพ็คเกจ (Package Loss), สภาพพร้อมใช้งานตลอดเวลา (Availability), และอัตราความผิดพลาดการรับ-ส่งข้อมูล (Error Rate) เป็นต้น

2.1.4.2 นำข้อมูลที่ได้มาเก็บรวบรวม แสดงผลและทำรายงานสรุป ซึ่งอาจอยู่ในรูปของตารางหรือแผนภาพกราฟที่ตามช่วงเวลา ซึ่งช่วยให้ผู้ดูแลเครือข่าย สามารถมองเห็นภาพรวมและประสิทธิภาพของระบบเครือข่าย รวมทั้งสามารถคาดการณ์แนวโน้มการใช้งานระบบเครือข่ายในอนาคตได้

2.1.4.3 การกำหนดระดับของประสิทธิภาพเครือข่ายที่ยอมรับได้ (Threshold) โดยผู้ดูแลเครือข่ายอาจเป็นผู้กำหนดระดับที่ยอมรับได้ ก่อนที่จะเกิดผลกระทบต่อประสิทธิภาพการทำงานของระบบเครือข่าย หากเกินกว่าระดับที่ตั้งไว้ ให้มีการแจ้งเตือนให้ผู้ดูแลเครือข่ายทราบเพื่อดำเนินการตรวจสอบและแก้ไขก่อนที่จะเกิดปัญหานั้น

2.1.5 การจัดการความมั่นคงปลอดภัย (Security Management)

ปัญหาของระบบเครือข่ายในด้านความมั่นคงปลอดภัย คือ การถูกบุกรุก ถูกโจมตีจากผู้ประสงค์ร้ายจากภายในและนอกองค์กร การเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต จึงมีความจำเป็นที่จะต้องมีการจัดการด้านความมั่นคงปลอดภัยให้กับระบบเครือข่ายภายในองค์กร โดยระบบบริหารจัดการเครือข่ายที่ดีต้องมีเครื่องมือเพื่อช่วยผู้ดูแลระบบ ในการตรวจสอบ, ควบคุมดูแลการเข้าถึงระบบเครือข่ายและอุปกรณ์เครือข่ายได้อย่างมีประสิทธิภาพ โดยใช้วิธีการเข้ารหัสข้อมูลหรือการกำหนดสิทธิในการใช้งานหรือเข้าถึงระบบเครือข่าย โดยมีวิธีการ ดังนี้

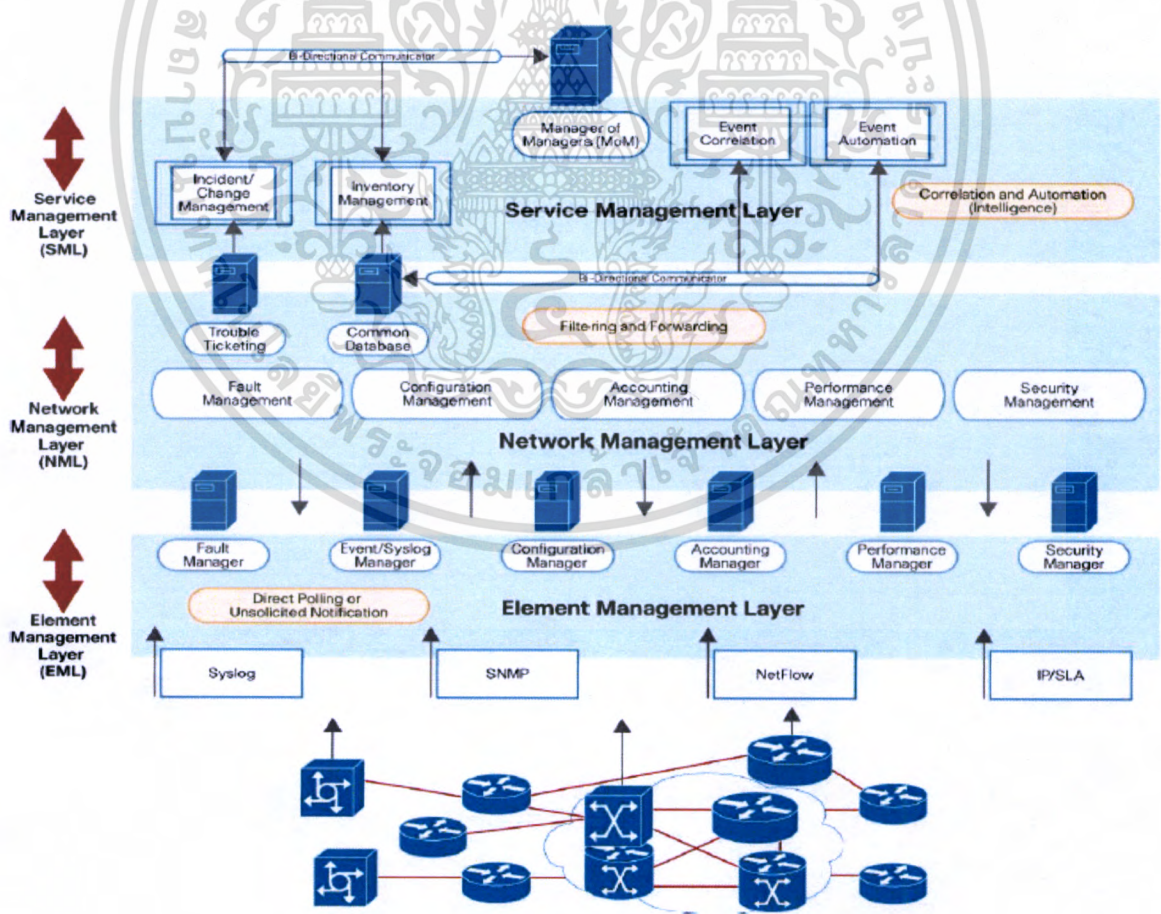
2.1.5.1 การกำหนดนโยบายจากผู้บริหาร เพื่อกำหนดระดับความสำคัญของข้อมูลในระบบเครือข่าย และกำหนดแนวทางการรักษาความมั่นคงปลอดภัยภายในองค์กร

2.1.5.2 การกำหนดจุดที่มีความเสี่ยง เพื่อตรวจหาช่องโหว่ที่อาจทำให้เกิดความเสี่ยงที่ผู้ประสงค์ร้ายจากภายในและนอกองค์กร สามารถบุกรุกเข้ามายังในระบบเครือข่ายได้

2.1.5.3 กำหนดสิทธิในการใช้งานหรือเข้าถึงระบบเครือข่ายให้กับผู้ใช้งาน รวมถึงสิทธิในการเข้าถึงอุปกรณ์เครือข่ายภายในองค์กร

2.1.5.4 มีการเก็บข้อมูลการใช้งานหรือเข้าถึงอุปกรณ์และระบบเครือข่ายอย่างต่อเนื่องตลอดเวลา รวมทั้งสามารถตรวจสอบย้อนหลังได้เมื่อเกิดปัญหา

ในส่วนของซิสโก้ได้มีการแบ่งสถาปัตยกรรมการจัดการเครือข่ายออกเป็นลำดับชั้น ตามรูปที่ 2.2 [2] โดยในระดับชั้นของการบริหารจัดการเครือข่ายจะเป็นสื่อกลางในการติดต่อสื่อสารระหว่างระดับชั้นจัดการด้านการบริการกับระดับชั้นของอุปกรณ์ในเครือข่าย โดยระดับชั้นของการบริหารจัดการเครือข่ายจะทำงานตามหลักของ FCAPS Model เพื่อเก็บรวบรวมข้อมูลจากระดับชั้นของอุปกรณ์ในเครือข่าย มาทำการคัดกรองข้อมูลและจัดระดับความสำคัญ จากนั้นทำการส่งข้อมูลและแสดงผลเป็นแผนภาพหรือรายงานสรุป ให้กับระดับชั้นจัดการด้านการบริการ ซึ่งเป็นระดับชั้นของผู้ดูแลระบบนำข้อมูลไปใช้วิเคราะห์และบริหารจัดการเครือข่ายต่อไป



รูปที่ 2.2 รูปแบบตามลำดับชั้นของ FCAPS Model ในเครือข่ายซิสโก้

เอกสารนี้เป็นเอกสารลิขสิทธิ์สงวนสิทธิ์ในชื่อของ Cisco เท่านั้น ผู้ใช้และผู้ดูแลระบบต้องปฏิบัติตามเงื่อนไขการใช้งานที่แนบมา ไม่ว่าการผิดใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

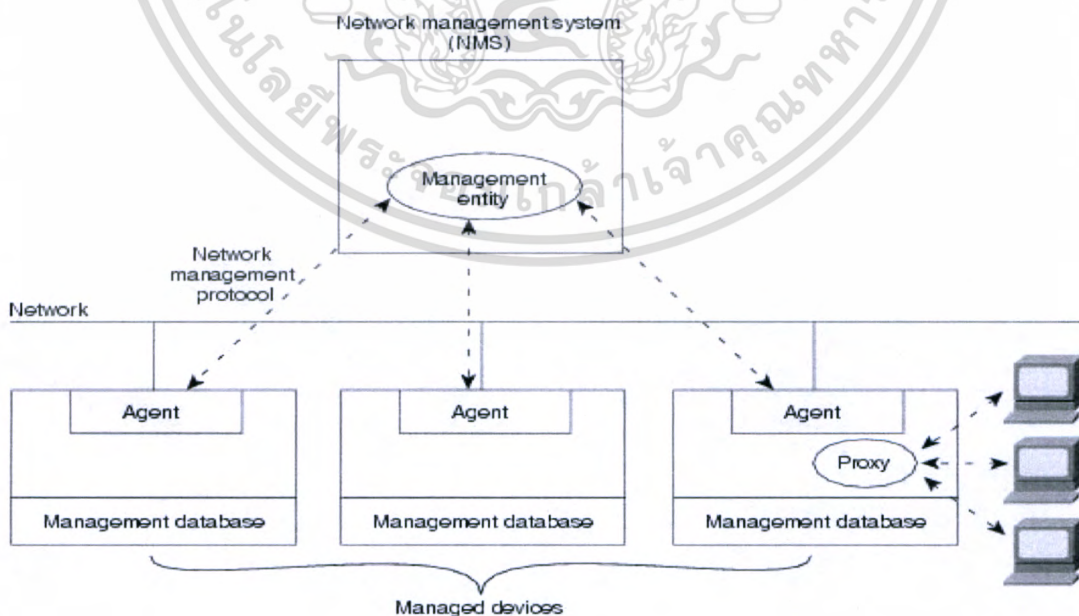
2.1.6 โครงสร้างของระบบบริหารจัดการเครือข่าย

ในระบบบริหารจัดการเครือข่าย จะมีโครงสร้างซึ่งประกอบด้วย 3 ส่วน ดังรูปที่ 2.3 [3] แสดงถึงส่วนประกอบต่างๆ ในโครงสร้างระบบบริหารจัดการเครือข่าย

2.1.6.1 ระบบจัดการเครือข่าย (Network Management System) ทำหน้าที่เป็นศูนย์กลางการควบคุม และเฝ้ามองเครือข่าย โดยจะทำการแปลความต้องการของผู้ดูแลระบบเครือข่าย ให้เป็นชุดคำสั่ง เพื่อใช้ในการตรวจสอบเครือข่าย ทำรายงานสถิติการใช้งานเครือข่าย เช่น ปริมาณผู้ใช้ ปริมาณข้อมูล สถานะของอุปกรณ์เครือข่ายและนำมาแสดงผล ให้ผู้ดูแลระบบ ได้นำข้อมูลเหล่านั้น ไปวิเคราะห์และวางแผนเกี่ยวกับการบริหารจัดการเครือข่ายต่อไป

2.1.6.2 อุปกรณ์เครือข่ายที่สามารถบริหารจัดการ (Managed Devices) คืออุปกรณ์เครือข่ายใดๆ ในระบบที่สามารถตรวจสอบและควบคุมได้ เช่น สวิตช์, เราเตอร์ เป็นต้น โดยอุปกรณ์เหล่านี้จะต้องมีเอเจนต์ซอฟต์แวร์ (Agent software) และฐานข้อมูลที่เก็บค่าต่างๆ ของอุปกรณ์นั้น (Management Information Base หรือ MIBs) เพื่อใช้สำหรับตั้งค่าหรือรายงานผลของตัวอุปกรณ์นั้น

2.1.6.3 โพรโตคอลบริหารเครือข่าย (Network Management Protocol) โดยโพรโตคอลบริหารเครือข่ายที่ใช้เป็นมาตรฐานร่วมกันคือโพรโตคอลเอสเอ็นเอ็มพี (SNMP) ซึ่งย่อมาจาก (Simple Network Management Protocol) ทำหน้าที่เป็นสื่อกลางในการรับส่งข้อมูลระหว่างระบบจัดการเครือข่ายกับอุปกรณ์เครือข่ายที่ต้องการจัดการผ่านทางระบบเครือข่ายที่เป็น TCP/IP



เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์รูปที่ 2.3 โครงสร้างของระบบบริหารจัดการเครือข่าย ไม่ว่ากรรมใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

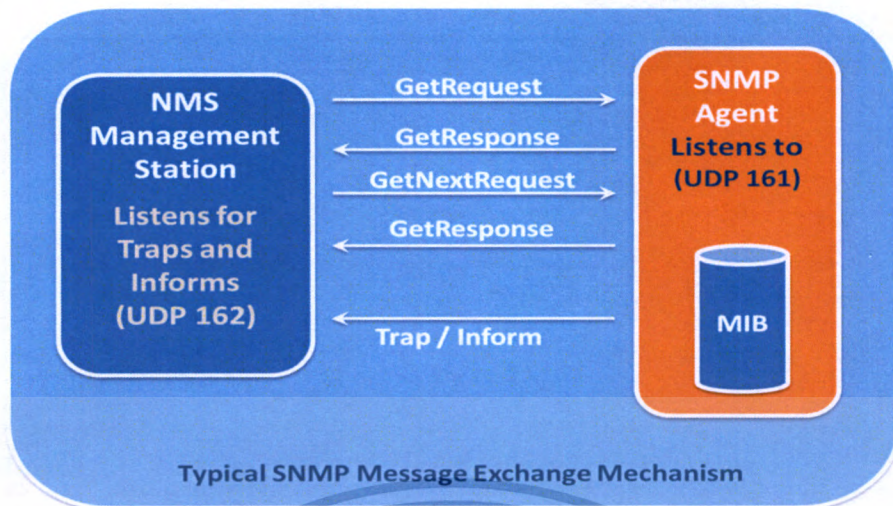
2.2 โพรโทคอลบริหารจัดการเครือข่าย

2.2.1 โพรโทคอลเอสเอ็นเอ็มพี (SNMP)

ในเครือข่ายอินเทอร์เน็ตและอินทราเน็ตที่ใช้โปรโตคอล TCP/IP จะประกอบด้วยอุปกรณ์เครือข่ายหลายรูปแบบและหลายผู้ผลิต เพื่อให้เป็นมาตรฐานกลางในการบริหารจัดการเครือข่าย ในปีพ.ศ. 2531 ทางไออีทีเอฟ (IETF: Internet Engineering Task Force) ซึ่งเป็นกลุ่มผู้ดูแลและรับผิดชอบในการกำหนดมาตรฐานต่างๆที่ใช้ในเครือข่ายอินเทอร์เน็ต ได้พัฒนาโปรโตคอลในการบริหารจัดการระบบเครือข่ายที่มีชื่อว่า โพรโทคอลเอสเอ็นเอ็มพี (SNMP) ซึ่งย่อมาจาก (Simple Network Management Protocol) เป็นโปรโตคอลในชั้นแอปพลิเคชัน (Application Layer) ของทีซีพี (Transmission Control Protocol TCP/IP) มีการทำงานแบบยูดีพี User Data Protocol (UDP) โดยใช้พอร์ต 161 และ 162 และเนื่องจากการทำงานของยูดีพีเป็นลักษณะแบบคอนเน็คชันเลส (Connectionless) คือไม่ต้องมีการสร้างคอนเน็คชัน (Connection) ก่อนที่จะทำการรับ-ส่งข้อมูล จึงทำให้สามารถรับ-ส่งข้อมูลได้อย่างรวดเร็วซึ่งเหมาะสำหรับที่จะใช้ส่งข้อความสั้นๆในระบบเครือข่าย โดยโปรโตคอลเอสเอ็นเอ็มพีนี้ใช้เพื่อบริหารจัดการกับอุปกรณ์ต่างๆ ที่เชื่อมต่ออยู่ในระบบเครือข่าย ทำให้ผู้ดูแลระบบสามารถ ตรวจสอบสถานะ ควบคุมอุปกรณ์ที่สนับสนุนโปรโตคอลเอสเอ็นเอ็มพีในระบบเครือข่ายได้จากระยะไกล และช่วยให้ระบบบริหารจัดการเครือข่ายสามารถเก็บรวบรวมข้อมูลสถานะที่เกิดขึ้นบนอุปกรณ์ เพื่อนำไปวิเคราะห์และแสดงผลให้กับผู้ดูแลระบบเครือข่ายเพื่อใช้ในการแก้ปัญหาความผิดพลาดของระบบที่เกิดขึ้นได้อย่างรวดเร็ว รวมทั้งใช้ในการจัดการประสิทธิภาพ และการวางแผนการเดินโตของเครือข่ายขององค์กรในอนาคตได้

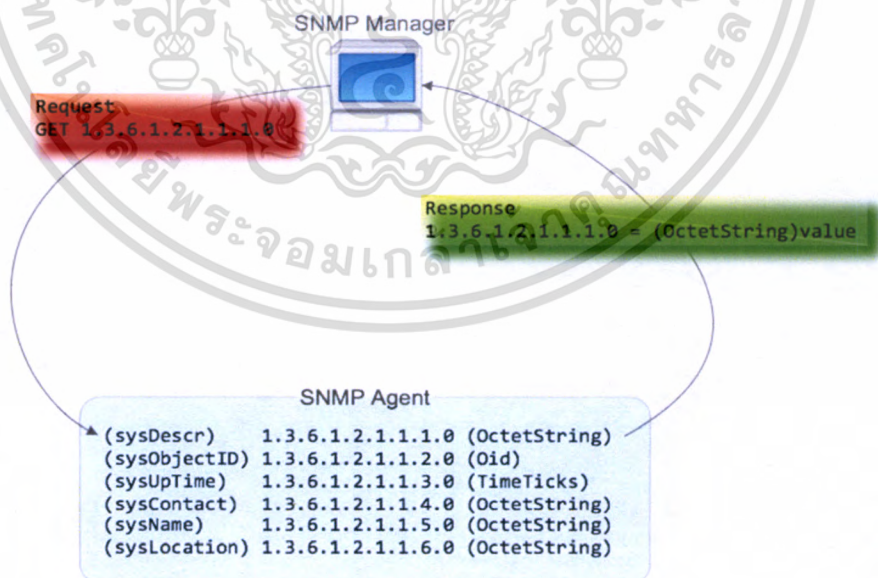
2.2.2 โครงสร้างของโปรโตคอลเอสเอ็นเอ็มพี

โปรโตคอลเอสเอ็นเอ็มพี เป็นโปรโตคอลที่ระบบบริหารจัดการเครือข่ายใช้รับ-ส่งข้อมูลเพื่อร้องขอและส่งข้อมูลจากอุปกรณ์เครือข่ายผ่านทางพอร์ต 161 และพอร์ต 162 สำหรับใช้ในการรับแตรัพ (Trap) การแจ้งเตือนจากอุปกรณ์เครือข่ายมายังระบบบริหารจัดการเครือข่าย ดังรูปที่ 2.4 [4] ในโปรโตคอลเอสเอ็นเอ็มพีนั้นจะมีคำสั่งที่ใช้รับส่งข้อมูลระหว่างระบบจัดการเครือข่ายกับอุปกรณ์เครือข่ายอยู่ 5 คำสั่งดังนี้



รูปที่ 2.4 โครงสร้างการทำงานของโปรโตคอลเอสเอ็นเอ็มพี(SNMP)

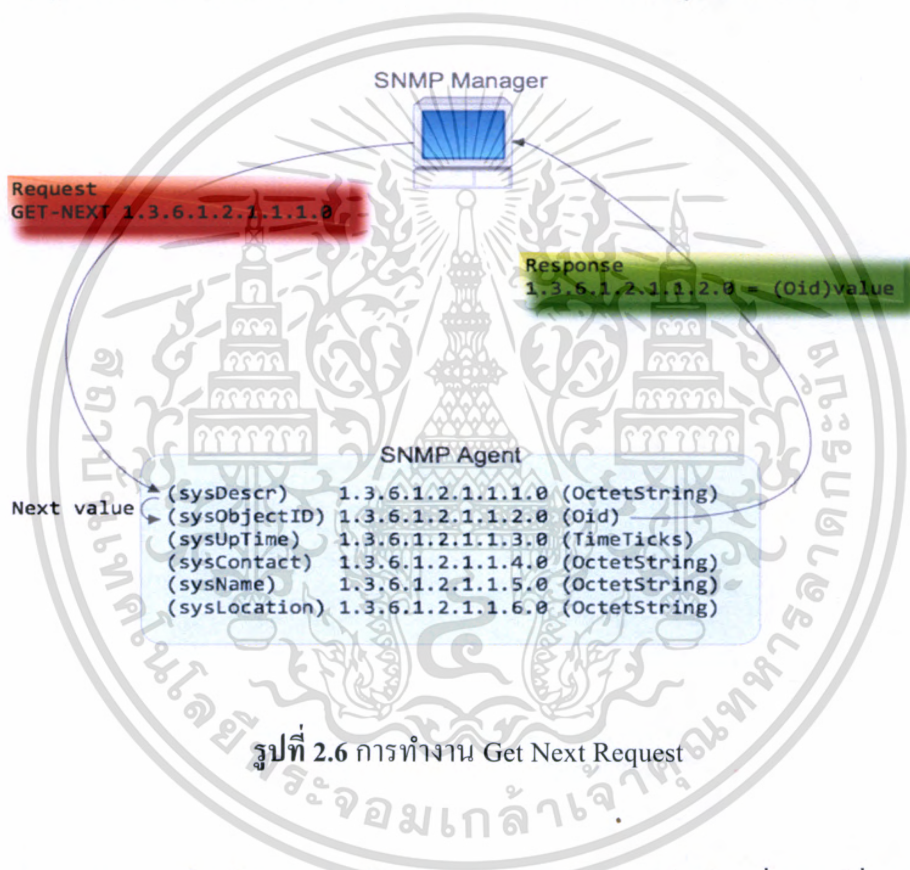
1. Get Request เป็นข้อความการร้องขอข้อมูลจากระบบจัดการเครือข่ายไปที่อุปกรณ์เครือข่ายเพื่อร้องขอข้อมูลออบเจกต์ในเอสเอ็นเอ็มพีเอเจนต์ (SNMP Agent) ดังรูปที่ 2.5 [5] โดยระบบจัดการเครือข่ายสามารถร้องขอข้อมูลออบเจกต์ได้หลายๆค่าพร้อมกันในหนึ่ง Get Request message ได้



รูปที่ 2.5 การทำงาน Get Request

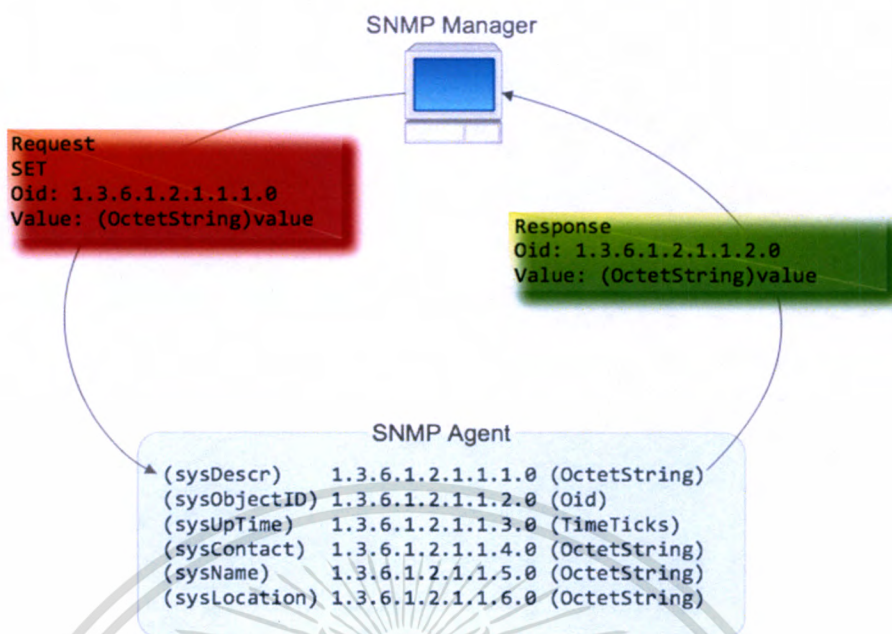
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. Get Next Request เป็นข้อความการร้องขอข้อมูลจากระบบจัดการเครือข่ายไปที่อุปกรณ์เครือข่ายสำหรับขอค่าตัวแปรต่อไปหลังจากได้รับคำตอบจากการร้องขอในครั้งแรก (ในกรณียังมีตัวแปรอื่นๆอีก) ข้อความการร้องขอนี้จะช่วยในกรณีที่ระบบจัดการเครือข่ายไม่ทราบแน่ชัดว่าข้อมูลออปเจกต์ที่มีอยู่ มีจำนวนเท่าใดบ้าง โดยจะสามารถส่ง Get Next Request ไปได้เรื่อยๆในการร้องขอข้อมูลออปเจกต์ที่ต้องการ จะต้องระบุค่าของออปเจกต์ (Object Identifier) หรือ (OID) ไปพร้อมกับกับ Get Next Request โดยตัวอย่างของการระบุค่าออปเจกต์ (OID) เช่น 1.3.6.1.4.1.2680.1.2.7.3.2.0 ดังรูปที่ 2.6 [5]



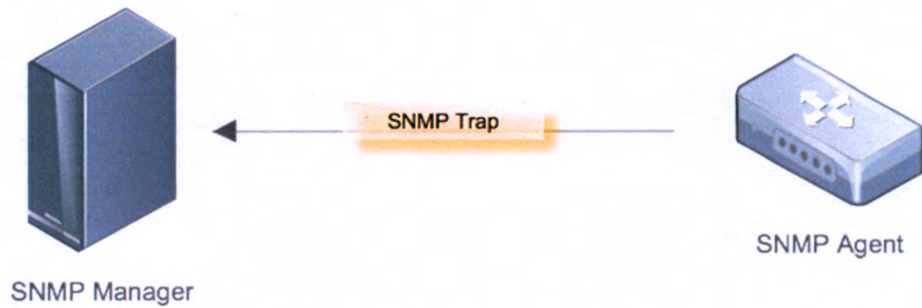
3. Set Request เป็นข้อความการร้องขอของระบบจัดการเครือข่ายเพื่อขอเปลี่ยนแปลงหรือกำหนดค่าของเอสเอ็นเอ็มพีเอเจนต์ ดังรูปที่ 2.7 [5]

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.7 การทำงาน Set Request

4. Get Response เป็นข้อความตอบกลับจากอุปกรณ์เครือข่ายไปหาระบบจัดการเครือข่ายโดยการตอบสนองคำร้องขอจะเป็นไปตามลักษณะของการร้องขอ ถ้าการร้องขอเป็น Get Request หรือ Get Next Request จะมีการตอบกลับโดยส่งค่าของข้อมูลที่มาจากเอสเอ็นเอ็มพีเอเจนต์ แต่ถ้าเป็น Set Request จะมีการตอบกลับโดยส่งค่าเป็นการยืนยันคำสั่งในการกำหนดหรือเปลี่ยนแปลงค่าเอสเอ็นเอ็มพีเอเจนต์ ว่าดำเนินการสำเร็จหรือไม่
5. Trap เป็นข้อความตอบกลับจากอุปกรณ์เครือข่ายของเอสเอ็นเอ็มพีเอเจนต์เมื่อเกิดเหตุการณ์ต่างๆ เช่น อุปกรณ์มีการเริ่มต้นทำงานใหม่ โดยจะกำหนดได้ว่าจะให้อุปกรณ์ส่งข้อมูลไปหาระบบจัดการเครือข่ายตัวไหน จากการระบุหมายเลขเครือข่าย (IP Address) ของระบบจัดการเครือข่ายนั้น ซึ่งทำให้ระบบจัดการเครือข่ายสามารถรับรู้เหตุการณ์ได้โดยไม่ต้องส่ง Get request มาถามอุปกรณ์เครือข่าย ทำให้ลดระยะเวลาและปริมาณข้อมูลในการติดต่อสื่อสาร ดังรูปที่ 2.8 [5]



รูปที่ 2.8 การทำงานของ SNMP Trap

2.2.3 รุ่นของโปรโตคอลเอสเอ็นเอ็มพี

โปรโตคอลเอสเอ็นเอ็มพีได้ถูกศึกษาและพัฒนาขึ้นมาเป็นรุ่นต่างๆ เพื่อให้มีความเหมาะสมในการใช้งานที่เกี่ยวกับการบริหารจัดการระบบเครือข่าย มีการเพิ่มประสิทธิภาพในด้านการรักษาความปลอดภัยและความถูกต้องมากขึ้น ปัจจุบันโปรโตคอลเอสเอ็นเอ็มพีได้ถูกพัฒนาขึ้นมาแล้วจำนวน 3 รุ่น โดยรุ่นแรกเรียกว่า SNMPv1 และมีการพัฒนาขึ้นเป็นรุ่นที่ 2 (SNMPv2) และรุ่นที่ 3 (SNMPv3) ตามลำดับ แต่ละรุ่นมีความสามารถในการทำงานที่เพิ่มมากขึ้นและแตกต่างกันดังแสดงในตารางที่ 2.1

ตารางที่ 2.1 แสดงการเปรียบเทียบการทำงานของโปรโตคอลเอสเอ็นเอ็มพีแต่ละรุ่น

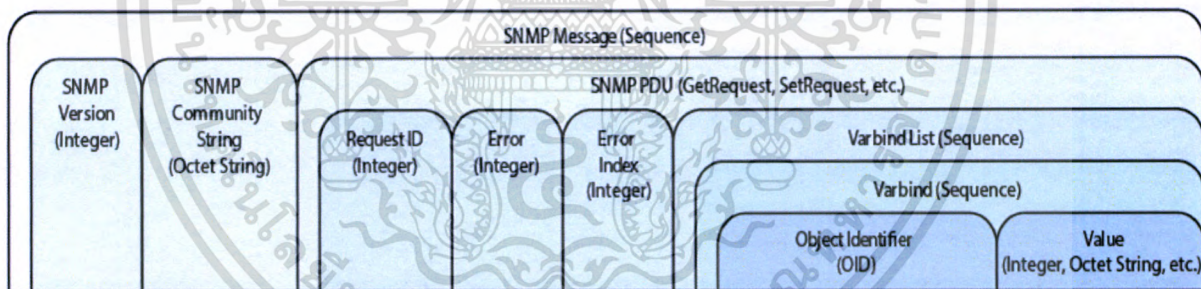
Feature	Version 1	Version 2	Version 3
GET request	Yes	Yes	Yes
GET-NEXT request	Yes	Yes	Yes
SET request	Yes	Yes	Yes
GET-BULK request	No	Yes	Yes
TRAP notification	Yes	Yes	Yes
INFORM notification	No	Yes	Yes
Community based security	Yes	Yes	No
User based security	No	No	Yes
Message Authentication	No	No	Yes
Message Encryption (privacy)	No	No	Yes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

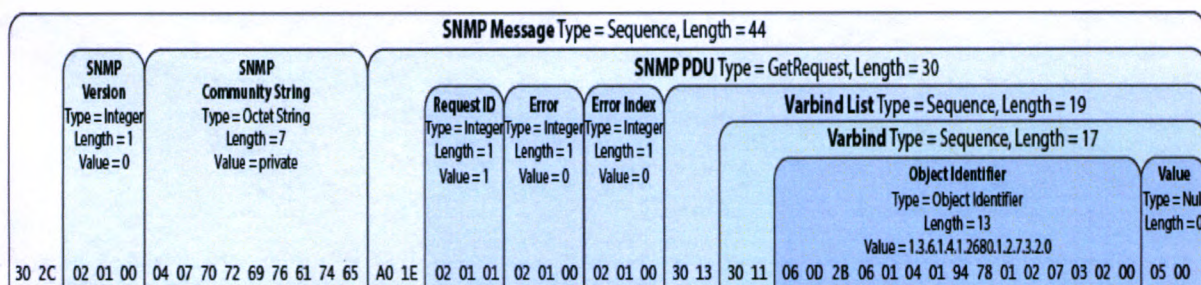
2.2.4 ชุดข้อมูลของข้อความเอสเอ็นเอ็มพี (SNMP Message)

ภายในโปรโตคอลเอสเอ็นเอ็มพีจะมีชุดข้อมูลเอสเอ็นเอ็มพี แมสเซจ (SNMP Message) ดังรูปที่ 2.9 [7] เป็นการแสดงโครงสร้างของเอสเอ็นเอ็มพีแมสเซจ ที่บรรจุข้อมูลสำหรับการจัดการ ซึ่งประกอบด้วย 3 ส่วน ดังนี้

- 2.3.3.1 เวอร์ชัน (Version) เป็นส่วนที่ระบุหมายเลขรุ่นของโปรโตคอลเอสเอ็นเอ็มพีที่ใช้
- 2.3.3.2 คอมมูนิตี (Community) เป็นส่วนที่ระบุถึงชื่อที่ใช้ตรวจสอบเพื่อกำหนดสิทธิและความปลอดภัยของเอสเอ็นเอ็มพี แมสเซจ ที่ใช้ในการร้องขอข้อมูลจากเอสเอ็นเอ็มพีเอเจนต์ บนอุปกรณ์เครือข่าย โดยชื่อของคอมมูนิตีที่ใช้ในระบบบริหารจัดการเครือข่าย จะต้องตรงกันกับที่ตั้งไว้ในอุปกรณ์เครือข่ายเท่านั้น
- 2.3.3.3 โปรโตคอลดาต้ายูนิต หรือ พีดียู (Protocol Data Unit : PDU) ภายในพีดียู แบ่งข้อมูลออกเป็น 3 ส่วน คือ พีดียูแท็ก (PDU Tag) บรรจุข้อมูลร้องขอและข้อมูลที่ได้รับตอบกลับมา, พีดียูเลนธ์ (PDU Length) บรรจุข้อมูลบอกความยาวของพีดียู และ พีดียูฟิลด์แวลู (PDU Field Value) ประกอบด้วยข้อมูล 4 ส่วน คือ Request Identifier, Error Status, Error Index และ Variable Bindings List โดยแต่ละส่วนของโปรโตคอลดาต้ายูนิตจะแสดงรายละเอียดและขนาดของข้อมูลในรูปที่ 2.10 [7]



รูปที่ 2.9 โครงสร้างของเอสเอ็นเอ็มพีแมสเซจ (SNMP Message)

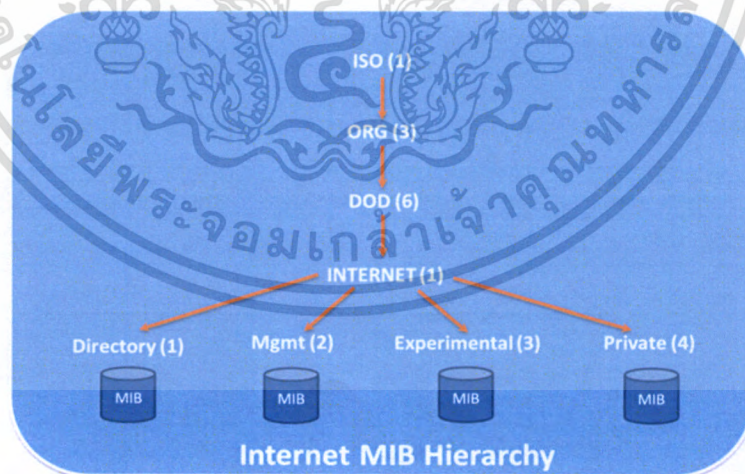


รูปที่ 2.10 รายละเอียดโครงสร้างของเอสเอ็นเอ็มพีแมสเซจ (SNMP Message)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา 146527 หรือแจ้งถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

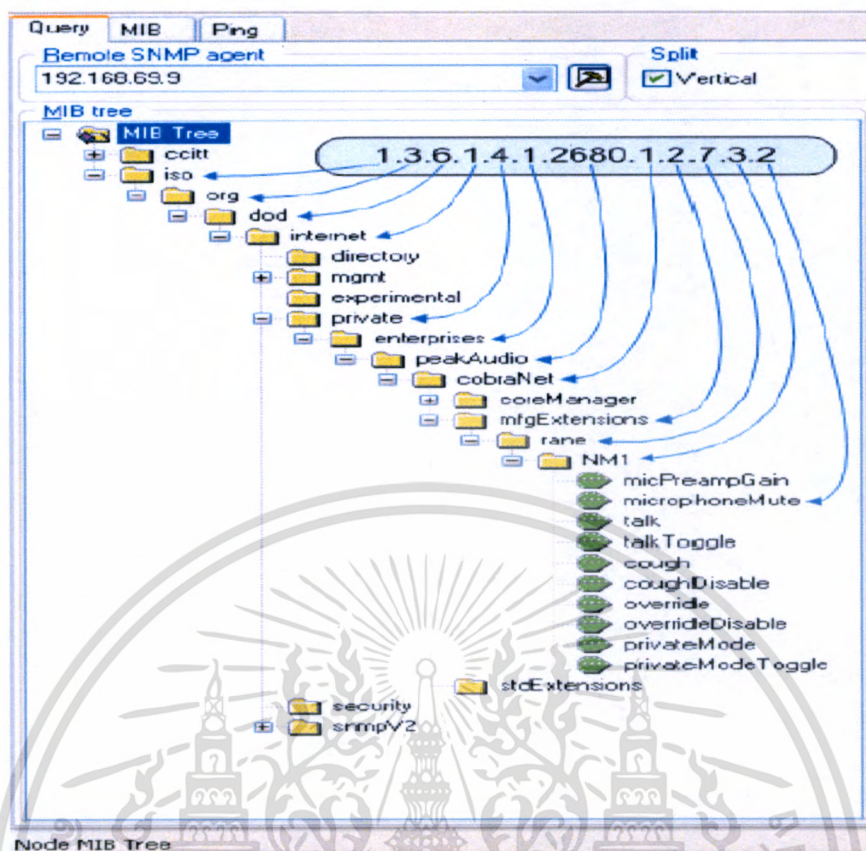
2.2.5 ฐานข้อมูลการจัดการ (Management Information Bases หรือ MIBs)

อุปกรณ์ใดๆที่เชื่อมต่ออยู่บนระบบเครือข่ายที่สนับสนุนโปรโตคอลเอสเอ็มไอจะมีการเก็บข้อมูลคุณสมบัติต่างๆของอุปกรณ์นั้นๆไว้ในฐานข้อมูลการจัดการ (Management Information Bases หรือ MIBs)ซึ่งฐานข้อมูลนี้จะอยู่บนตัวของอุปกรณ์เหล่านั้น ภายใน MIBs จะบรรจุข้อมูล เช่น ข้อมูลคุณลักษณะ สถานะ สถิติด้านประสิทธิภาพ ค่าต่างๆของอุปกรณ์ที่กำหนดไว้เป็นต้น โครงสร้างของ MIBs เป็นส่วนหนึ่งของโครงสร้างเอสเอ็มไอ Structure of Management Information หรือ (SMI) ดังรูปที่ 2.11 [4] โดยถูกกำหนดโดยความร่วมมือกันระหว่าง International Organization for Standardization (ISO) และ Consultative Committee International Telegraph and Telephone (CCITT) ให้มีลักษณะโครงสร้างแบบต้นไม้ (Tree) เรียงกันเป็นลำดับชั้น(Hierarchical) มีส่วนที่เรียกว่า Root และแตกแยกออกมาเป็นโหนดย่อย ในการอ้างอิงแต่ละโหนดภายในต้นไม้ โดยแต่ละโหนดบนโครงสร้างแบบต้นไม้ก็คือ ออบเจกต์ (Object) โดยแต่ละออบเจกต์จะมีหมายเลขกำกับอยู่ซึ่งหมายเลขดังกล่าวนี้เรียกว่า Object Identifier หรือ (OID) โดยเราจะใช้ OID ในการระบุตำแหน่งของข้อมูลที่อยู่ในโครงสร้างเอสเอ็มไอ จากรูปที่ 2.11 ถ้าเราจะเข้าถึงโหนดที่ชื่อ Mgmt จะได้ OID เป็น 1.3.6.1.2 สำหรับเส้นทางที่จะนำไปสู่โหนดของ Mgmt นั้นจะต้องผ่านทาง ISO (1), ORG (Organization)(3), DOD (Department Of Defense) (6), Internet (1), Mgmt (Management) (2) โดยปกติการอ้างอิงถึง OID จะเขียนปิดท้าย ด้วย 0 ดังนั้น 1.3.6.1.2.0 คือการอ้างอิงถึงตัวแปร Mgmt. นี้โดยหากใช้โปรแกรมที่สามารถดู MIBs ได้จะแสดงตัวอย่างดังรูปที่ 2.12 [8]



รูปที่ 2.11 โครงสร้างของ Structure of Management Information หรือ (SMI)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.12 การเรียกดูโครงสร้างของ MIBs Tree ผ่านโปรแกรม

แต่เดิมนั้นมีโหนดที่เชื่อมต่อกับ MIB-1 อยู่ 8 กลุ่ม จากนั้นได้มีการปรับปรุงโครงสร้างของ MIBs เพื่อให้ครอบคลุมกับข้อมูลของอุปกรณ์ต่างๆและเทคโนโลยีที่เกิดขึ้นมาใหม่จึงเกิดเป็น MIB-2 โดย MIB-2 จะสามารถแบ่งได้เป็น 11 กลุ่มซึ่งแสดงในรูปที่ 2.13 [9] แต่ละกลุ่มมีรายละเอียดดังนี้

2.2.5.1 System เป็นกลุ่มที่แสดงรายละเอียดทั่วไปของอุปกรณ์ นั้นได้แก่ ชนิดของฮาร์ดแวร์ ระบบปฏิบัติการ ระยะเวลาของระบบตั้งแต่เริ่มทำงาน เป็นต้น

2.2.5.2 Interface เป็นกลุ่มที่แสดงรายละเอียดข้อมูลที่เกี่ยวข้องกับ ฟิสิคอลลินเตอร์เฟส (Physical Interface) ของอุปกรณ์ ที่มีการติดตั้งอยู่บนอุปกรณ์ และข้อมูลที่แสดงถึงเหตุการณ์ ต่างๆ ที่เกิดขึ้นกับอินเตอร์เฟส เช่น หมายเลขอินเตอร์เฟส จำนวนอินเตอร์เฟส, ชนิดของอินเตอร์เฟส และ ความสามารถในการรับ-ส่งข้อมูลของอินเตอร์เฟส เป็นต้น

2.2.5.3 Address Translation (AT) เป็นกลุ่มที่ทำหน้าที่เป็นตารางอ้างอิงระหว่างเน็ตเวิร์คแอดเดรสกับฟิสิคอลลินเตอร์เฟส (Physical Address) โดยเน็ตเวิร์คแอดเดรสจะเป็นไอพีแอดเดรส

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

และในส่วนของ ฟิสิกอลแอดเดรสนั้นจะขึ้นอยู่กับประเภทของเครือข่าย เช่น ถ้าเป็นอีเทอร์เน็ต (Ethernet) ก็จะใช้อีเทอร์เน็ตแอดเดรสเป็นฟิสิกอลแอดเดรส

2.2.5.4 Internet Protocol (IP) เป็นกลุ่มที่แสดงข้อมูลเกี่ยวกับไอพีแอดเดรสที่ถูกกำหนดให้กับแต่ละอินเตอร์เฟซของอุปกรณ์ และรวมถึงเก็บข้อมูลสำหรับการเลือกเส้นทางในเครือข่ายอินเทอร์เน็ต

2.2.5.5 Internet Control Message Protocol (ICMP) เป็นกลุ่มที่แสดงข้อมูลเกี่ยวกับโปรโตคอลไอซีเอ็มพี ที่ใช้ในการวิเคราะห์เครือข่าย

2.2.5.6 Transmission Control Protocol (TCP) เป็นกลุ่มที่แสดงข้อมูลการทำงานที่เกี่ยวกับโปรโตคอลทีซีพี เช่น ข้อมูลการเชื่อมต่อของอุปกรณ์โดยใช้โปรโตคอลทีซีพี ข้อมูลสถานะของทีซีพี เป็นต้น

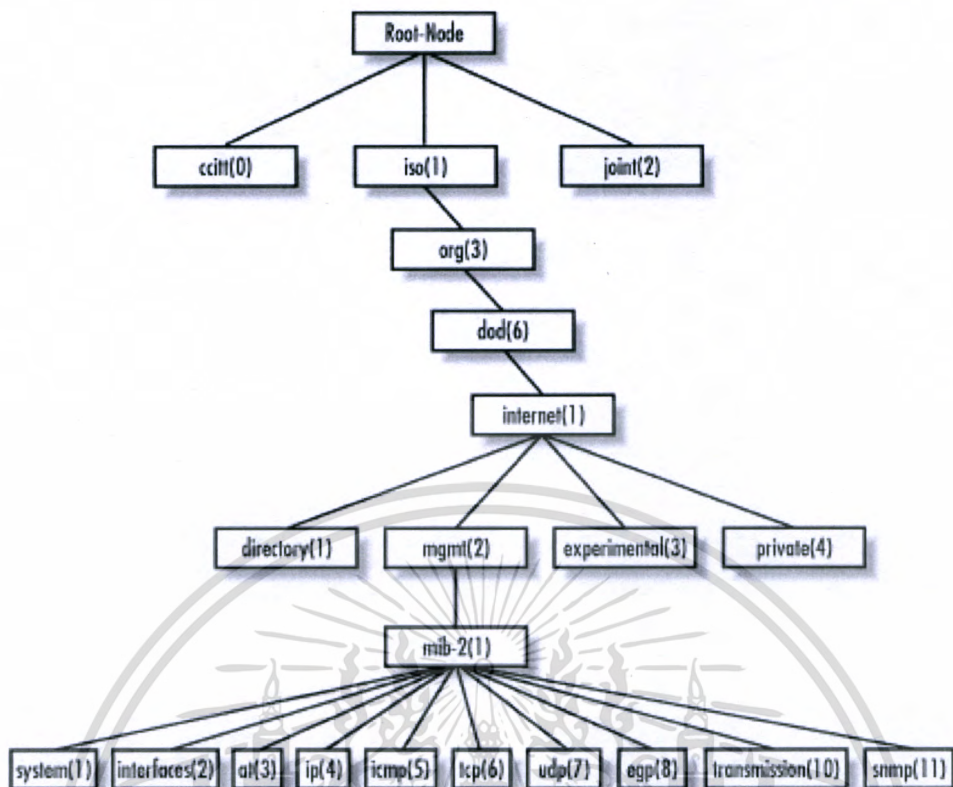
2.2.5.7 User Datagram Protocol (UDP) เป็นกลุ่มที่แสดงข้อมูลการทำงานที่เกี่ยวกับโปรโตคอลยูดีพี เช่น ข้อมูลการเชื่อมต่อของอุปกรณ์โดยใช้โปรโตคอลยูดีพี จำนวนยูดีพีที่เกิดความผิดพลาด เป็นต้น

2.2.5.8 Exterior Gateway Protocol (EGP) เป็นกลุ่มที่แสดงข้อมูลเกี่ยวกับโปรโตคอลอีจีพี เช่น ตารางข้อมูลของโปรโตคอลอีจีพี จำนวนอีจีพีแพ็คเก็ตที่ได้รับ

2.2.5.9 Common Management Information Protocol over TCP/IP (CMOT) เป็นกลุ่มที่เก็บไว้ใช้ในอนาคตเพื่อใช้กับโปรโตคอลซีเอ็มไอพี (CMIP) ที่ทำงานบนเครือข่ายอินเทอร์เน็ต

2.2.5.10 Transmission เป็นกลุ่มที่เกี่ยวข้องกับสื่อที่ใช้ในการรับ-ส่งข้อมูลตามชนิดของอินเตอร์เฟซที่มีใช้ในระบอบตามที่กำหนด เช่น X.25, RJ45, FDDI เป็นต้น

2.2.5.11 Simple Network Management Protocol (SNMP) เก็บข้อมูลที่เกี่ยวข้องกับการทำงานของโปรโตคอลเอสเอ็นเอ็มพี และการจัดการเครือข่ายด้วยโปรโตคอลเอสเอ็นเอ็มพี

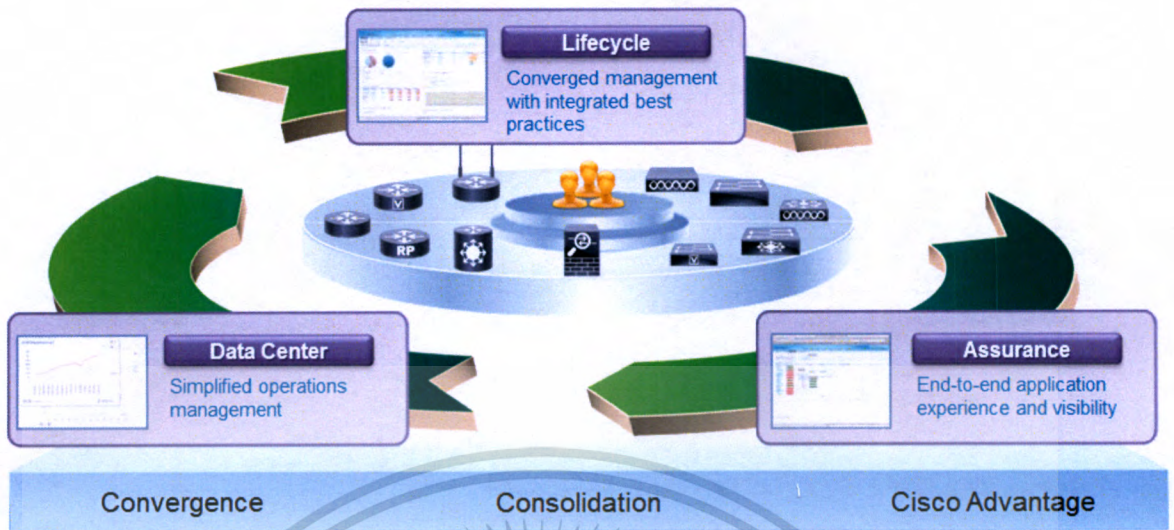


รูปที่ 2.13 โครงสร้างของ MIB-2

2.3 สถาปัตยกรรมของระบบบริการจัดการเครือข่ายซิสโก้

2.3.1 ระบบบริการจัดการเครือข่ายซิสโก้ (Cisco Prime Infrastructure)

ระบบบริหารจัดการเครือข่ายซิสโก้ (Cisco Prime Infrastructure) เป็นระบบที่ช่วยบริหารจัดการอุปกรณ์เครือข่ายต่างๆ ของซิสโก้ เช่น สวิตช์ เราเตอร์ อุปกรณ์เครือข่ายไร้สาย อุปกรณ์ดูแลความปลอดภัยบนเครือข่าย เป็นต้น โดยมีเครื่องมือที่ช่วยในการทำงานของผู้ดูแลระบบให้สะดวก รวดเร็ว และง่ายขึ้น พร้อมทั้งสามารถบริหารจัดการอุปกรณ์เครือข่ายจากศูนย์กลางและมีการแสดงผลเป็นแผนภาพทำให้เข้าใจได้ง่าย ช่วยให้ผู้ดูแลระบบสามารถจัดเตรียม (Provisioning) ดูแลเฟ้าระวัง (Monitoring) เพิ่มความสามารถในการแก้ไขปัญหา (Troubleshooting) บนระบบเครือข่าย ทำให้การบริหารจัดการเครือข่ายทำได้มีประสิทธิภาพมากขึ้น ดังรูปที่ 2.14 [10]



รูปที่ 2.14 ภาพรวมของระบบบริการจัดการเครือข่ายซิสโก้

2.3.2 ความสามารถของระบบบริการจัดการเครือข่ายซิสโก้ (Cisco Prime Infrastructure)

ความสามารถของระบบบริการจัดการเครือข่ายซิสโก้ (Cisco Prime Infrastructure) สามารถแบ่งแยกย่อยออกมาได้ 2 กลุ่มหลักคือ

1. ความสามารถในการบริหารจัดการวงจรชีวิตของอุปกรณ์เครือข่ายซิสโก้ (Lifecycle Management) ในส่วนนี้จะศูนย์กลางการบริหารจัดการอุปกรณ์เครือข่ายของซิสโก้ที่ติดตั้งใช้ใช้งานในระบบเครือข่าย โดยมีความสามารถดังนี้
 - ความสามารถการสังเกตการณ์ ตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่าย
 - ความสามารถในการจัดทำรายการอุปกรณ์เครือข่ายซิสโก้ที่มีอยู่ในเครือข่าย
 - การจัดทำมาตรฐานในการจัดการค่าที่ติดตั้ง (Configuration) บนอุปกรณ์เครือข่ายให้เป็นมาตรฐานเดียวกัน มีเครื่องมือเปรียบเทียบเพื่อค่าที่ติดตั้งของใหม่และของเก่า มีความสามารถในการตั้งเวลาในการจัดเก็บค่าที่ติดตั้งบนอุปกรณ์เครือข่ายตามช่วงเวลา ที่ผู้ดูแลระบบกำหนดได้โดยอัตโนมัติ เป็นศูนย์กลางการจัดเก็บค่าที่ติดตั้งและจัดทำข้อมูลสรุปรายการการปรับปรุงแก้ไขค่าที่ติดตั้งบนอุปกรณ์เครือข่าย
 - ความสามารถในการจัดทำแผนภาพ เพื่อแสดงการเชื่อมต่อของเครือข่ายที่ใช้สายและแสดงการครอบคลุมของสัญญาณในเครือข่ายไร้สาย
 - ความสามารถในการแสดงผล ช่วยวิเคราะห์ข้อมูลและแจ้งให้กับผู้ดูแลเครือข่ายทราบ ในกรณีอุปกรณ์เครือข่ายเกิดความผิดปกติ หรือมีปริมาณของข้อมูลเกินกว่าค่าที่ทางผู้ดูแลเครือข่ายตั้งไว้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. ความสามารถในการบริหารจัดการความเชื่อมั่นในการสื่อสารข้อมูลของอุปกรณ์เครือข่ายซิสโก้ (Assurance Management) ในส่วนนี้จะป็นศูนย์กลางด้านการบริหารจัดการข้อมูลการใช้งานและการสื่อสารบนอุปกรณ์เครือข่ายของซิสโก้ โดยมีความสามารถดังนี้
 - ความสามารถในการวิเคราะห์การใช้งานบนเครือข่ายของแต่ละผู้ใช้งาน เช่น ปริมาณการใช้งาน จำนวนข้อมูลที่ใช้งาน และชนิดของซอฟต์แวร์ที่ใช้งานบนเครือข่าย
 - ความสามารถในการทำงานร่วมกับโปรโตคอลวิเคราะห์เครือข่ายที่ติดตั้งอยู่ในอุปกรณ์เครือข่ายของซิสโก้ เช่น Net-Flow, Flexible Net-Flow, NBAR2 เป็นต้น

2.3.3 ความต้องการใช้งานทรัพยากรของระบบ

ระบบบริการจัดการเครือข่ายซิสโก้ (Cisco Prime Infrastructure) ถูกออกแบบมาให้สามารถติดตั้งและใช้งานได้ง่ายโดยการติดตั้งสามารถเลือกทำได้ 2 วิธีคือ

1. Virtual: ระบบบริการจัดการเครือข่ายซิสโก้ (Cisco Prime Infrastructure) จะทำให้อยู่ในรูปแบบของไฟล์ Open Virtualization Archive (OVA) ทำให้สามารถติดตั้งใช้งานบนระบบ VMware ESXi ได้ทันที โดยความต้องการใช้งานทรัพยากรขั้นต่ำของระบบสามารถดูได้จากตารางที่ 2.2

ตารางที่ 2.2 ความต้องการใช้งานทรัพยากรขั้นต่ำในการติดตั้งบน Virtual

Requirement	Express	Express-Plus	Standard	Professional
VMware Version	ESXi 5.1 or 5.5	ESXi 5.1 or 5.5	ESXi 5.1 or 5.5	ESXi 5.1 or 5.5
Virtual CPUs	4	8	16	16
Memory (DRAM)	12 GB	16 GB	16 GB	24 GB
HDD Size	300 GB	600 GB	900 GB	1.2 TB
Throughput (Disk IOPS)	200 MB/s	200 MB/s	200 MB/s	320 MB/s

2. Physical: ระบบบริการจัดการเครือข่ายซิสโก้ (Cisco Prime Infrastructure) จะถูกติดตั้งเสร็จมาในเซิร์ฟเวอร์ของซิสโก้ ซึ่งมีชื่อเรียกว่า (Cisco Unified Computing System) หรือ (UCS) โดยใช้ระบบ VMware ESXi เป็นพื้นฐานการทำงาน โดยความต้องการใช้งานทรัพยากรพื้นฐานของระบบสามารถดูได้จากตารางที่ 2.3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.3 ความต้องการใช้งานทรัพยากรขั้นต่ำในการติดตั้งบน Physical

Physical Appliance Options	Appliance Image Format	Bare Metal/ISO
	Equivalent 1.x Option	Physical Appliance
Hardware Specifications	CPU (cores/threads)	10 C/20 T
	Memory	64 GB
	Disk Capacity	4x900 GB
	RAID Level	RAID 10
	Disk I/O Speed	320 MBps
Devices	Maximum unified APs	20,000
	Maximum autonomous APs	3000
	Maximum WLAN controllers	1000
	Maximum wired (switches, routers)	13,000
	Maximum MSEs	25
	NAMs	1000
	Maximum number of devices	24,000
Clients	Wired clients	50,000
	Wireless clients	200,000
	Changing clients (every 5 min.)	40,000
Monitoring	Events sustained rate (events/sec)	1000
	Netflow rate (flows/sec)	80,000
	Max interfaces	350,000
	Max NAM polling data enabled	40
System	Max number sites/campus	2500
	Max groups	150
	Max virtual domains	1200
System Users	Concurrent GUI clients	50
	Concurrent API clients	5

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3.4 รายละเอียดแต่ละรุ่นของระบบบริการจัดการเครือข่ายซิสโก้ (Cisco Prime Infrastructure)

ระบบบริการจัดการเครือข่ายซิสโก้ (Cisco Prime Infrastructure) ถูกออกแบบมาให้รองรับรับกับจำนวนของอุปกรณ์เครือข่ายในเครือข่ายและขนาดของเครือข่ายแต่ละองค์กรจากตารางที่ 2.4 จะแสดงรายละเอียดแต่ละรุ่นของระบบบริการจัดการเครือข่ายซิสโก้ (Cisco Prime Infrastructure) โดยแต่ละรุ่นของระบบบริการจัดการเครือข่ายซิสโก้ (Cisco Prime Infrastructure) จะมีความสามารถในการทำงานเหมือนกัน แต่แตกต่างกันที่ความสามารถในการรองรับกับจำนวนของอุปกรณ์เครือข่ายและขนาดของเครือข่ายในแต่ละองค์กรที่จะนำไปใช้

ตารางที่ 2.4 รายละเอียดแต่ละรุ่นของระบบบริการจัดการเครือข่ายซิสโก้

Parameter (Maximums)	Express	Express-Plus	Standard	Professional
Unified APs	300	25,00	5,000	20,000
Autonomous Aps	300	500	3,000	3,000
Wired Devices	300	1,000	6,000	13,000
NAMs	5	5	500	1,000
Controllers	5	25	500	1,000
Wired Clients	6,000	50,000	50,000	50,000
Wireless Clients	4,000	30,000	75,000	200,000
Cisco Mobility Services Engine (MSE)	1	1	6	12
Changing Clients (every 5 minutes)	1,000	5,000	25,000	40,000
Events Sustained Rate (events per second)	100	100	300	1,000
NetFlow Rate (flows per second)	3,000	3,000	16,000	80,000
Supported Hourly Host Records	144,000	720,000	2,100,000	12,000,000
Interfaces	12,000	50,000	250,000	350,000
NAM Data Polling Enabled	5	5	20	40
Polling Interfaces (polling of trunk ports)	2,400	8000	48,000	100,000
Number of Sites per Campus	200	500	2,500	2,500
Concurrent GUI Clients	5	10	25	50
Local Users	100	500	1,000	1,000
Location Groups	50	50	1,000	1,000

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3

การดำเนินงาน

ในการดำเนินงาน ศึกษา ทดลอง และทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) ผู้จัดทำได้ดำเนินการติดตั้งซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) ในเวอร์ชันทดลองใช้ (Trial Version) บนระบบ VMware ESXi ที่มีใช้งานอยู่แล้วในองค์กร โดยจะเลือกใช้ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) รุ่น Express ซึ่งเพียงพอและสามารถรองรับกับจำนวนอุปกรณ์เครือข่ายที่จะนำมาทดสอบ จากนั้นได้ทำการเชื่อมต่อระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) เข้ากับระบบเครือข่ายขององค์กรที่ใช้งานอยู่จริงและทำการคัดเลือกอุปกรณ์เครือข่ายของซิสโก้ที่ติดตั้งใช้งานอยู่จริงในองค์กรมาทำการทดลอง และทดสอบกับซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) โดยมีขั้นตอนในการดำเนินการดังนี้

3.1 ประเภทของอุปกรณ์เครือข่ายที่ใช้ในการทดลอง

ในสารนิพนธ์ฉบับนี้ได้แบ่งประเภทอุปกรณ์เครือข่ายที่ใช้ในการทดลอง ตามลักษณะการให้บริการของอุปกรณ์เครือข่าย โดยแบ่งออกเป็น 3 กลุ่มดังนี้

3.1.1 อุปกรณ์เครือข่ายไร้สาย เป็นอุปกรณ์ที่ทำหน้าที่เป็นโครงสร้างหลักในการเชื่อมต่อระบบเครือข่ายภายในองค์กรเข้าไว้ด้วยกัน ได้แก่ สวิตช์ตามลำดับชั้นต่าง เช่น Core switch, Distribution switch และ Access switch

3.1.2 อุปกรณ์เครือข่ายไร้สาย เป็นอุปกรณ์ที่ทำหน้าที่ให้บริการเครือข่ายไร้สายกับผู้ใช้งาน โดยอุปกรณ์เครือข่ายไร้สายของซิสโก้ที่ใช้งานอยู่ในองค์กรจะเป็นแบบระบบควบคุมจากศูนย์กลาง (Centralize Controller Base)

3.1.2 อุปกรณ์เครือข่ายระยะไกล เป็นอุปกรณ์ที่มีหน้าที่ทำการเชื่อมต่อระบบเครือข่ายระยะไกลระหว่างสำนักงานใหญ่กับสาขาต่างๆขององค์กร ซึ่งก็คือ อุปกรณ์เครือข่ายเราเตอร์

3.2 สภาพแวดล้อมที่ใช้ในการทดสอบ

เนื่องจากต้องทำการเชื่อมต่อระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) เข้ากับระบบเครือข่ายขององค์กรที่ใช้งานอยู่จริงและทำการทดสอบกับอุปกรณ์เครือข่ายของซิสโก้ที่ติดตั้งใช้งานอยู่ในองค์กร โดยในการทดลอง และทดสอบนี้ได้แบ่งสภาพแวดล้อมออกเป็น 3 แบบตามลักษณะของเครือข่ายและอุปกรณ์เครือข่ายที่ใช้งาน ดังนี้

3.2.1 เครือข่ายสวิตช์ เป็นเครือข่ายโครงสร้างหลักในการเชื่อมต่อระบบเครือข่ายแต่ละ

เอกสารนี้เป็นทรัพย์สินที่ภายในองค์กรเข้าไว้ด้วยกัน ดังแสดงในรูปที่ 3.2 ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

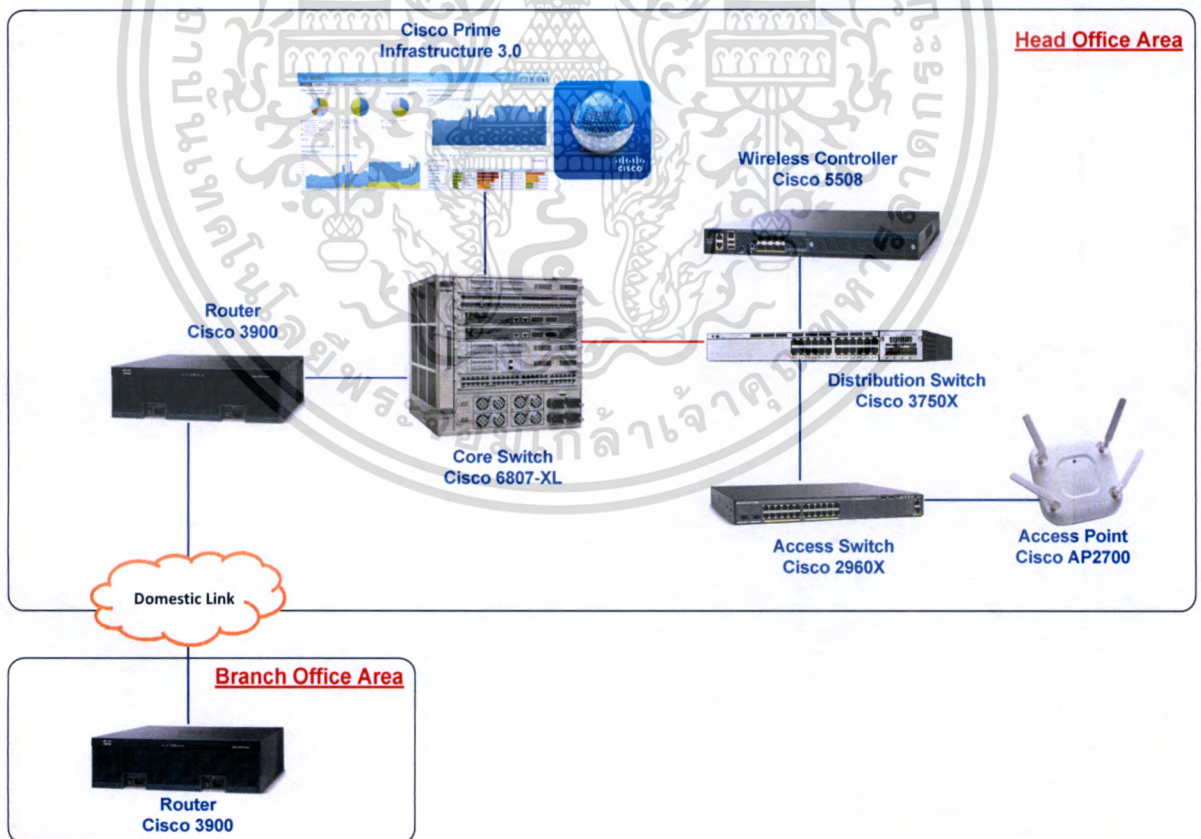
3.2.2 เครือข่ายไร้สาย เป็นเครือข่ายที่ติดตั้งและให้บริการเฉพาะพื้นที่ภายในองค์กร เพื่อรองรับการเชื่อมต่อกับเครื่องลูกข่ายที่ต้องการเครือข่ายไร้สาย ดังแสดงในรูปที่ 3.3

3.2.3 เครือข่ายเราเตอร์ เป็นเครือข่ายที่ใช้เชื่อมต่อระบบเครือข่ายระยะไกลระหว่างสำนักงานใหญ่กับสาขาต่างๆขององค์กร ดังแสดงในรูปที่ 3.4

3.3 แผนภาพแสดงการเชื่อมต่อระบบ

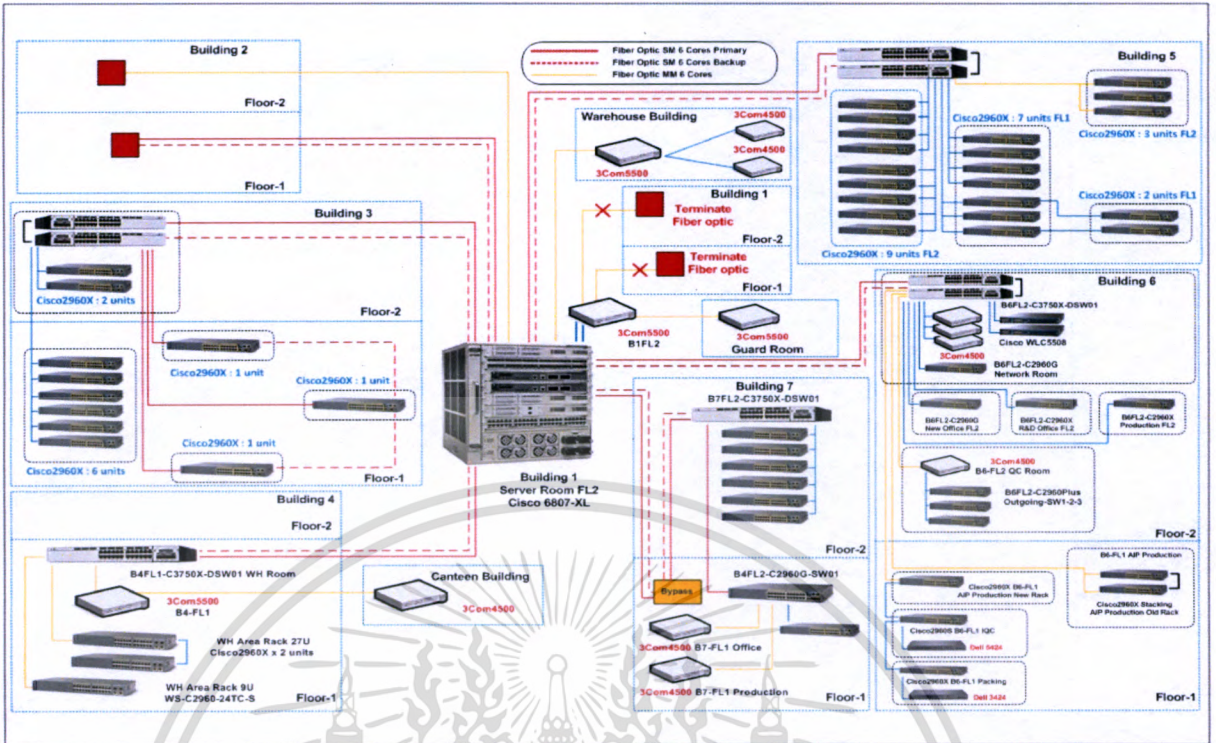
แผนภาพแสดงการเชื่อมต่อระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) เข้ากับระบบเครือข่ายขององค์กร ดังรูปที่ 3.1 ซึ่งประกอบด้วย

1. ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure 3.0)
2. อุปกรณ์เครือข่ายของซิสโก้ที่ติดตั้งใช้งานอยู่จริงในองค์กร ทั้ง 3 กลุ่ม คือ
 - อุปกรณ์เครือข่ายไร้สาย Core Switch, Distribution Switch และ Access Switch
 - อุปกรณ์เครือข่ายไร้สาย Cisco Wireless Controller และ Access Point
 - อุปกรณ์เครือข่ายระยะไกล Router

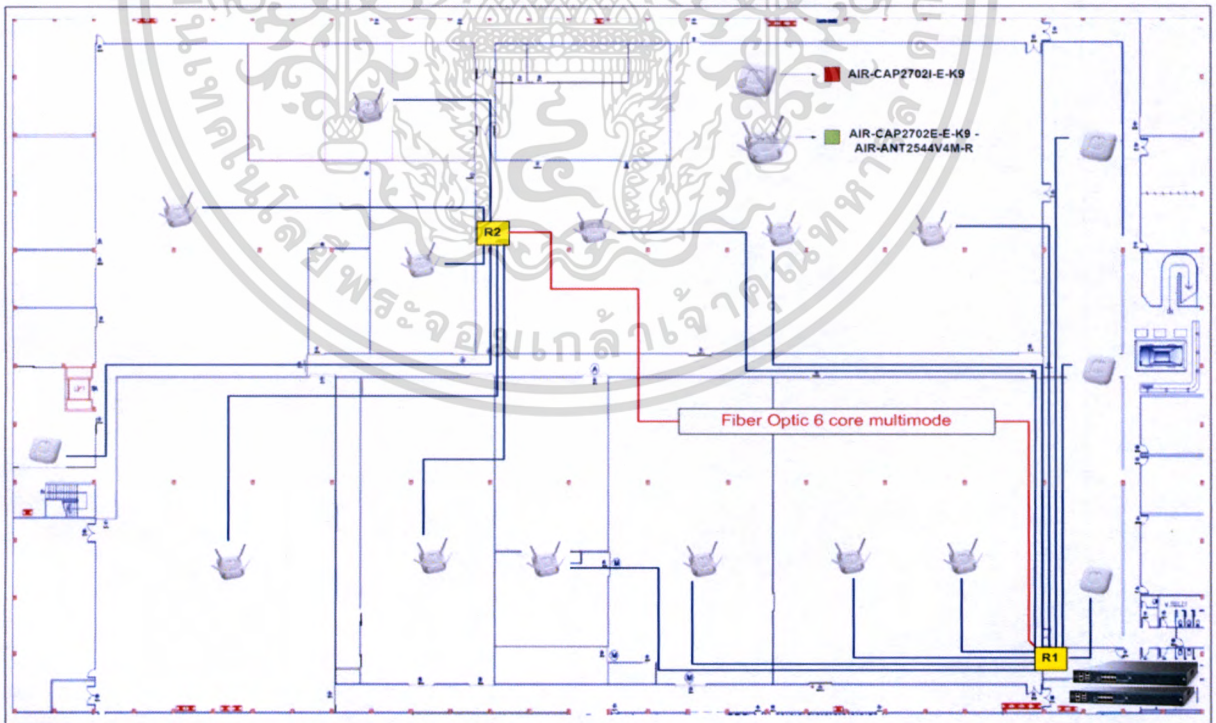


รูปที่ 3.1 แผนภาพแสดงการเชื่อมต่อระบบระบบเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

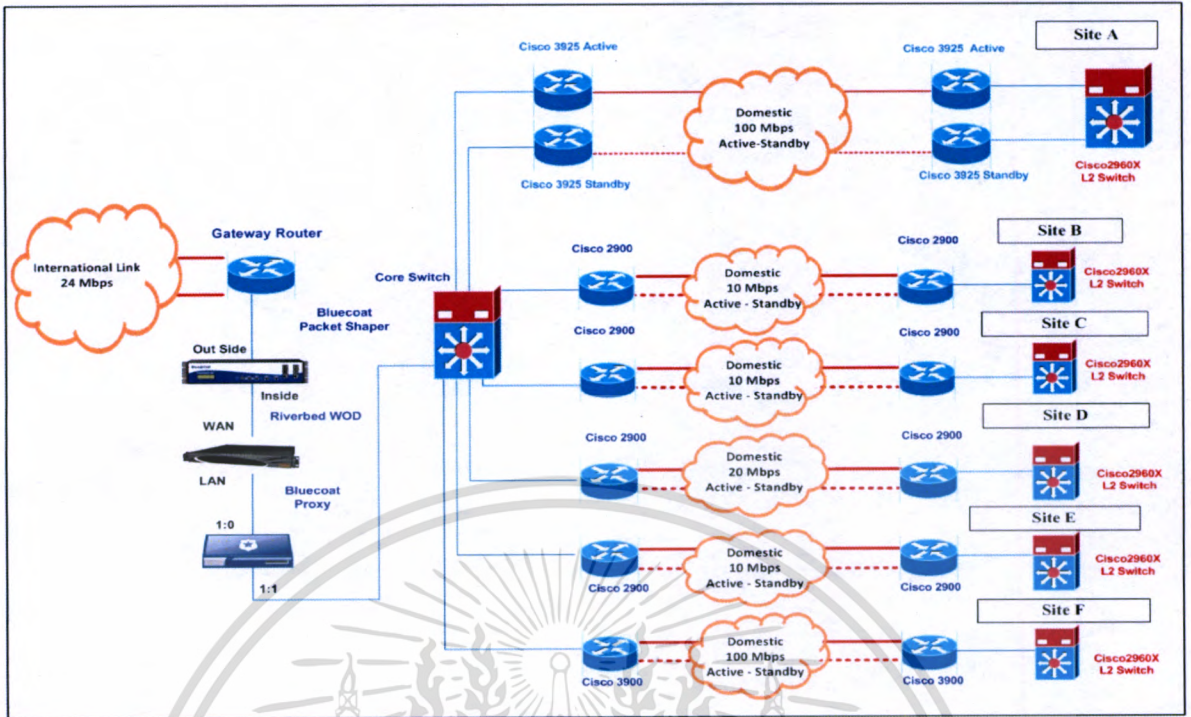


รูปที่ 3.2 แสดงเครือข่ายสวิตช์



รูปที่ 3.3 แสดงเครือข่ายไร้สาย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.4 แสดงเครือข่ายเราเตอร์

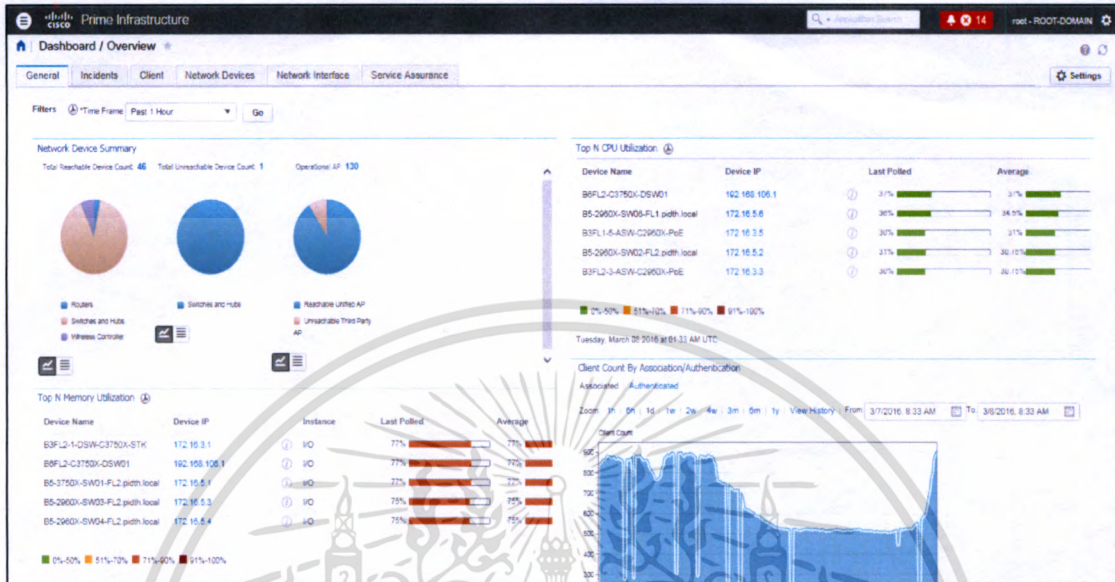
3.4 ขั้นตอนการดำเนินงาน

หลังจากติดตั้งและปรับแต่งค่าต่างๆของระบบบริหารจัดการเครือข่ายของซิสโก้ ผ่านทางคอมมานด์ไลน์ ที่ติดตั้งบน VMware เป็นที่เรียบร้อยแล้ว จะสามารถเข้าไปใช้งานระบบบริหารจัดการเครือข่ายของซิสโก้ผ่านทางเว็บไซต์ ดังรูปที่ 3.5 จะแสดงหน้าจอ Login เข้าสู่ระบบของระบบบริหารจัดการเครือข่ายของซิสโก้



เอกสารนี้เป็นเอกสารรูปที่ 3.5 แสดงหน้าจอ Login เข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้ โยชน์ด้านการค้า ไม่ว่าการณ์ใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อทำการ Login เข้าสู่ระบบเรียบร้อยแล้ว จะแสดงหน้าจอแสดงภาพรวมของระบบบริหารจัดการเครือข่ายของซิสโก้ดังรูปที่ 3.6 ซึ่งจะแสดงสถานะโดยรวมของอุปกรณ์ในระบบเครือข่าย



รูปที่ 3.6 แสดงหน้าจอภาพรวมของระบบบริหารจัดการเครือข่ายของซิสโก้

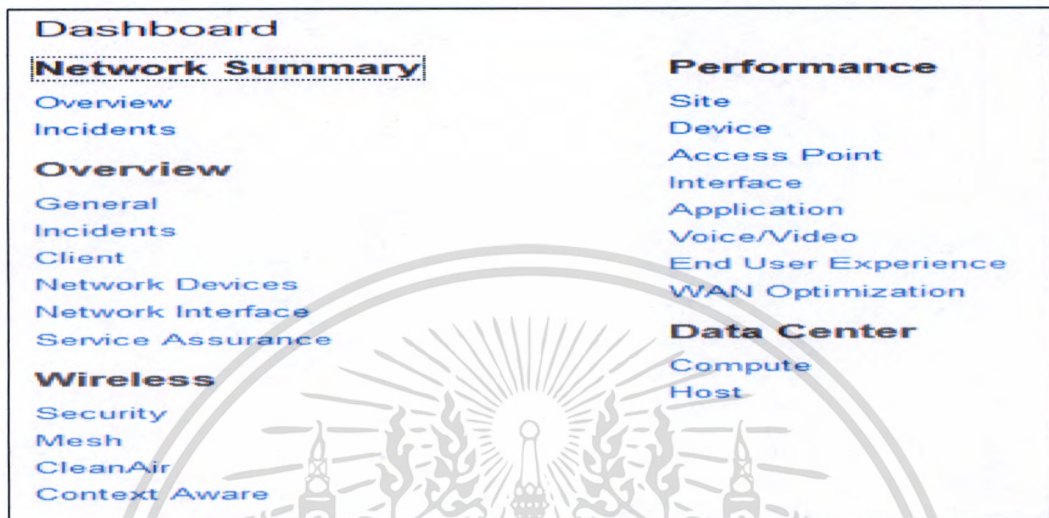
ลักษณะตัวเลือกของระบบบริหารจัดการเครือข่ายของซิสโก้จะแบ่งออกเป็น 8 หัวข้อหลัก ดังรูปที่ 3.7 โดยแต่ละตัวเลือกจะมีหัวข้อย่อยตามลักษณะงานด้านการบริหารจัดการเครือข่ายดังนี้



รูปที่ 3.7 แสดงหน้าจอตัวเลือกหลักของระบบบริหารจัดการเครือข่ายของซิสโก้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับนักเรียนเพื่อการศึกษเท่านั้น เมื่อผู้ใดเห็นไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Dashboard จะแสดงในส่วนของภาพรวมของอุปกรณ์ในระบบเครือข่ายทั้งที่เป็นแบบไร้สาย แบบไร้สาย และระยะไกลทำให้ผู้ดูแลระบบสามารถเข้าดูภาพรวมที่เกิดขึ้นบนระบบเครือข่ายได้อย่างสะดวกและรวดเร็ว ดังรูปที่ 3.8



รูปที่ 3.8 แสดงหน้าจอตัวเลือก Dashboard ของระบบบริหารจัดการเครือข่ายของซิสโก้

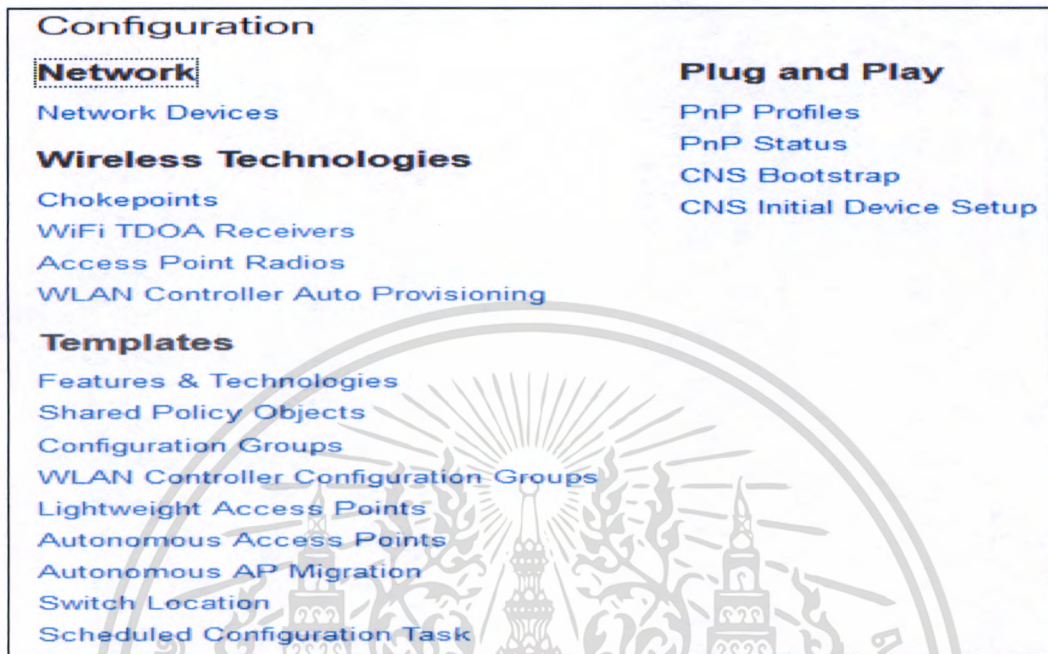
Monitor จะแสดงรายละเอียดสถานะของตัวอุปกรณ์เครือข่าย เพื่อให้สามารถดูสถานะของอุปกรณ์เครือข่าย เช่น CPU, Memory และรายละเอียดอื่นๆของอุปกรณ์เครือข่าย ดังรูปที่ 3.9



รูปที่ 3.9 แสดงหน้าจอตัวเลือก Monitor ของระบบบริหารจัดการเครือข่ายของซิสโก้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับกรใช้งานเพื่อการศึกษเท่านั้น ไม่อนุญาตให้นำไปเผยแพร่บนสื่อออนไลน์ การนำเอกสารนี้ไปใช้โดยไม่ผ่านการอนุญาตจากเจ้าของเอกสารถือเป็นการละเมิดลิขสิทธิ์และต้องแจ้งถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Configuration จะเป็นส่วนที่ดูแลและบริหารจัดการเกี่ยวกับค่าการติดตั้งบนตัวอุปกรณ์ โดยสามารถเข้าไปแก้ไข ปรับเปลี่ยนและจัดเก็บค่าต่างๆบนตัวอุปกรณ์เครือข่ายได้ ดังรูปที่ 3.10



รูปที่ 3.10 แสดงหน้าจอตัวเลือก Configuration ของระบบบริหารจัดการเครือข่ายของซิสโก้

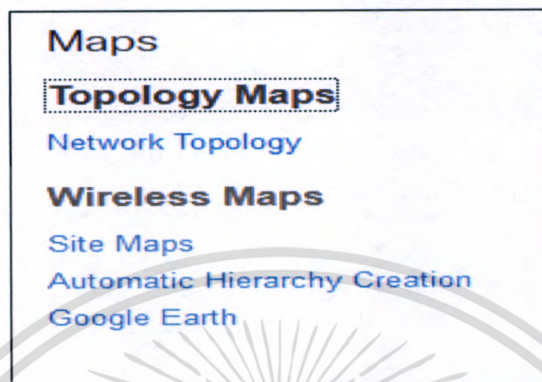
Inventory จะเป็นส่วนที่ดูแลและบริหารจัดการเกี่ยวกับจำนวนอุปกรณ์ที่ใช้กับระบบบริหารจัดการเครือข่ายของซิสโก้ ดังรูปที่ 3.11 โดยส่วนนี้เป็นส่วนเริ่มต้นในการใช้ระบบบริหารจัดการเครือข่ายของซิสโก้เพราะต้องทำการเพิ่มอุปกรณ์เครือข่ายเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้ผ่านทางตัวเลือก Inventory นี้



รูปที่ 3.11 แสดงหน้าจอตัวเลือก Inventory ของระบบบริหารจัดการเครือข่ายของซิสโก้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Maps จะเป็นส่วนที่ดูแลและบริหารจัดการเกี่ยวกับแผนภาพการเชื่อมต่อของอุปกรณ์เครือข่าย ที่ใช้กับระบบบริหารจัดการเครือข่ายของซิสโก้ ดังรูปที่ 3.12 โดยในส่วนของแผนภาพสามารถแสดงการเชื่อมต่อของอุปกรณ์เครือข่ายในแบบต่างๆได้



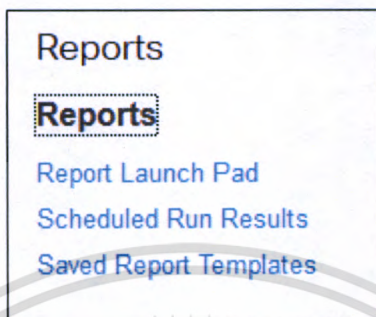
รูปที่ 3.12 แสดงหน้าจอตู้เลือก Maps ของระบบบริหารจัดการเครือข่ายของซิสโก้

Services จะเป็นส่วนที่ดูแลและบริหารจัดการเกี่ยวกับการแสดงข้อมูลบัญชีการใช้งานบนเครือข่ายของผู้ใช้งานบนอุปกรณ์เครือข่าย ที่ใช้กับระบบบริหารจัดการเครือข่ายของซิสโก้ ดังรูปที่ 3.13 โดยมีความสามารถในการทำงานร่วมกับโปรโตคอลวิเคราะห์เครือข่ายที่ติดตั้งอยู่ในอุปกรณ์เครือข่ายของซิสโก้ เช่น Net-Flow, Flexible Net-Flow, NBAR2 และ Application Visibility Control (AVC) และนำข้อมูลมาแสดงผลในรูปแบบของแผนภูมิได้



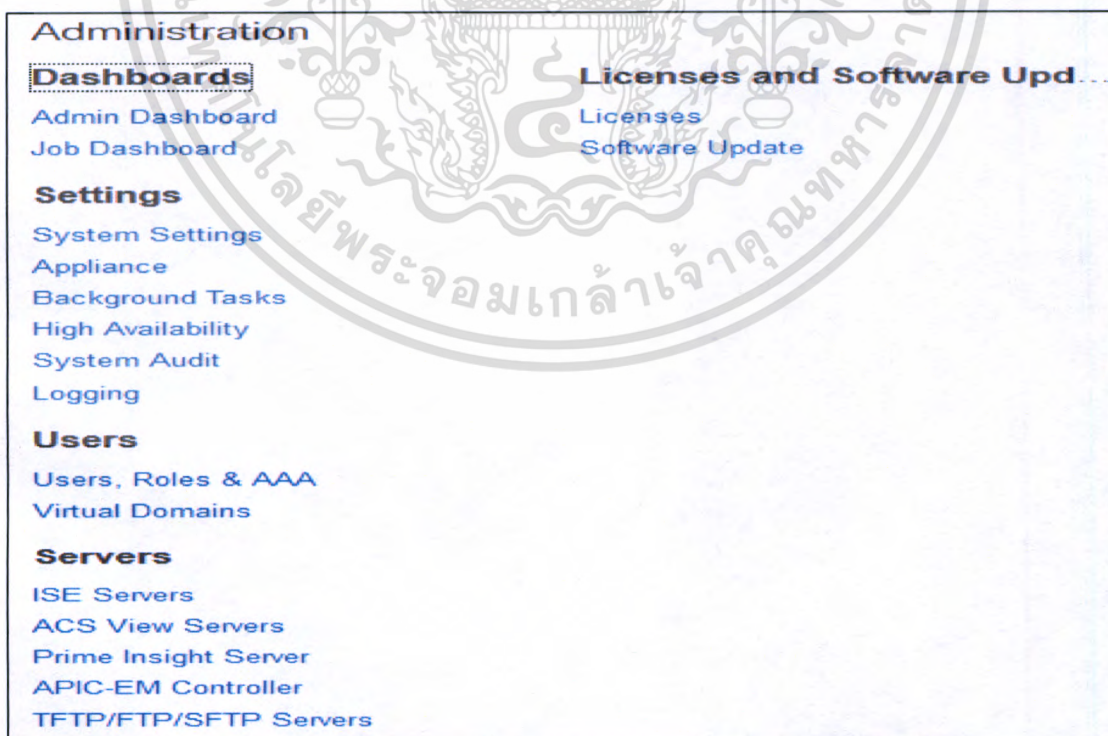
เอกสารนี้เป็นทรัพย์สินของ Cisco และแสดงหน้าจอตู้เลือก Services ของระบบบริหารจัดการเครือข่ายของซิสโก้ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Reports จะเป็นส่วนที่ดูแลและบริหารจัดการเกี่ยวกับรูปแบบรายงานของระบบบริหารจัดการเครือข่ายของซิสโก้ ดังรูปที่ 3.14 โดยในส่วนของรายงานนี้ สามารถสร้างรูปแบบรายงานตามที่เราต้องการและสามารถตั้งกำหนดเวลาในการสร้างรายงานได้



รูปที่ 3.14 แสดงหน้าจอตัวเลือก Reports ของระบบบริหารจัดการเครือข่ายของซิสโก้

Administration จะเป็นส่วนที่ดูแลและบริหารจัดการเกี่ยวกับการตั้งค่าต่างๆ เช่น การดูข้อมูลจำนวน License ที่ใช้งานและการปรับปรุงรุ่นซอฟต์แวร์ของระบบบริหารจัดการเครือข่ายของซิสโก้ ดังรูปที่ 3.15



เอกสารนี้ **รูปที่ 3.15** แสดงหน้าจอตัวเลือก Administration ของระบบบริหารจัดการเครือข่ายของซิสโก้
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อได้ศึกษาและทำความเข้าใจตัวเลือกต่างๆของระบบบริหารจัดการเครือข่ายของซิสโก้แล้ว ขั้นตอนต่อไปคือการเพิ่มอุปกรณ์เครือข่ายที่ต้องการจะบริหารจัดการเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้ ซึ่งขั้นตอนนี้เป็นขั้นตอนที่สำคัญ โดยต้องเตรียมข้อมูลของอุปกรณ์เครือข่ายของซิสโก้ดังนี้ หมายเลขเครือข่าย, คอมมูนิตี (Community) ของเอ็นเอ็มพีโปรโตคอลเอสเอ็นเอ็มพี (SNMP), Username และ Password สำหรับเข้าสู่อุปกรณ์ผ่านทาง Telnet และเว็บไซต์โดยเข้าไปที่ตัวเลือก Inventorys และไปที่ Add Devices จากนั้นใส่ข้อมูลต่างๆของอุปกรณ์เครือข่ายที่เตรียมไว้เมื่อใส่ข้อมูลเรียบร้อยแล้ว ระบบบริหารจัดการเครือข่ายของซิสโก้จะทำการตรวจสอบข้อมูลกับอุปกรณ์เครือข่าย ถ้าข้อมูลที่ใส่เข้าไปถูกต้องและครบถ้วน ระบบบริหารจัดการเครือข่ายของซิสโก้จะสามารถเพิ่มอุปกรณ์เครือข่ายเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้ได้ ซึ่งการทำวิธีนี้จะเป็นการเพิ่มอุปกรณ์เครือข่ายเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้แบบทีละตัว ดังรูปที่ 3.16

รูปที่ 3.16 การเพิ่มอุปกรณ์เครือข่ายเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้แบบทีละตัว

ถ้าในกรณีที่เป็นระบบเครือข่ายที่มีขนาดใหญ่และมีอุปกรณ์เครือข่ายจำนวนมาก ระบบบริหารจัดการเครือข่ายของซิสโก้มีเครื่องมือที่ช่วยอำนวยความสะดวกในการค้นหาและเพิ่มอุปกรณ์เครือข่ายเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้ ซึ่งจะช่วยลดเวลาและเพิ่มความสะดวกให้กับผู้ดูแลระบบเครือข่ายได้ โดยเข้าไปที่ตัวเลือก Inventorys และเลือกที่ตัวเลือก

Discovery ดังรูปที่ 3.17 สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
 เอกสารนี้เป็นเอกสารลิขสิทธิ์ของ Cisco Systems, Inc. ห้ามเผยแพร่หรือทำซ้ำโดยไม่ได้รับอนุญาตจาก Cisco Systems, Inc. หากต้องการข้อมูลเพิ่มเติม กรุณาติดต่อฝ่ายขายของ Cisco Systems, Inc. หรือไปที่ www.cisco.com ไม่ว่าการพิมพ์ขึ้นลิขสิทธิ์ของ Cisco Systems, Inc. หรือทำซ้ำโดยไม่ได้รับอนุญาตจาก Cisco Systems, Inc. หากต้องการข้อมูลเพิ่มเติม กรุณาติดต่อฝ่ายขายของ Cisco Systems, Inc. หรือไปที่ www.cisco.com

Discovery Jobs

Selected 1 / Total 8

Show Quick Filter

Name	Status	Start Time	End Time	Discovery Settings	Reachable	Filtered	Unreachab
Job_Discovery_12_56_52_962_2_11_2015	SUCCESS	2015-Nov-02 05:56:53	2015-Nov-02 05:57:00	PISCTH	0	0	20
Job_Discovery_12_58_23_593_2_11_2015	SUCCESS	2015-Nov-02 05:58:23	2015-Nov-02 05:58:30	PISCTH	0	0	19
Job_Discovery_13_1_31_502_2_11_2015	SUCCESS	2015-Nov-02 06:01:31	2015-Nov-02 06:03:12	PISCTH	16	0	3
Job_Discovery_13_53_22_514_2_11_2015	SUCCESS	2015-Nov-02 06:53:22	2015-Nov-02 06:53:30	PAPMRTH	12	0	0

Discovery Jobs Instances of Job_Discovery_12_56_52_962_2_11_2015

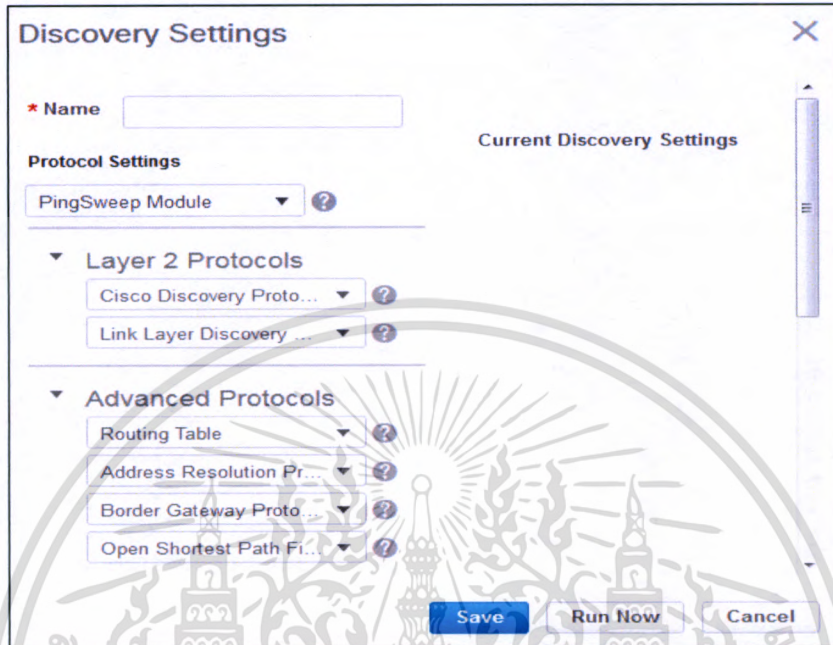
Name	Status	Start Time	End Time	Discovery Settings	Reachable	Filtered	Unreachable
Job_Discovery_12_56_52_962_2_11_2015	SUCCESS	2015-Nov-02 05:56:53	2015-Nov-02 05:57:00	PISCTH	0	0	20

รูปที่ 3.17 แสดงการค้นหาอุปกรณ์เครือข่ายของระบบบริหารจัดการเครือข่ายของซิสโก้

ในส่วนของ Discovery จะมีหน้าจอให้ผู้ใช้สามารถใส่ค่าเหมือนกับการเพิ่มอุปกรณ์ทีละตัวแต่จะสามารถใส่ค่าหมายเลขเครือข่ายเป็นช่วงของหมายเลขเครือข่ายตามที่ต้องการและสามารถกำหนดตารางเวลาในการการค้นหาและเพิ่มอุปกรณ์เครือข่ายเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้ดังรูปที่ 3.18 เพราะการค้นหาและเพิ่มอุปกรณ์เครือข่ายเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้ กับระบบเครือข่ายที่มีขนาดใหญ่และมีอุปกรณ์เครือข่ายที่มีจำนวนมาก อาจส่งผลทำให้เกิดปริมาณข้อมูลที่อยู่บนเครือข่ายเพิ่มมากขึ้นและทำให้เกิดความคับคั่งบนระบบเครือข่ายขึ้นได้ รวมถึงทำให้ทรัพยากรบนตัวอุปกรณ์เครือข่าย เช่น CPU, Memory จะถูกใช้งานเพิ่มมากขึ้นด้วย ซึ่งอาจส่งผลกระทบต่อสถานะของอุปกรณ์เครือข่ายและระบบเครือข่ายโดยรวม ดังนั้นจึงควรทำการการค้นหาและเพิ่มอุปกรณ์เครือข่ายเป็นช่วงของค่าหมายเลขเครือข่ายที่มีจำนวนไม่มาก เช่น อาจจะเริ่มทีละ 25-50 หมายเลขเครือข่ายเป็นต้น และควรทำการค้นหาและเพิ่มอุปกรณ์เครือข่ายเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้ในช่วงเวลาที่มีผู้ใช้งานเครือข่ายน้อย เพื่อป้องกันผลกระทบที่อาจจะเกิดกับระบบเครือข่ายได้ โดยระบบบริหารจัดการเครือข่ายของซิสโก้มีเครื่องมือให้ผู้ใช้สามารถกำหนดตารางเวลาในการค้นหาและเพิ่มอุปกรณ์เครือข่ายได้ โดยเมื่อ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ถึงตามกำหนดเวลาที่ตั้งค่าไว้ ระบบบริหารจัดการเครือข่ายของซิสโก้จะทำการค้นหาและเพิ่มอุปกรณ์เครือข่ายให้อัตโนมัติ ดังรูปที่ 3.19



รูปที่ 3.18 การตั้งค่าค้นหาและเพิ่มอุปกรณ์เครือข่าย

Administration / Dashboards / Job Dashboard / Job_Discovery_9_26_35_393_10_11_2015

Recurrence None
Description Immediate_Run_Discovery

Showing latest 5 Job instances [Show All](#) Total 1

Show All

Run ID	Status	Duration (hh:mm:ss)	Start Time	Completion Time
4842827	Success	00:07:13	2015-11-10 02:26	2015-11-10 02:33

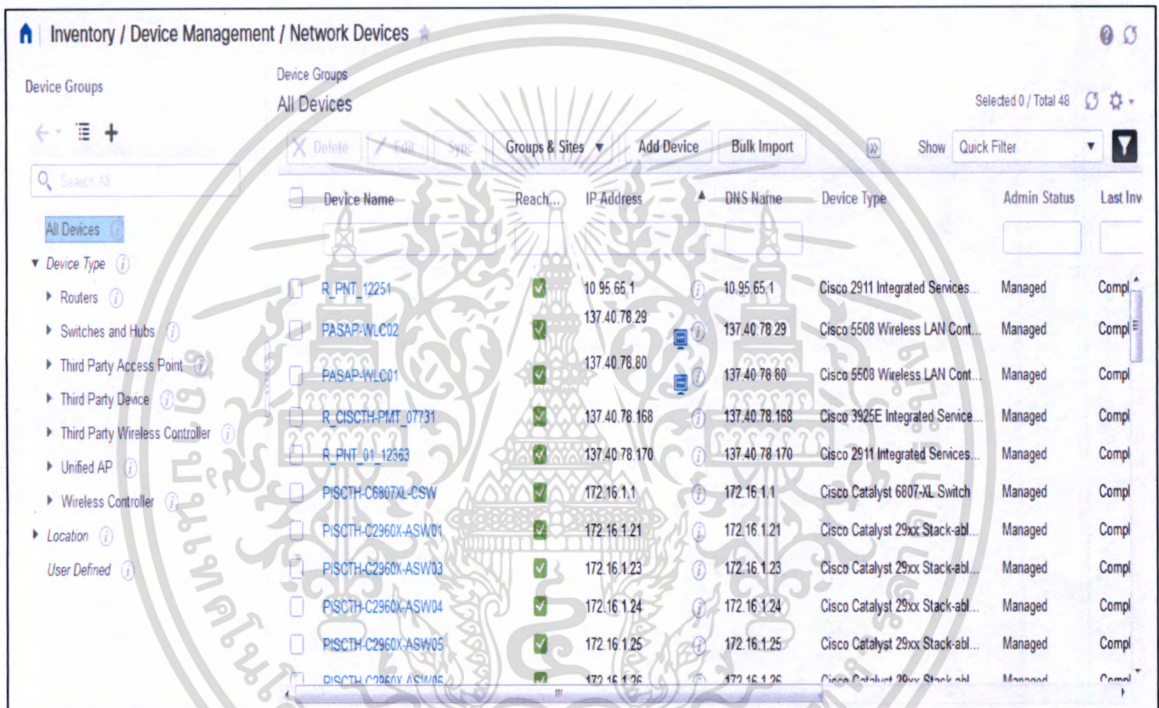
Reachable Filtered Unreachable

Device IP	System Object ID	System Name	System Location	New Device
172.16.5.53	1.3.6.1.4.1.43.1.16.4.3.21	PIDTH-3Com4500-Spare	Marlborough, MA 01752 USA	Existing
172.16.1.26	1.3.6.1.4.1.9.1.1208	PISCTH-C2960X-ASW06		Existing
172.16.5.9	1.3.6.1.4.1.9.1.1208	PIDTH-WH-B4FL1-C2960X-AS...		Existing
172.16.6.4	1.3.6.1.4.1.43.1.16.4.3.21	B6-4500-PASAP-OutGoing-FL2	Marlborough, MA 01752 USA	New
172.16.6.102	1.3.6.1.4.1.9.1.1207	RFEL1-C2960X-ASW06		New

รูปที่ 3.19 แสดงผลการค้นหาและเพิ่มอุปกรณ์เครือข่ายตามกำหนดเวลา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อทำการเพิ่มอุปกรณ์เครือข่ายเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้เสร็จเรียบร้อยแล้ว จะสามารถเข้าไปดูรายการอุปกรณ์เครือข่ายดังรูปที่ 3.20 ระบบบริหารจัดการเครือข่ายของซิสโก้ จะแสดงรายละเอียดของอุปกรณ์เครือข่าย โดยจะสามารถจัดหมวดหมู่ แยกตามชื่อ ชนิดของ อุปกรณ์ โดยดูจากรายการของจำนวนอุปกรณ์ทั้งหมด พร้อมทั้งยังสามารถจัดเรียงลำดับตาม หมายเลขเครือข่าย หรือชื่อของอุปกรณ์เครือข่ายตามลำดับตัวอักษรได้ และมีตัวเลือกสำหรับการ ค้นหาตามชื่อหรือหมายเลขเครือข่าย เพื่อให้ผู้ใช้งานทำการการค้นหาอุปกรณ์เครือข่ายได้ง่ายและ สะดวกรวดเร็ว



Device Name	Reach...	IP Address	DNS Name	Device Type	Admin Status	Last Inv
R_PNT_12251	✓	10.95.65.1	10.95.65.1	Cisco 2911 Integrated Services...	Managed	Compl
PASAP-WLC02	✓	137.40.78.29	137.40.78.29	Cisco 5508 Wireless LAN Cont...	Managed	Compl
PASAP-WLC01	✓	137.40.78.80	137.40.78.80	Cisco 5508 Wireless LAN Cont...	Managed	Compl
R_CISCTH-PMT_07731	✓	137.40.78.168	137.40.78.168	Cisco 3925E Integrated Service...	Managed	Compl
R_PNT_01_12563	✓	137.40.78.170	137.40.78.170	Cisco 2911 Integrated Services...	Managed	Compl
PISCTH-C6807X-CSW	✓	172.16.1.1	172.16.1.1	Cisco Catalyst 6807-XL Switch	Managed	Compl
PISCTH-C2960X-ASW01	✓	172.16.1.21	172.16.1.21	Cisco Catalyst 29xx Stack-abl...	Managed	Compl
PISCTH-C2960X-ASW03	✓	172.16.1.23	172.16.1.23	Cisco Catalyst 29xx Stack-abl...	Managed	Compl
PISCTH-C2960X-ASW04	✓	172.16.1.24	172.16.1.24	Cisco Catalyst 29xx Stack-abl...	Managed	Compl
PISCTH-C2960X-ASW05	✓	172.16.1.25	172.16.1.25	Cisco Catalyst 29xx Stack-abl...	Managed	Compl
PISCTH-C2960X-ASW06	✓	172.16.1.26	172.16.1.26	Cisco Catalyst 29xx Stack-abl...	Managed	Compl

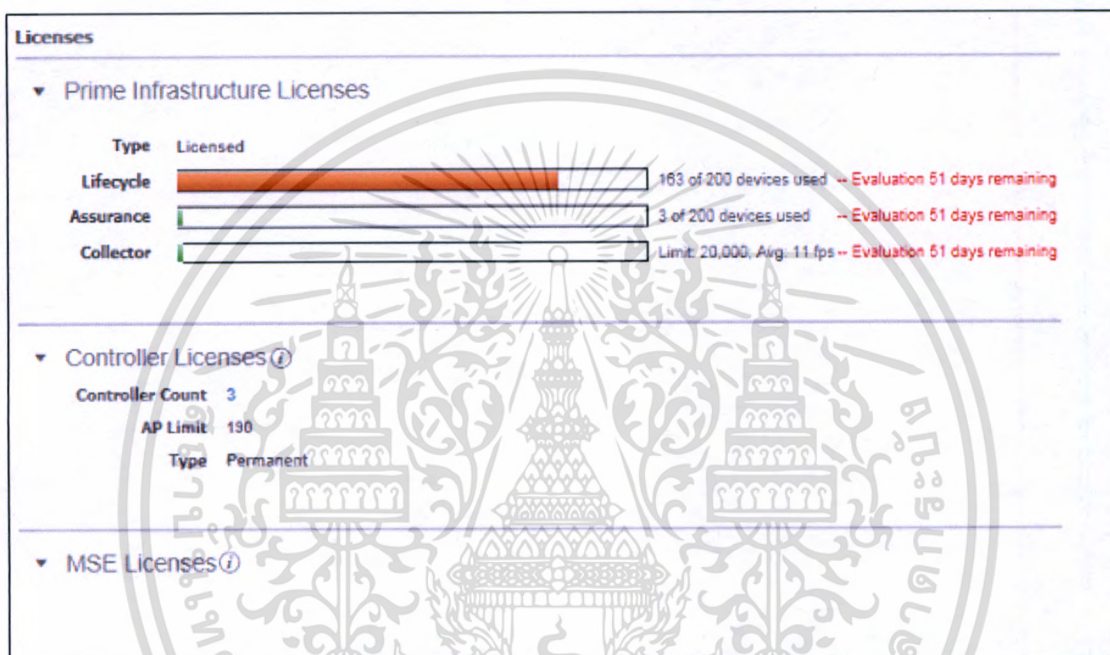
รูปที่ 3.20 แสดงรายการจำนวนอุปกรณ์เครือข่าย

เมื่อทำการเพิ่มจำนวนอุปกรณ์เครือข่ายในระบบบริหารจัดการเครือข่ายของซิสโก้ตามที่ ต้องการเรียบร้อยแล้ว ผู้ใช้งานสามารถตรวจสอบจำนวนของ License ของระบบบริหารจัดการเครือข่าย ของซิสโก้ได้โดยเข้าไปที่ตัวเลือก Administrations ซึ่งจะมีส่วนที่ดูแลและบริหารจัดการเกี่ยวกับการ ข้อมูลจำนวน License ของระบบบริหารจัดการเครือข่ายของซิสโก้ ดังรูปที่ 3.21 จะแสดงจำนวน License ที่ได้ทำการเพิ่มอุปกรณ์เครือข่ายเข้าไปในระบบบริหารจัดการเครือข่ายของซิสโก้โดยการ นับจำนวน License ของระบบบริหารจัดการเครือข่ายของซิสโก้จะแบ่งเป็น 2 แบบคือ

Lifecycle จะเป็น License ที่นับตามจำนวนตัวอุปกรณ์เครือข่ายที่เพิ่มเข้าไปในระบบ บริหารจัดการเครือข่ายของซิสโก้ โดยอุปกรณ์เครือข่ายหนึ่งตัว จะนับเป็นหนึ่ง License

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น เมื่อนำมาใช้ในเชิงพาณิชย์หรือการดำเนินงานอื่นใดโดยไม่ได้รับอนุญาตจากเจ้าของเอกสารจะถือว่าผิดกฎหมายและไม่อาจรับผิดชอบได้ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Assurance จะเป็น License ที่นับตามจำนวนตัวอุปกรณ์เครือข่ายที่มีความสามารถในการให้ข้อมูลโปรโตคอลวิเคราะห์เครือข่ายที่ติดตั้งอยู่ในอุปกรณ์เครือข่ายของซิสโก้ เช่น Net-Flow, Flexible Net-Flow, NBAR2 และ Application Visibility Control (AVC) เมื่อทำการเปิดการใช้งานฟังก์ชันเหล่านี้บนอุปกรณ์เครือข่ายที่มีความสามารถให้ข้อมูลโปรโตคอลวิเคราะห์เครือข่ายและถ้าต้องการให้ระบบบริหารจัดการเครือข่ายของซิสโก้ทำการรับและแสดงผลข้อมูลจะต้องใช้ Assurance License นี้ โดยอุปกรณ์เครือข่ายหนึ่งตัว จะนับเป็นหนึ่ง License



รูปที่ 3.21 แสดงจำนวน License อุปกรณ์เครือข่ายของระบบบริหารจัดการเครือข่ายของซิสโก้

เมื่อเข้าใจภาพรวมและการทำงานของระบบบริหารจัดการเครือข่ายของซิสโก้ดังที่กล่าวมาเบื้องต้นแล้ว ขั้นตอนต่อไปจะเป็นการทดลองและทดสอบความสามารถของระบบบริหารจัดการเครือข่ายของซิสโก้ โดยใช้หลักการของระบบบริหารจัดการเครือข่าย FCAPS Model และนำเอาระบบบริหารจัดการเครือข่ายของซิสโก้มาช่วยในการบริหารจัดการเครือข่ายที่ใช้งานอยู่ในปัจจุบัน รวมทั้งนำมาช่วยแก้ไขปัญหาและช่วยอำนวยความสะดวกในการทำงานให้กับผู้ดูแลระบบเครือข่าย เพื่อเพิ่มประสิทธิภาพในการทำงานและการบริหารจัดการเครือข่ายให้ดียิ่งขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

ผลการทดลอง

เนื่องจากระบบบริหารจัดการเครือข่ายของซิสโก้มีฟังก์ชันสนับสนุนการทำงานที่ช่วยในการบริหารจัดการเครือข่ายที่หลากหลาย เพื่อเป็นเกณฑ์ในการทดลองและวัดผลความสามารถของระบบบริหารจัดการเครือข่ายของซิสโก้ ผู้จัดทำได้นำเอาโมเดลมาตรฐานในการบริหารจัดการเครือข่าย (FCAPS Model) ทั้ง 5 ด้าน รวมถึงปัญหาในการบริหารจัดการเครือข่ายที่เกิดขึ้นในองค์กรมาใช้ทดลองและวัดผลในแต่ละด้านของระบบบริหารจัดการเครือข่ายของซิสโก้ดังนี้

4.1 การจัดการความผิดพลาด (Fault Management)

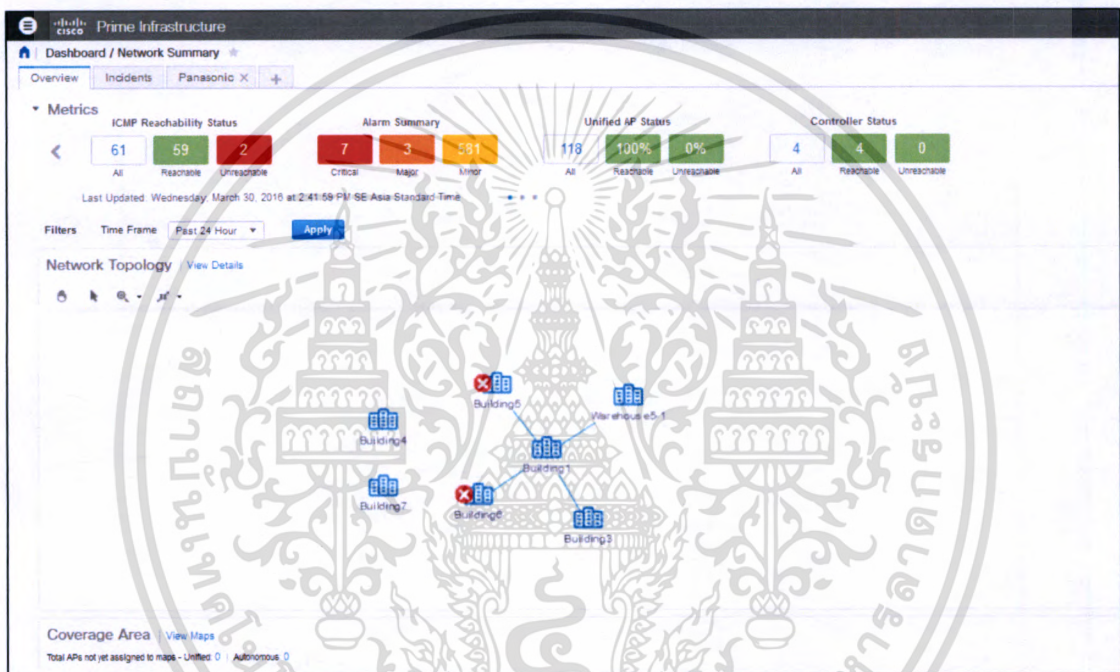
เนื่องจากระบบเครือข่ายที่ดีจะต้องอยู่ในสภาพพร้อมใช้งานตลอดเวลา เมื่อระบบเกิดปัญหาหรือความผิดพลาดขึ้น จะอาจส่งผลทำให้ระบบเครือข่ายหยุดการให้บริการ หรือทำให้การบริการไม่ต่อเนื่องและไม่เต็มประสิทธิภาพ ซึ่งจะส่งผลกระทบต่อความน่าเชื่อถือของระบบเครือข่าย ดังนั้นผู้ดูแลระบบจะต้องมีวิธีการป้องกันและบริหารจัดการความผิดพลาดที่เกิดขึ้นในระบบเครือข่ายให้มีประสิทธิภาพ เพื่อตอบสนองความต้องการของผู้ใช้ และสร้างความน่าเชื่อถือให้กับระบบเครือข่าย

ระบบบริหารจัดการเครือข่ายที่ดีจะต้องมีเครื่องมือที่คอยดูแล ตรวจสอบ เฝ้าระวังและเก็บรวบรวมข้อมูลความผิดพลาดที่เกิดขึ้นในระบบเครือข่ายได้อย่างมีประสิทธิภาพ เพื่อให้ผู้ดูแลระบบสามารถนำข้อมูลเหล่านั้นมาใช้วิเคราะห์และตัดสินใจ ในการแก้ปัญหาได้อย่างรวดเร็วที่สุด ซึ่งในระบบงานในปัจจุบันของผู้จัดทำ ยังไม่มีระบบหรือเครื่องมือที่ช่วยดูแล ตรวจสอบ เฝ้าระวังและเก็บรวบรวมข้อมูลความผิดพลาดที่เกิดขึ้นได้ในระบบเครือข่าย โดยต้องรอให้เกิดปัญหาเกิดขึ้นกับอุปกรณ์หรือระบบเครือข่ายก่อน ผู้ดูแลระบบจึงจะสามารถเข้าไปแก้ไขปัญหาได้ ซึ่งในบางครั้งต้องใช้เวลาในการหาสาเหตุและแก้ไขปัญหา ทำให้ส่งผลกระทบต่อผู้ใช้งาน ความน่าเชื่อถือของระบบเครือข่ายและส่งผลกระทบต่อธุรกิจขององค์กร ดังนั้นจึงได้ทำการทดลองและทดสอบระบบบริหารจัดการเครือข่ายของซิสโก้ในด้านการจัดการความผิดพลาดของระบบเครือข่ายดังนี้

4.1.1 การตรวจสอบสถานะต่างๆของภาพรวมเครือข่าย

เมื่อทำการเพิ่มอุปกรณ์เครือข่ายเข้าไปในระบบบริหารจัดการเครือข่ายของซิสโก้แล้ว ระบบบริหารจัดการเครือข่ายของซิสโก้จะทำการตรวจสอบสถานะ เฝ้าระวัง เก็บรวบรวมข้อมูล และความผิดพลาดที่เกิดขึ้นบนอุปกรณ์เครือข่าย ทำให้ผู้ดูแลระบบสามารถรับทราบข้อมูลสถานะของภาพรวมของเครือข่ายได้ เช่น สถานะของอุปกรณ์เครือข่าย ปริมาณการรับส่งข้อมูลบนอุปกรณ์เครือข่ายที่ใช้งานจริงในระบบเครือข่าย ประสิทธิภาพและความสามารถในการรองรับการใช้งาน

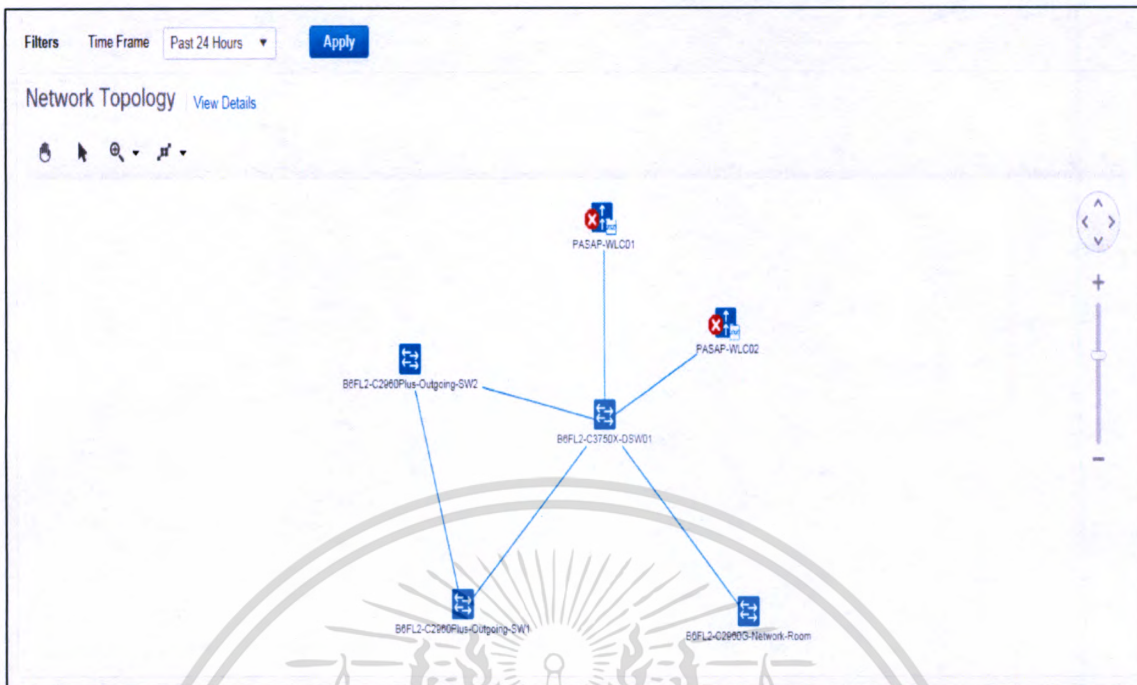
ของอุปกรณ์เครือข่าย การตรวจสอบสถานะของภาพรวมของเครือข่ายจากศูนย์กลางของระบบบริหารจัดการเครือข่ายของซิสโก้จะแสดงสถานะของอุปกรณ์และภาพรวมของระบบเครือข่ายที่เกิดขึ้น บนหน้าจอแสดงผลภาพรวมที่เป็นแบบแผนภูมิ ทำให้ผู้ดูแลระบบสามารถมองเห็นภาพรวมของระบบเครือข่ายและตรวจสอบสถานะของอุปกรณ์เครือข่ายได้ง่ายดังรูปที่ 4.1 เป็นหน้าจอแสดงผลภาพรวมของระบบเครือข่ายของระบบบริหารจัดการเครือข่ายของซิสโก้ โดยในหน้าจอแสดงผลภาพรวมของระบบเครือข่ายนี้ ผู้ดูแลระบบสามารถปรับแต่งตำแหน่งของแผนภูมิ รวมถึงเลือกแผนภูมิเพื่อนำมาแสดงผลที่หน้าจอหลักได้



รูปที่ 4.1 แสดงหน้าจอภาพรวมของระบบเครือข่าย

ในกรณีที่อุปกรณ์เครือข่ายเกิดปัญหาขึ้น เช่น เกิดการหยุดการทำงาน หรือมีการเริ่มต้นการทำงานใหม่ระบบบริหารจัดการเครือข่ายของซิสโก้จะแสดงผลที่เกิดขึ้นบนหน้าจอแสดงผลรวมดังรูปที่ 4.2 หรือสามารถดูจากหน้าจอรายการของอุปกรณ์เครือข่ายได้ดังรูปที่ 4.3 ซึ่งทำให้ทางผู้ดูแลระบบสามารถเข้าไปดูสถานะของอุปกรณ์เครือข่ายแต่ละประเภทได้อีกด้วย ช่วยให้ผู้ดูแลระบบเครือข่ายสามารถเห็นภาพรวมของเครือข่ายและสถานะของอุปกรณ์เครือข่ายทั้งหมดได้ง่าย ทำให้สามารถรับทราบปัญหาที่เกิดขึ้นและแก้ไขปัญหาได้อย่างรวดเร็วและตรงจุด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.2 แสดงหน้าจอสถานะของอุปกรณ์เครือข่ายที่เกิดปัญหา

Device Name	Reachability	IP Address	DNS Name	Device Type	Admin Status	Last Inventory Collect
PISCTH-C2960X-ASW01	✓	172.16.1.21	172.16.1.21	Cisco Catalyst 29xx Stack-abl...	Managed	Completed
PISCTH-C2960X-ASW03	✓	172.16.1.23	172.16.1.23	Cisco Catalyst 29xx Stack-abl...	Managed	Completed
PISCTH-C2960X-ASW04	✓	172.16.1.24	172.16.1.24	Cisco Catalyst 29xx Stack-abl...	Managed	Completed
PISCTH-C2960X-ASW05	✓	172.16.1.25	172.16.1.25	Cisco Catalyst 29xx Stack-abl...	Managed	Completed
PISCTH-C2960X-ASW05	✓	172.16.1.26	172.16.1.26	Cisco Catalyst 29xx Stack-abl...	Managed	Completed
PISCTH-C2960X-ASW07	✓	172.16.1.27	172.16.1.27	Cisco Catalyst 29xx Stack-abl...	Managed	Completed
PISCTH-C2960X-ASW08	✓	172.16.1.28	172.16.1.28	Cisco Catalyst 29xx Stack-abl...	Managed	Completed
PISCTH-C2960X-ASW09	✓	172.16.1.29	172.16.1.29	Cisco Catalyst 29xx Stack-abl...	Managed	Completed
PAPTH-Cisco2960G	✓	172.16.1.100	172.16.1.100	Cisco Catalyst 2960G-24TC S...	Managed	Completed
PITHC-HDVC-B1	✓	172.16.1.111	172.16.1.111	Cisco Catalyst 2960-24TC S...	Managed	Completed
PIDTH-HDVC-B5	✗	172.16.1.112	172.16.1.112	Cisco Catalyst 2960-24TC S...	Managed	Completed
B3FL2-1-DSW-C3750X-STK	✓	172.16.3.1	172.16.3.1	Cisco 3750 Stackable Switches	Managed	Completed
B3FL2-2-ASW-C2960X	✓	172.16.3.2	172.16.3.2	Cisco Catalyst 29xx Stack-abl...	Managed	Completed

รูปที่ 4.3 แสดงหน้าจอสถานะตามชนิดของอุปกรณ์เครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

นอกจากนั้นผู้ดูแลระบบสามารถเข้าไปดูสาเหตุของปัญหาที่ส่งมาจากตัวอุปกรณ์เครือข่าย เช่น Event log หรือ Syslog ได้ ทำให้ผู้ดูแลระบบสามารถนำข้อมูลนั้นไปวิเคราะห์เพื่อหาสาเหตุและทำการแก้ไขปัญหารวมทั้งหาทางป้องกันปัญหาที่จะเกิดขึ้นได้อีกด้วยดังรูปที่ 4.4 และ 4.5 แสดง Event log หรือ Syslog ที่เกิดขึ้นบนตัวอุปกรณ์เครือข่าย โดยจะแสดงเรียงลำดับตามวันและเวลาที่เกิดขึ้น สามารถจัดลำดับตามระดับความสำคัญของแต่ละเหตุการณ์และสาเหตุของปัญหาที่เกิดขึ้นกับอุปกรณ์เครือข่าย รวมถึงรายละเอียดของเหตุที่เกิดขึ้นได้อีกด้วย

The screenshot shows a network management interface with a tab for 'Alarms'. It displays a list of alarms, with one selected: 'Access point 'PASAP-RD_AP-10' associated with controller 'PASAP-WLC01' draws low power from Ethernet...'. The alarm is marked as 'Critical' and 'Not Acknowledged'. Below the alarm list, there is a 'General Info' section with details such as 'Failure Source', 'AP Details', 'Acknowledged', 'Category', 'Created', 'Modified', and 'Generated By'. A 'Messages' section also provides a detailed description of the failure: 'Access point 'PASAP-RD_AP-10' associated with controller 'PASAP-WLC01' draws low power from Ethernet. Failure reason: draws 15.4 watts from Ethernet.'

รูปที่ 4.4 แสดงรายละเอียดของปัญหาที่เกิดขึ้นกับอุปกรณ์เครือข่าย

The screenshot shows a network management interface with a tab for 'Events'. It displays a list of events with columns for 'Description', 'Failure Source', 'Timestamp', 'Severity', 'Category', 'Condition', and 'Correlated'. The events include various warnings and errors, such as 'Rogue AP' being no longer detected, 'Interference threshold violation', and 'Port' being down on a device. The severity levels range from 'Minor' to 'Critical'.

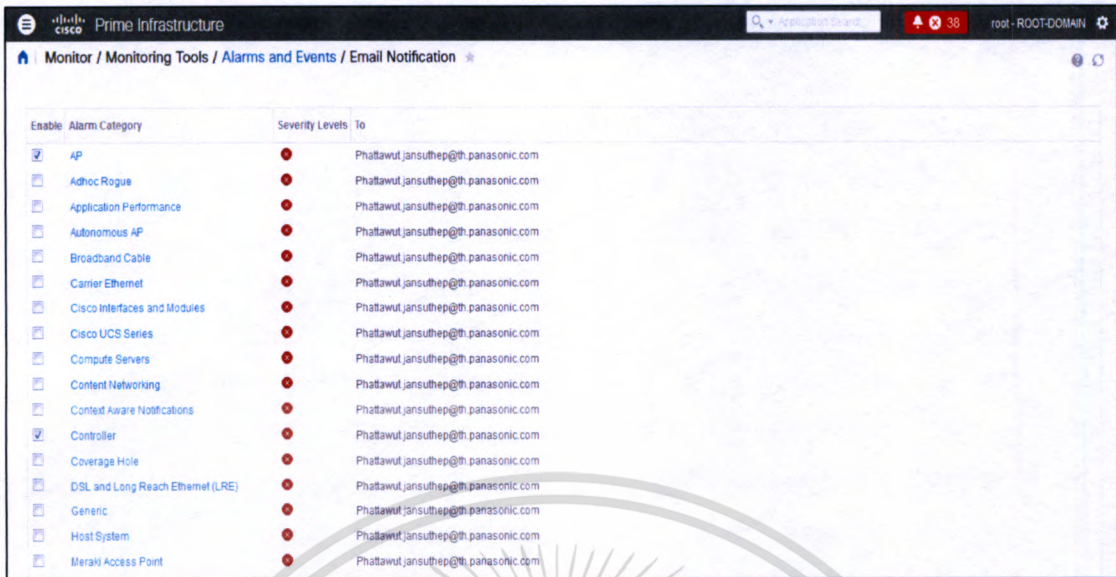
รูปที่ 4.5 แสดงลำดับเหตุการณ์ที่เกิดขึ้นกับอุปกรณ์เครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

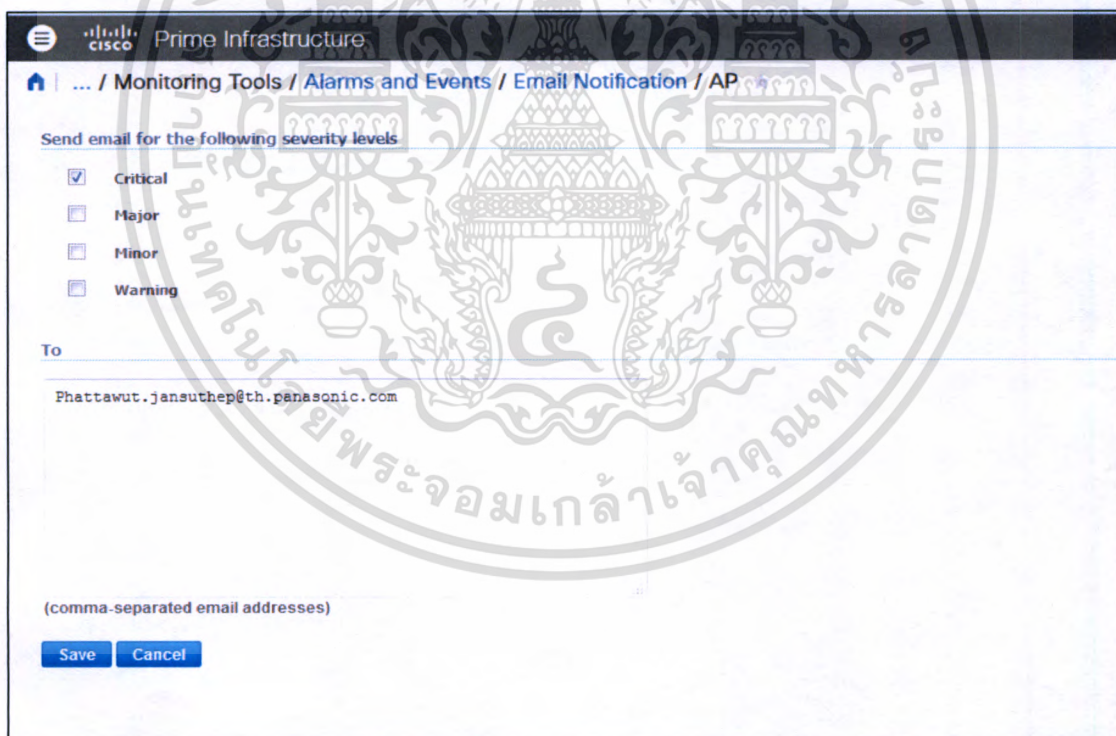
4.1.2 การแจ้งเตือนเมื่อพบความผิดปกติขึ้นในระบบ

นอกจากระบบบริหารจัดการเครือข่ายของซิสโก้จะสามารถแสดงผลเมื่อตรวจพบความผิดปกติที่เกิดขึ้นบนอุปกรณ์หรือระบบเครือข่ายได้แล้ว ในกรณีที่ผู้ดูแลระบบเครือข่ายไม่สามารถเข้ามาดูที่หน้าจอแสดงผลของระบบบริหารจัดการเครือข่ายของซิสโก้หรือเป็นช่วงนอกเวลาทำงานของผู้ดูแลระบบเครือข่าย ระบบบริหารจัดการเครือข่ายของซิสโก้สามารถแจ้งเตือนผู้ดูแลระบบเครือข่ายเมื่อระบบเครือข่ายหรืออุปกรณ์เครือข่ายเกิดปัญหาขึ้น โดยระบบบริหารจัดการเครือข่ายของซิสโก้สามารถแจ้งเตือนผู้ดูแลระบบเครือข่ายผ่านทางอีเมล โดยผู้ดูแลระบบเครือข่ายสามารถเลือกชนิดของอุปกรณ์เครือข่ายและระดับความสำคัญที่เกิดขึ้นเพื่อให้ระบบบริหารจัดการเครือข่ายของซิสโก้ทำการแจ้งเตือน ดังรูปที่ 4.6 แสดงการแจ้งเตือนตามชนิดของอุปกรณ์เครือข่าย และสามารถเลือกระดับความสำคัญที่เกิดขึ้น ดังรูปที่ 4.7 ทำให้ผู้ดูแลระบบเครือข่ายสามารถรับทราบข้อมูลเมื่อระบบเครือข่ายหรืออุปกรณ์เครือข่ายเกิดปัญหาได้ทันทีทุกเวลา และช่วยให้ผู้ดูแลระบบเครือข่ายสามารถแจ้งเตือนกับผู้บริหารและทีมงาน ทำให้สามารถแก้ไขปัญหาได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้น

เนื่องจากระบบบริหารจัดการเครือข่ายของซิสโก้จะมีรูปแบบที่กำหนดมาให้แล้วและไม่สามารถปรับเปลี่ยนได้ ถ้าเป็นระบบเครือข่ายขนาดใหญ่ที่มีอุปกรณ์เครือข่ายเป็นจำนวนมาก เมื่อมีเหตุการณ์ที่เกิดขึ้นกับอุปกรณ์เครือข่ายและระบบเครือข่ายก็จะมีปริมาณการแจ้งเตือนมากขึ้นตามไปด้วย ดังนั้นผู้ดูแลระบบเครือข่ายจึงควรเลือกการแจ้งเตือนผ่านทางอีเมลเฉพาะสาเหตุหรือเหตุการณ์ที่สำคัญและจำเป็นเท่านั้น เพราะถ้าไม่เลือกเฉพาะสาเหตุหรือเหตุการณ์ที่สำคัญและจำเป็น จะส่งผลทำให้มีจำนวนอีเมลที่ถูกส่งจากระบบบริหารจัดการเครือข่ายของซิสโก้ไปหาผู้ดูแลเครือข่ายเป็นจำนวนมาก รูปที่ 4.8 แสดงภาพตัวอย่างอีเมลการแจ้งเตือนของระบบบริหารจัดการเครือข่ายของซิสโก้ โดยเนื้อหาในอีเมลจะแสดงข้อมูลรายละเอียดของสาเหตุหรือเหตุการณ์ที่เกิดขึ้นกับอุปกรณ์เครือข่ายให้ผู้ดูแลระบบรับทราบข้อมูล โดยระบบบริหารจัดการเครือข่ายของซิสโก้จะทำการแจ้งเตือนสาเหตุหรือเหตุการณ์ที่เกิดขึ้นกับอุปกรณ์เครือข่ายทั้งตอนที่เกิดความผิดปกติขึ้นและหลังจากที่กลับเข้าสู่สภาวะปกติ ทำให้ผู้ดูแลระบบเครือข่ายทราบลำดับเหตุการณ์และช่วงเวลาที่เกิดปัญหาหรือความผิดปกติที่เกิดขึ้นกับอุปกรณ์เครือข่ายและระบบเครือข่ายได้

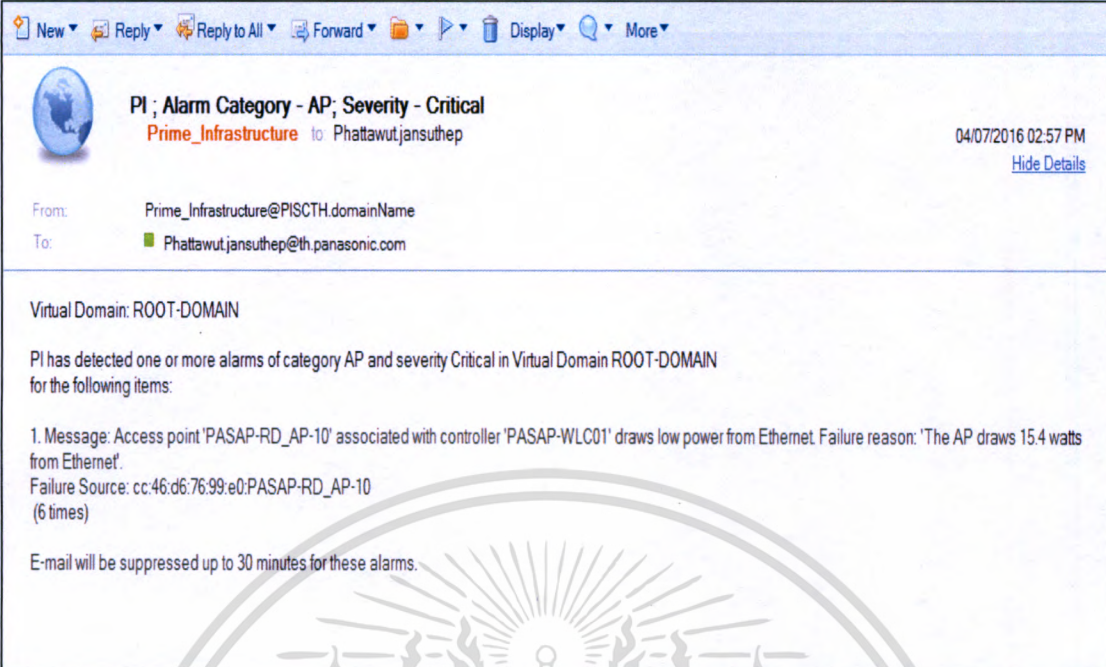


รูปที่ 4.6 แสดงชนิดของอุปกรณ์เครือข่ายที่ต้องการแจ้งเตือน





รูปที่ 4.7 แสดงหน้าจอการเลือกระดับความสำคัญเพื่อแจ้งเตือนผ่านอีเมล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



New Reply Reply to All Forward Display More

 **PI ; Alarm Category - AP; Severity - Critical**
Prime_Infrastructure to Phattawut.jansuthep 04/07/2016 02:57 PM
[Hide Details](#)

From: Prime_Infrastructure@PISCTH.domainName
 To:  Phattawut.jansuthep@th.panasonic.com

Virtual Domain: ROOT-DOMAIN

PI has detected one or more alarms of category AP and severity Critical in Virtual Domain ROOT-DOMAIN for the following items:

1. Message: Access point 'PASAP-RD_AP-10' associated with controller 'PASAP-WLC01' draws low power from Ethernet. Failure reason: 'The AP draws 15.4 watts from Ethernet'.
 Failure Source: cc:46:d6:76:99:e0:PASAP-RD_AP-10
 (6 times)

E-mail will be suppressed up to 30 minutes for these alarms.

รูปที่ 4.8 แสดงภาพตัวอย่างอีเมลการแจ้งเตือน

4.2 การจัดการค่าที่ตั้งไว้ (Configuration Management)

ค่าการติดตั้งบนอุปกรณ์เครือข่าย เป็นข้อมูลที่สำคัญที่ผู้ดูแลเครือข่ายต้องมีการเก็บรักษาและสำรองข้อมูลไว้ เพื่อความสะดวกในการปรับแต่ง เปลี่ยนแปลงค่าการทำงานของอุปกรณ์เครือข่าย ให้ถูกต้องเหมาะสม สอดคล้องกับหน้าที่ของแต่ละอุปกรณ์ในระบบเครือข่าย หรืออาจมีไว้เพื่อกู้คืนค่าการติดตั้ง เมื่อมีการเปลี่ยนอุปกรณ์เครือข่ายใหม่หรือกู้คืนทั้งระบบเมื่อระบบเครือข่ายเกิดปัญหาขึ้น ซึ่งงานด้านการจัดการค่าที่ตั้งไว้บนอุปกรณ์เครือข่ายเป็นงานที่เพิ่มภาระให้กับผู้ดูแลระบบเครือข่ายเป็นอย่างมาก เนื่องจากเป็นงานที่ต้องทำเป็นประจำและถ้าเป็นระบบเครือข่ายขนาดใหญ่ที่มีอุปกรณ์ในระบบเครือข่ายเป็นจำนวนมาก จะต้องใช้เวลาในการดำเนินการเก็บรวบรวมค่าที่ตั้งไว้บนอุปกรณ์เครือข่ายมากขึ้นตามไปด้วย และในบางครั้งอาจเกิดความผิดพลาดในการดำเนินการจัดเก็บรวบรวมค่าที่ตั้งไว้บนอุปกรณ์เครือข่ายขึ้นได้ เช่น เก็บข้อมูลซ้ำซ้อน เก็บข้อมูลทับของเดิม หรือ เก็บข้อมูลไม่ครบ เพราะผู้ดูแลระบบเครือข่ายจะต้องเข้าถึงอุปกรณ์เครือข่ายจากระยะไกลผ่านทาง Telnet เข้าไปที่อุปกรณ์เครือข่ายทีละตัว และทำการส่งคำสั่งเพื่อดำเนินการเก็บรวบรวมค่าที่ตั้งไว้บนอุปกรณ์เครือข่ายมาไว้ที่เครื่องคอมพิวเตอร์ของผู้ดูแลระบบเครือข่ายผ่านทางซอฟต์แวร์ที่ใช้โปรโตคอล Trivial File Transfer Protocol หรือ (TFTP)

จากปัญหาที่กล่าวมาผู้จัดทำได้นำเอาระบบบริหารจัดการเครือข่ายของซิสโก้มาทำการทดลองและทดสอบ เนื่องจากระบบบริหารจัดการเครือข่ายของซิสโก้มีเครื่องมือที่ช่วยผู้ดูแลระบบ

เครือข่ายในการจัดเก็บและกู้คืนค่าการติดตั้งให้กับอุปกรณ์เครือข่าย ได้สะดวกรวดเร็ว โดยสามารถทำการจัดเก็บค่าที่ติดตั้งไว้ได้เองอัตโนมัติ ตามช่วงของวันและเวลาที่ทางผู้ดูแลเครือข่ายได้กำหนดไว้ ทำให้สามารถบริหารจัดการค่าที่ติดตั้งไว้จากศูนย์กลางและครอบคลุมทุกอุปกรณ์ในระบบเครือข่ายดังนี้

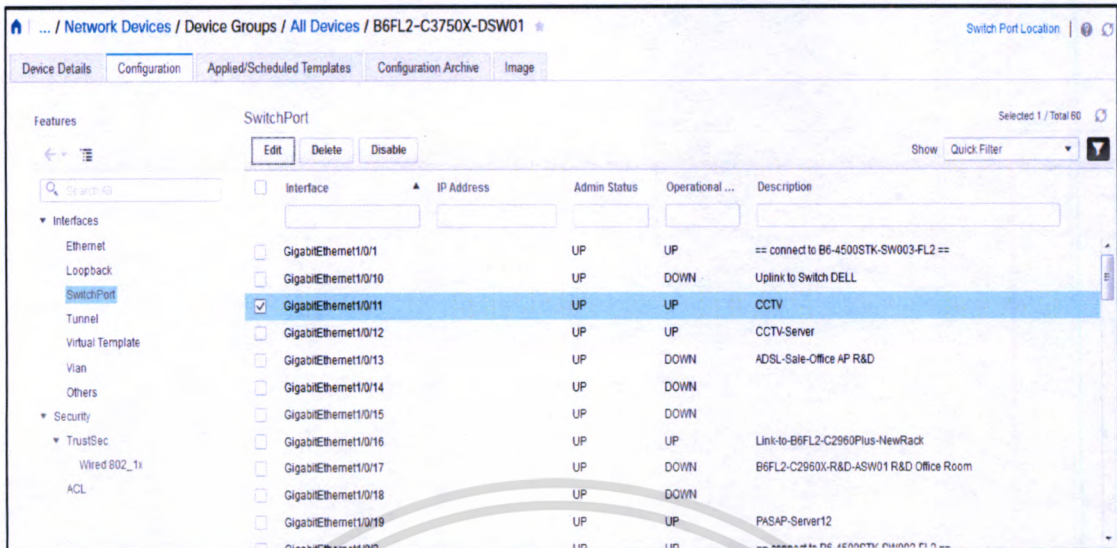
4.2.1 การจัดการค่าที่ติดตั้งบนอุปกรณ์เครือข่ายจากศูนย์กลาง

ระบบบริหารจัดการเครือข่ายของซิสโก้มีเครื่องมือที่สามารถเข้าไปแก้ไขและปรับเปลี่ยนค่าการติดตั้งใช้งานบนอุปกรณ์เครือข่ายผ่านทางเว็บไซต์ของระบบบริหารจัดการเครือข่ายของซิสโก้ โดยการเข้าไปเลือกอุปกรณ์เครือข่ายที่เราเพิ่มไว้ในรายการอุปกรณ์เครือข่ายของระบบบริหารจัดการเครือข่ายของซิสโก้ดังรูปที่ 4.9 จากนั้นระบบบริหารจัดการเครือข่ายของซิสโก้จะแสดงรายการข้อมูลอินเทอร์เน็ตเฟสของอุปกรณ์เครือข่ายที่เลือก เพื่อให้ผู้ดูแลระบบเครือข่ายเข้าไปดำเนินการแก้ไขและปรับเปลี่ยนค่าการติดตั้งใช้งานดังรูปที่ 4.10 และ 4.11 โดยความสามารถในการแก้ไขและปรับเปลี่ยนค่าการติดตั้งบนตัวอุปกรณ์เครือข่ายของระบบบริหารจัดการเครือข่ายของซิสโก้จะขึ้นอยู่กับชนิดและรุ่นของอุปกรณ์เครือข่ายของซิสโก้ ในบางรุ่นอาจจะสามารถแก้ไขและปรับเปลี่ยนค่าการติดตั้งบนตัวอุปกรณ์เครือข่ายได้หลายค่า แต่ในบางรุ่นสามารถแก้ไขและปรับเปลี่ยนค่าการติดตั้งบนตัวอุปกรณ์เครือข่ายได้แค่แบบพื้นฐาน ซึ่งเท่าที่ทำการทดลองทดสอบกับอุปกรณ์เครือข่ายของซิสโก้ที่ติดตั้งใช้งานในองค์กร พบว่าระบบบริหารจัดการเครือข่ายของซิสโก้มีความสามารถในการแก้ไขและปรับเปลี่ยนค่าการติดตั้งใช้งานได้อย่างดีและทำให้สามารถแก้ไขและปรับเปลี่ยนค่าการติดตั้งใช้งานบนตัวอุปกรณ์เครือข่ายได้สะดวกและรวดเร็วขึ้น

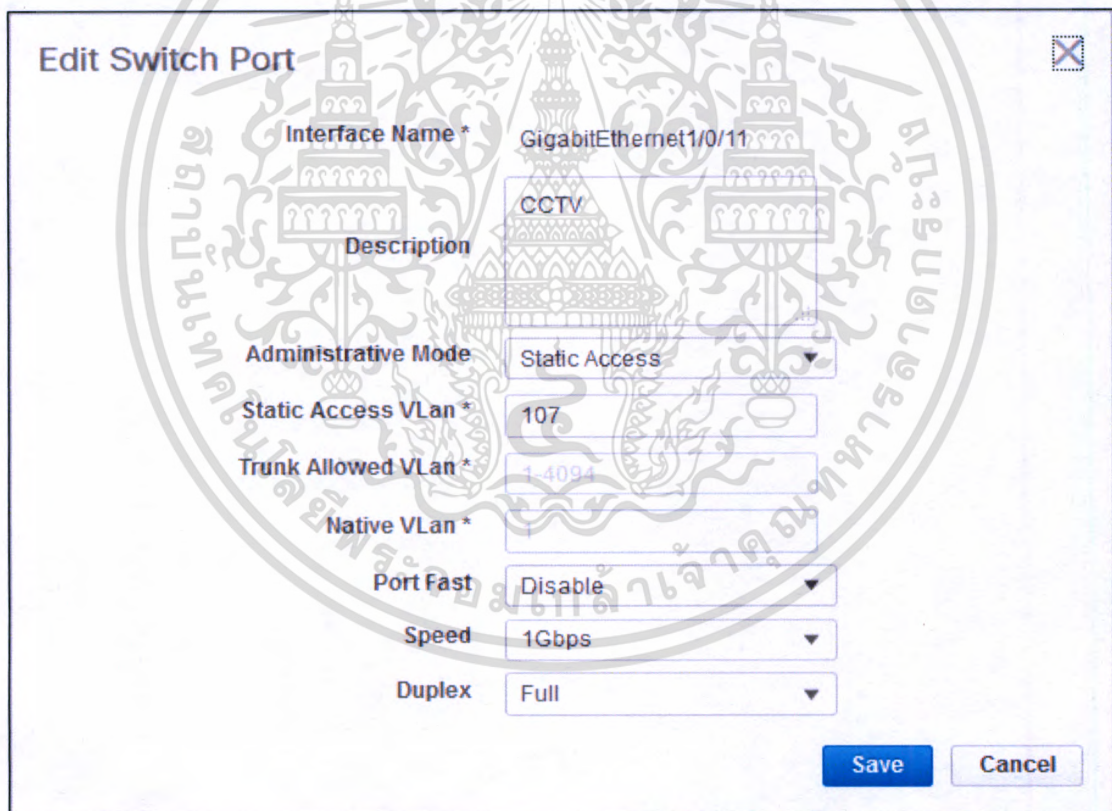
Device Name	Reachab...	IP Address	DNS Name	Device Type	Admin Status	Last Inv
R_PNT_01_12363	✓	137.40.78.170	137.40.78.170	Cisco 2911 Integrated Services Router G2	Managed	Comple
B7FL2-C2960-SW06	✓	172.16.7.106	172.16.7.106	Cisco Catalyst 2960-24TC Switch	Managed	Comple
B7FL2-C2960-SW04	✓	172.16.7.104	172.16.7.104	Cisco Catalyst 2960-24TC Switch	Managed	Comple
B6FL2-C2960G-NewO...	✓	172.16.6.198	172.16.6.198	Cisco Catalyst 2960S-24TS-S Switch	Managed	Comple
B7FL2-C2960-SW03	✓	172.16.7.103	172.16.7.103	Cisco Catalyst 2960-24TC Switch	Managed	Comple
PISCTH-C2950X-Cant...	✓	172.16.4.22	172.16.4.22	Cisco Catalyst 29xx Stack-able Ethernet Switch	Managed	Comple
PISCTH-C2950X-ASW07	✓	172.16.1.27	172.16.1.27	Cisco Catalyst 29xx Stack-able Ethernet Switch	Managed	Comple
R_PNT_12251	✓	10.95.65.1	10.95.65.1	Cisco 2911 Integrated Services Router G2	Managed	Comple
B1FL1-C3850-DSW01	✓	172.16.8.1	172.16.8.1	Cisco Catalyst38xx stack-able ethernet switch	Managed	Comple
Pa5AP-WLC01	✓	137.40.78.80	137.40.78.80	Cisco 5508 Wireless LAN Controller	Managed	Comple
PISCTH-C2950X-B4W...	✓	172.16.4.21	172.16.4.21	Cisco Catalyst 29xx Stack-able Ethernet Switch	Managed	Comple
B7FL1-C2960G-SW01	✓	172.16.7.101	172.16.7.101	Cisco Catalyst 29xx Stack-able Ethernet Switch	Managed	Comple
B7FL2-C2960-SW05	✓	172.16.7.105	172.16.7.105	Cisco Catalyst 2960-24TC Switch	Managed	Comple

รูปที่ 4.9 เลือกอุปกรณ์เครือข่ายที่ต้องการปรับเปลี่ยนค่า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



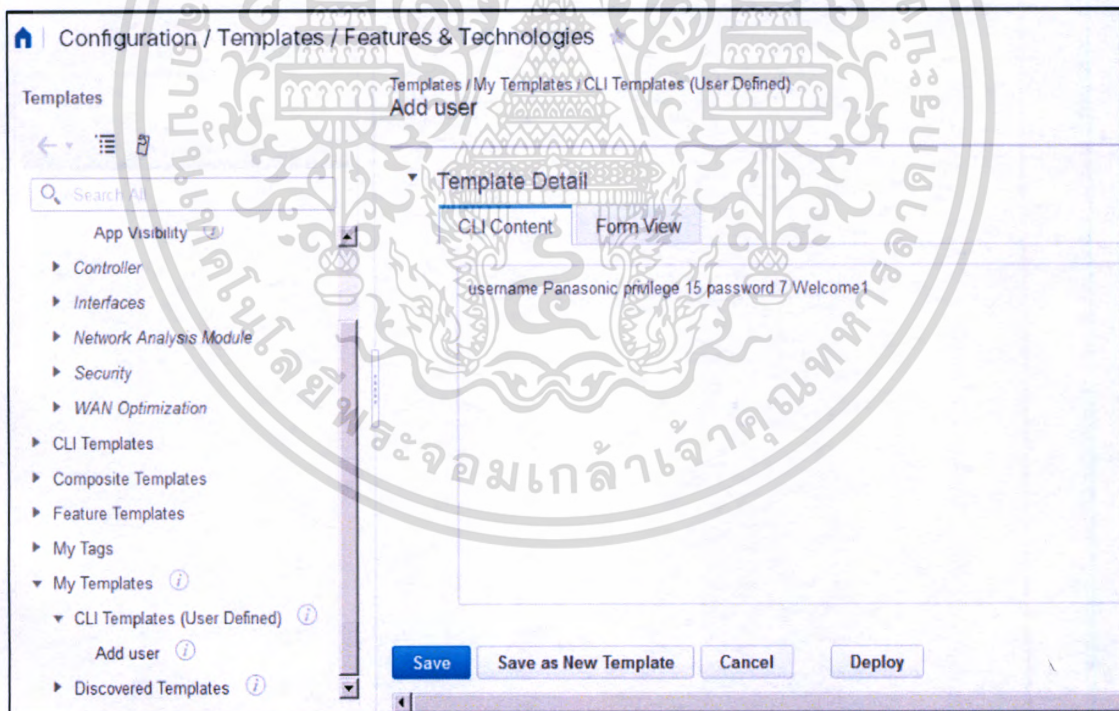
รูปที่ 4.10 เลือกอินเทอร์เฟซที่ต้องการจะเปลี่ยนแปลงค่าที่ตั้งไว้



รูปที่ 4.11 แสดงข้อมูลที่ต้องการจะเปลี่ยนแปลงค่าที่ตั้งไว้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในกรณีที่มีการแก้ไขหรือปรับเปลี่ยนค่าการติดตั้งกับทุกอุปกรณ์บนระบบเครือข่าย เช่น ต้องการเปลี่ยนแปลงชื่อบัญชีผู้ดูแลระบบหรือรหัสผ่านบนตัวอุปกรณ์เครือข่ายจากระบบเดิมผู้ดูแลระบบจะต้องเข้าถึงอุปกรณ์เครือข่ายจากระยะไกล (Remote Access) ผ่านทาง Telnet เข้าไปที่อุปกรณ์เครือข่ายที่ละตัว เพื่อทำการแก้ไขค่าที่ตั้งไว้ ซึ่งเพิ่มภาระการทำงานและใช้เวลาในการดำเนินการมาก แต่ในระบบบริหารจัดการเครือข่ายของซิสโก้จะมีเครื่องมือที่สามารถแก้ไขค่าที่ตั้งไว้ให้กับทุกๆ อุปกรณ์เครือข่ายจากศูนย์กลาง โดยสามารถสร้างรูปแบบคำสั่งเองหรือใช้รูปแบบที่ระบบบริหารจัดการเครือข่ายของซิสโก้มีให้ เพื่อนำมาใช้แก้ไขค่าที่ตั้งไว้ให้กับทุกๆ อุปกรณ์เครือข่ายดังรูปที่ 4.12 เป็นการสร้างรูปแบบคำสั่งขึ้นเองเพื่อทำการเพิ่มชื่อบัญชีผู้ดูแลระบบและรหัสผ่านบนตัวอุปกรณ์เครือข่าย เมื่อสร้างรูปแบบคำสั่งเรียบร้อยแล้วจะต้องทำการเลือกอุปกรณ์เครือข่ายที่เราต้องการจะทำการส่งคำสั่งนี้ไปให้ โดยสามารถเลือกอุปกรณ์เครือข่ายที่ละตัวหรือที่หลายๆตัวดังรูปที่ 4.13 โดยความสามารถในการเพิ่มและแก้ไขค่าที่ตั้งไว้จากศูนย์กลางให้กับทุกๆ อุปกรณ์ในระบบเครือข่ายของระบบบริหารจัดการเครือข่ายของซิสโก้ ทำให้ช่วยลดภาระงาน เพิ่มความสะดวกและลดเวลาในการทำงานของผู้ดูแลระบบเครือข่ายได้เป็นอย่างมาก



รูปที่ 4.12 การสร้างรูปแบบคำสั่งเพื่อเพิ่มกับให้อุปกรณ์เครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

General → Validation Criteria → Template Selection → Device Selection

To enable device selection at least one template needs to be added to the 'Selected Templates' table
Add and select devices to save the configuration group for deployment.

Selected Devices Selected 0 / Total 1

Show

<input type="checkbox"/>	Name	Description	Type	IP Address	Vendor
<input type="checkbox"/>	PISCTH-C2960X-Canteen...	PISCTH-C2960X-Canteen01	Switches and Hubs	172.16.4.22	Cisco

รูปที่ 4.13 แสดงลำดับการส่งรูปแบบคำสั่งเพื่อเพิ่มกับให้อุปกรณ์เครือข่าย

ข้อควรระวังเมื่อทำการแก้ไขหรือปรับเปลี่ยนค่าการติดตั้งใช้งานผ่านทางระบบบริหารจัดการเครือข่ายของซิสโก้ เนื่องจากระบบบริหารจัดการเครือข่ายของซิสโก้มีการทำงานแบบเว็บไซต์ ซึ่งจะแตกต่างกับแบบ คอมมานด์ไลน์ ที่ผู้ดูแลระบบคุ้นเคย ในการเข้าไปทำการแก้ไขและปรับเปลี่ยนค่าการติดตั้งใช้งานบนตัวอุปกรณ์เครือข่ายของซิสโก้ผ่านทางเว็บไซต์ นั้นจะต้องทำความเข้าใจในแต่หัวข้อ ซึ่งจะอ้างอิงมาจากรูปแบบของคอมมานด์ไลน์ เพราะเมื่อทำการแก้ไขหรือปรับเปลี่ยนค่าการติดตั้งใช้งานเรียบร้อยแล้ว ระบบบริหารจัดการเครือข่ายของซิสโก้จะทำการส่งข้อมูลไปที่ตัวอุปกรณ์เครือข่ายและจะมีผลทันทีเหมือนกับการแก้ไขหรือปรับเปลี่ยนค่าการติดตั้งใช้งานผ่านทางคอมมานด์ไลน์ ดังนั้นจึงควรระมัดระวังในการแก้ไขหรือปรับเปลี่ยนค่าการติดตั้งใช้งานเพราะอาจส่งผลกระทบต่อตัวอุปกรณ์และระบบเครือข่ายขึ้นได้

4.2.2 การจัดเก็บข้อมูลที่ตั้งไว้บนอุปกรณ์เครือข่ายจากศูนย์กลาง

เมื่อทำการกำหนดค่าการติดตั้งใช้งานบนตัวอุปกรณ์เครือข่ายเป็นที่เรียบร้อยแล้ว ผู้ดูแลระบบเครือข่ายควรจะต้องมีการจัดเก็บรักษาและสำรองค่าการติดตั้งใช้งานไว้ เพื่อความสะดวกในการใช้อ้างอิงเพื่อปรับแต่งหรือเปลี่ยนแปลงค่าการทำงานของอุปกรณ์เครือข่ายให้ถูกต้องเหมาะสมสอดคล้องกับหน้าที่ของแต่ละอุปกรณ์ในระบบเครือข่าย หรืออาจมีไว้เพื่อกู้คืนค่าการติดตั้ง เมื่อมีการเปลี่ยนอุปกรณ์ใหม่หรือกู้คืนทั้งระบบเครือข่ายเมื่อระบบเครือข่ายเกิดปัญหาขึ้น ซึ่งงานด้านการจัดเก็บค่าที่ตั้งไว้บนอุปกรณ์เครือข่ายเป็นงานที่เพิ่มภาระให้กับผู้ดูแลระบบเครือข่ายเป็นอย่างมาก เนื่องจากเป็นงานที่ต้องทำเป็นประจำและถ้าอุปกรณ์ในระบบเครือข่ายมีจำนวนมาก จะใช้เวลาใน

การดำเนินการเก็บรวบรวมค่าที่ตั้งไว้บนอุปกรณ์เครือข่ายมากขึ้นตามไปด้วย ยกตัวอย่างในองค์กรของผู้จัดทำได้มีการรับนโยบายและต้องปฏิบัติตามข้อกำหนดจากสำนักงานใหญ่ในต่างประเทศ ให้มีการจัดเก็บรวบรวมค่าที่ตั้งไว้บนอุปกรณ์เครือข่ายทุกๆเดือน รวมถึงก่อนและหลังที่มีการปรับแต่งหรือเปลี่ยนแปลงค่าที่ตั้งไว้บนอุปกรณ์เครือข่ายทุกครั้ง ทำให้เพิ่มภาระการทำงานให้กับผู้จัดทำในทุกๆเดือนและทุกครั้งที่มีการปรับแต่งหรือเปลี่ยนแปลงค่าที่ตั้งไว้บนอุปกรณ์เครือข่าย และเนื่องจากในระบบเครือข่ายในองค์กรมีอุปกรณ์ในระบบเครือข่ายจำนวนมาก ทำให้ต้องเสียเวลาในการจัดเก็บรวบรวมค่าที่ตั้งไว้บนอุปกรณ์เครือข่ายโดยต้องใช้เวลา 2-3 วันของทุกๆเดือนหรืออาจมากกว่านั้นถ้ามีงานสำคัญแทรกเข้ามาระหว่างดำเนินการในการจัดเก็บรวบรวมค่าที่ตั้งไว้บนอุปกรณ์เครือข่าย และในบางครั้งก็เกิดความผิดพลาดในการดำเนินการจัดเก็บรวบรวมค่าที่ตั้งไว้ ทำให้ต้องเสียเวลาในการตรวจสอบและต้องทำการจัดเก็บข้อมูลค่าที่ตั้งไว้ใหม่ จากปัญหาที่เกิดขึ้นจึงได้มีการนำเอาระบบบริหารจัดการเครือข่ายของซิสโก้มาทดสอบและทดสอบเพื่อช่วยในการดำเนินการจัดเก็บรวบรวมค่าที่ตั้งไว้ โดยระบบบริหารจัดการเครือข่ายของซิสโก้จะสามารถทำการจัดเก็บรวบรวมค่าที่ตั้งไว้ โดยต้องไปที่อุปกรณ์เครือข่ายที่ละตัวและเลือกที่ตัวเลือก Schedule Configuration Archive ซึ่งผู้ดูแลระบบเครือข่ายเข้าไปทำการตั้งค่าเพียงครั้งแรกครั้งเดียวเท่านั้น โดยระบบบริหารจัดการเครือข่ายของซิสโก้จะมีตัวเลือกการตั้งเวลาเพื่อจัดเก็บรวบรวมค่าที่ตั้งไว้ได้หลายแบบ เช่น จัดเก็บทันที ตั้งเวลาเป็นนาที่หรือชั่วโมง รวมถึงสามารถตั้งเป็นรอบการทำงาน เช่น ทุกๆวัน ทุกๆเดือน หรือทุกๆปีก็ได้ ดังรูปที่ 4.14

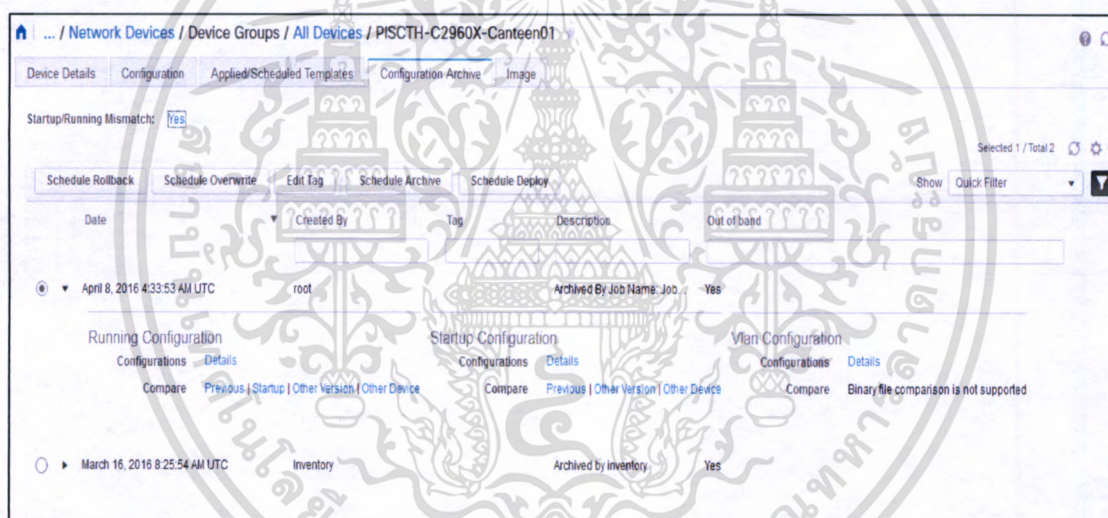
The screenshot shows a 'Schedule Configuration Archive' dialog box with the following fields and options:

- Job Name:** Job_Config-Archive_4_54_14_959_AM_4_8_2016
- Start Time:** 04/08/2016 04:54 AM (MM/dd/yyyy hh:mm AM/PM)
- Recurrence:** None, Minute, Hourly, Daily, Weekly, **Monthly**, Yearly
- Settings:**
 - The: First
 - of every: 1 month(s)
 - Day: Sunday
- End Time:**
 - No End Date/Time** (selected)
 - Every: 1 Times
 - End at: 04/08/2016 04:54 AM (MM/dd/yyyy hh:mm AM/PM)
- Buttons:** Submit, Cancel

รูปที่ 4.14 แสดงการจัดเก็บค่าที่ตั้งไว้ทุกๆเดือน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบบริหารจัดการเครือข่ายของซิสโก้จะแสดงหน้าจอการตั้งเวลาการจับเก็บข้อมูลที่ตั้งค่าไว้เป็นช่วงเวลาต่างๆให้ผู้ใช้งานเลือกใช้ โดยสามารถเลือกวันที่จะทำการจับเก็บข้อมูลที่ตั้งค่าไว้ของทุกเดือน ดังตัวอย่างในรูปที่ 4.14 เป็นการจับเก็บข้อมูลที่ตั้งค่าไว้ของทุกวันอาทิตย์แรกของทุกเดือนเมื่อถึงเวลาที่กำหนดไว้ ระบบบริหารจัดการเครือข่ายของซิสโก้จะทำการจับเก็บข้อมูลที่ตั้งค่าไว้โดยอัตโนมัติและผู้ดูแลระบบสามารถเข้าไปตรวจสอบสถานะการทำงานของระบบบริหารจัดการเครือข่ายของซิสโก้ได้ โดยระบบบริหารจัดการเครือข่ายของซิสโก้จะเก็บข้อมูลรายละเอียดการทำงานที่ตั้งค่าไว้ทุกครั้งดังรูปที่ 4.15 ทำให้สามารถตรวจสอบได้ว่าการจับเก็บข้อมูลที่ตั้งค่าไว้ตามวันและเวลาที่กำหนดไว้ทำงานได้ครบและเสร็จสมบูรณ์หรือไม่ ทำให้ผู้ดูแลระบบมั่นใจได้ว่าการจับเก็บข้อมูลที่ตั้งค่าไว้บนตัวอุปกรณ์เครือข่ายเป็นไปอย่างถูกต้อง ครบถ้วนและตรงตามเวลาที่กำหนด ซึ่งเป็นการลดภาระการทำงานของผู้ดูแลระบบ และสามารถลดเวลาที่ต้องสูญเสียไปกับการจับเก็บข้อมูลที่ตั้งค่าไว้บนตัวอุปกรณ์เครือข่ายได้อีกด้วย

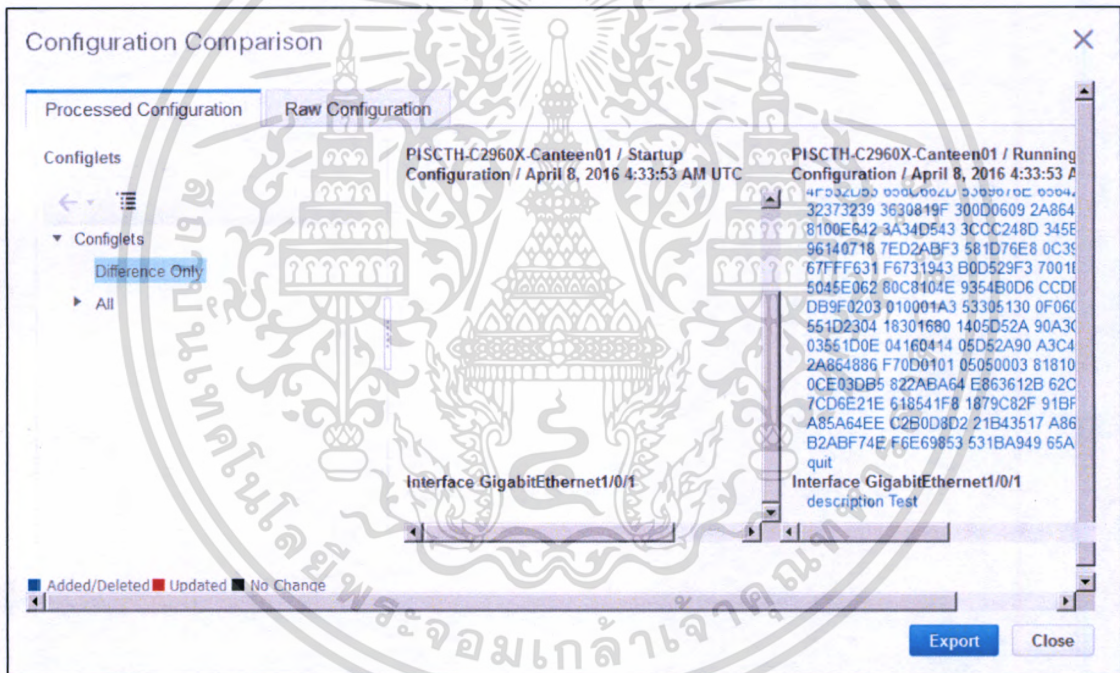


รูปที่ 4.15 แสดงข้อมูลที่ต้องการจะเปลี่ยนแปลงค่าที่ตั้งไว้

4.2.3 การเปรียบเทียบค่าที่ตั้งไว้บนอุปกรณ์เครือข่าย

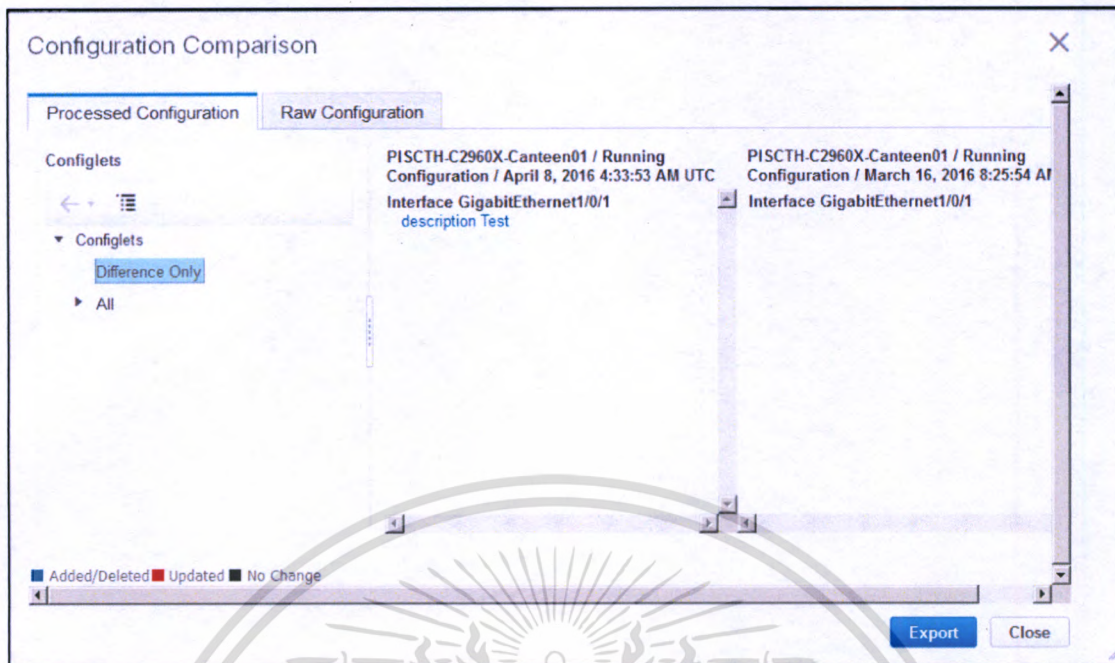
เมื่อมีการเพิ่มหรือแก้ไขค่าที่ติดตั้งไว้บนอุปกรณ์เครือข่าย ในบางครั้งผู้ดูแลระบบต้องการที่จะเปรียบเทียบค่าที่ติดตั้งไว้เดิมกับค่าติดตั้งที่มีการเพิ่มหรือแก้ไข หรือต้องการจะทราบว่ามีการเพิ่มหรือแก้ไขค่าที่ติดตั้งไว้บนอุปกรณ์เครือข่ายตรงไหนไปและเมื่อไหร่ ซึ่งถ้าไม่มีเครื่องมือที่ช่วยอำนวยความสะดวก จะทำได้ยากและเสียเวลาในการดำเนินการมาก เพราะต้องทำการตรวจสอบจากหน้าจอกอมมานด์ไลน์ ที่ละบรรทัดซึ่งอาจเกิดความผิดพลาดและเสียเวลาเป็นอย่างมาก ใน

ระบบบริหารจัดการเครือข่ายของซิสโก้มีเครื่องมือที่ช่วยในการเปรียบเทียบค่าที่ติดตั้งไว้ โดยสามารถเปรียบเทียบค่าที่ติดตั้งไว้ระหว่าง Running Configuration และ Startup Configuration หรือเปรียบเทียบค่าที่ติดตั้งไว้ของเดิมที่ถูกจัดเก็บกับของปัจจุบันได้ดังรูปที่ 4.16 เป็นการเปรียบเทียบค่าที่ติดตั้งไว้ระหว่าง Running Configuration และ Startup Configuration และรูปที่ 4.17 เป็นการเปรียบเทียบค่าที่ติดตั้งไว้ของเดิมที่ถูกจัดเก็บกับของปัจจุบัน ทำให้ผู้ดูแลระบบเครือข่ายสามารถเปรียบเทียบค่าที่ติดตั้งไว้บนอุปกรณ์เครือข่าย ได้อย่างสะดวกและรวดเร็ว และสามารถตรวจสอบค่าที่ติดตั้งไว้บนอุปกรณ์เครือข่ายว่ามีการเพิ่มหรือแก้ไขค่าที่ติดตั้งไว้ตอนไหนและตรวจสอบได้ว่ามี การเพิ่มหรือแก้ไขค่าที่ติดตั้งไว้ตรงไหนไว้บ้าง นอกจากนี้ในระบบบริหารจัดการเครือข่ายของซิสโก้ยังสามารถนำเอาค่าที่ติดตั้งไว้ที่จัดเก็บอยู่บนระบบบริหารจัดการเครือข่ายของซิสโก้ออกมาในรูปแบบของ Text File เพื่อนำไปใช้ในงานอื่นๆ ได้อีกด้วยโดยรูปที่ 4.18

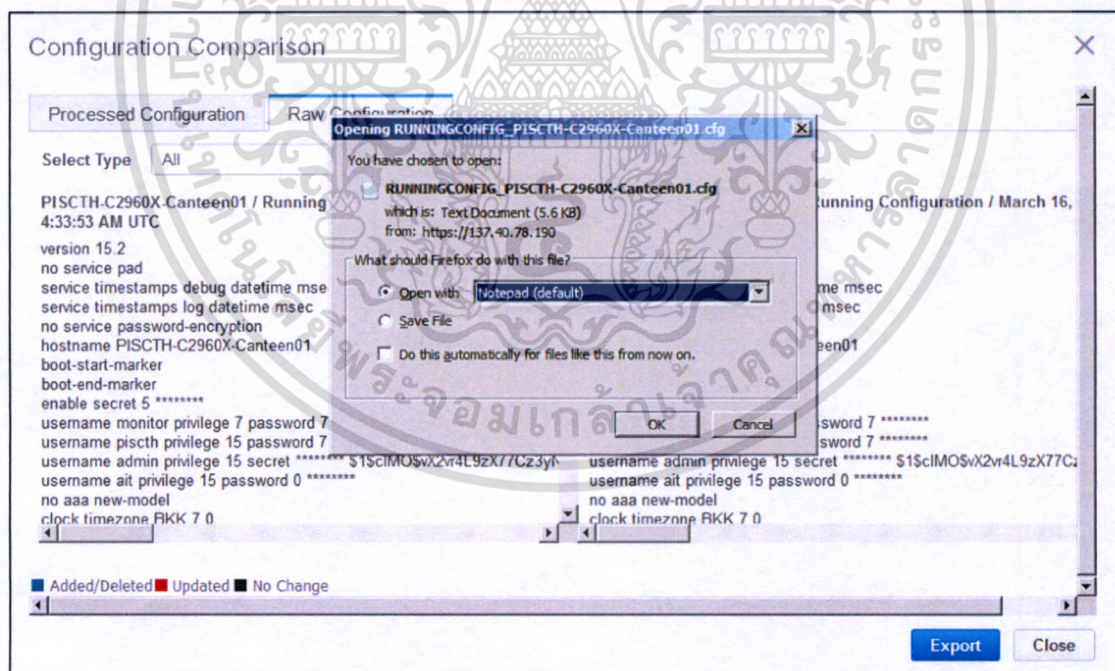


รูปที่ 4.16 การเปรียบเทียบค่าที่ติดตั้งไว้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.17 การเปรียบเทียบค่าที่ติดตั้งไว้ของเดิมกับปัจจุบัน



รูปที่ 4.18 นำข้อมูลค่าที่ตั้งไว้จากจากระบบบริหารจัดการเครือข่ายของซิสโก้

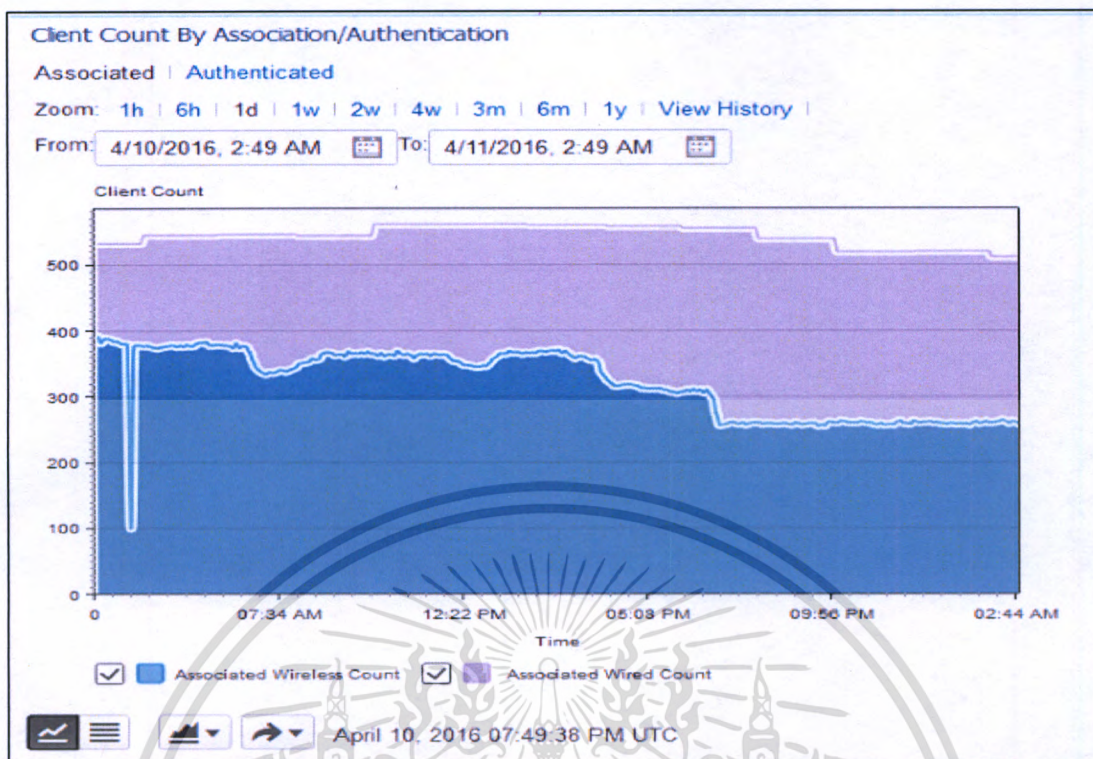
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3 การจัดการบัญชีผู้ใช้เครือข่าย (Account Management)

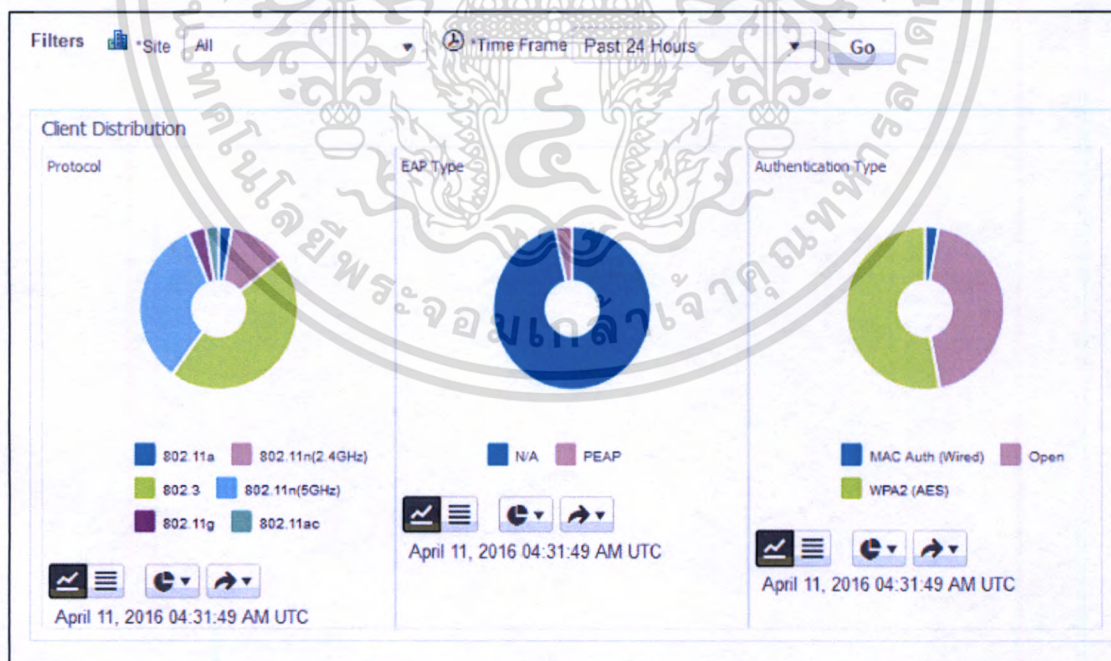
ระบบบริหารจัดการเครือข่ายของซิสโก้มีความสามารถในการทำงานร่วมกับโปรโตคอลวิเคราะห์เครือข่ายที่ติดตั้งอยู่ในอุปกรณ์เครือข่ายของซิสโก้ เช่น Net-Flow, Flexible Net-Flow, NBAR2 และ Application Visibility Control (AVC) โดยระบบบริหารจัดการเครือข่ายของซิสโก้จะทำการรับข้อมูลโปรโตคอลวิเคราะห์เครือข่ายที่ส่งมาจากอุปกรณ์เครือข่ายเช่น เราเตอร์ สวิตช์ หรือ อุปกรณ์ควบคุมเครือข่ายไร้สายจากศูนย์กลาง มาแสดงผลในรูปแบบแผนภูมิตามช่วงเวลา ทำให้ผู้ดูแลระบบเครือข่ายสามารถนำข้อมูลเหล่านี้มาวิเคราะห์และสามารถทราบว่ามีโปรโตคอลอะไรบ้างที่ส่งผ่านบนตัวอุปกรณ์เครือข่าย

4.3.1 แสดงข้อมูลบัญชีผู้ใช้งานบนอุปกรณ์เครือข่าย

ในระบบเครือข่ายที่มีการยืนยันตัวตนก่อนที่จะเข้าใช้งานระบบเครือข่าย โดยทั่วไปมักจะใช้โปรโตคอล 802.1X บนระบบเครือข่ายแบบใช้สายและไร้สาย ในระบบบริหารจัดการเครือข่ายของซิสโก้จะสามารถเก็บรวบรวมข้อมูลการยืนยันตัวตนของผู้ใช้งานบนอุปกรณ์เครือข่ายแบบใช้สายและไร้สายได้และนำมาแสดงเป็นแผนภูมิ ทำให้ผู้ดูแลระบบเครือข่ายสามารถทราบว่ามีผู้เข้าใช้งานระบบเครือข่ายที่มีการยืนยันตัวตนก่อนที่จะเข้าใช้งานเครือข่ายเป็นจำนวนเท่าไรดังรูปที่ 4.19 แสดงจำนวนผู้ใช้งานเครือข่ายไร้สายที่มีการยืนยันตัวตนก่อนที่จะเข้าใช้งานระบบเครือข่าย นอกจากนี้ระบบบริหารจัดการเครือข่ายของซิสโก้ยังสามารถแสดงโปรโตคอล 802.1X บนระบบเครือข่ายแบบใช้สายและไร้สายที่ถูกใช้งานดังรูปที่ 4.20 และเมื่อทำการเลือกที่แผนภูมิแสดงโปรโตคอล 802.1X บนระบบเครือข่ายไร้สายจะแสดงรายละเอียดของผู้ใช้งานในแต่ละโปรโตคอล 802.1X ดังรูปที่ 4.21 ทำให้ผู้ดูแลระบบสามารถนำข้อมูลเหล่านี้มาใช้ตรวจสอบด้านความปลอดภัยทำเป็นรายงานหรือใช้เพื่อวิเคราะห์ปัญหาในระบบเครือข่ายได้



รูปที่ 4.19 แสดงปริมาณการยืนยันตัวตนที่เข้าใช้งานระบบเครือข่าย



รูปที่ 4.20 แสดงแผนภูมิปริมาณโปรโตคอล 802.1X

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Monitor / Monitoring Tools / Clients and Users ★

Clients Search Results - Reset

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

	MAC Address	IP Address	IP Type	User Name	Type	Vendor	Location	Device Name
<input type="radio"/>	2c:33:7a:69:93:89	10.84.97.51	IPv4	PANASONIC02Rungrit_Int	🔒	Hon	System Ca...	WLC5508-B5
<input type="radio"/>	2c:33:7a:69:96:3b	10.84.97.61	IPv4	02jiranant_boo	🔒	Hon	System Ca...	WLC5508-B5
<input type="radio"/>	34:68:95:a5:de:71	10.84.60.29	IPv4	PANASONIC02Parinya_Khe	🔒	Hon	System Ca...	WLC5508-B5
<input type="radio"/>	2c:33:7a:69:94:66	10.84.97.79	IPv4	PANASONIC02Teechunya...	🔒	Hon	System Ca...	WLC5508-B5
<input type="radio"/>	2c:33:7a:69:95:ca	10.84.97.58	IPv4	PANASONIC02Supaporn...	🔒	Hon	System Ca...	WLC5508-B5
<input type="radio"/>	2c:33:7a:69:94:5d	10.84.97.46	IPv4	PANASONIC02Somchai_K...	🔒	Hon	System Ca...	WLC5508-B5
<input type="radio"/>	2c:33:7a:69:92:f4	10.84.97.23	IPv4	PANASONIC02Surin_Sur	🔒	Hon	System Ca...	WLC5508-B5
<input type="radio"/>	2c:33:7a:69:96:74	10.84.97.24	IPv4	PANASONIC02napapa_pua	🔒	Hon	System Ca...	WLC5508-B5
<input type="radio"/>	2c:33:7a:69:90:e4	10.84.97.67	IPv4	PANASONIC02Nittaya_Sai	🔒	Hon	System Ca...	WLC5508-B5
<input type="radio"/>	34:68:95:a5:da:ee	10.84.97.52	IPv4	PANASONIC02Rungnapa...	🔒	Hon	System Ca...	WLC5508-B5
<input type="radio"/>	2c:33:7a:69:95:c8	10.84.97.59	IPv4	PANASONIC02Somchai_K...	🔒	Hon	System Ca...	WLC5508-B5
<input type="radio"/>	2c:33:7a:69:95:46	10.84.97.80	IPv4	PANASONIC02oranuch_pit	🔒	Hon	System Ca...	WLC5508-B5

รูปที่ 4.21 แสดงรายละเอียดของผู้ใช้งานบน โพรโตคอล 802.1X

ระบบบริหารจัดการเครือข่ายของซิสโก้ยังมีเครื่องมือที่ช่วยในการวิเคราะห์ข้อมูลผู้ใช้งาน โดยสามารถแสดงรายละเอียดถึงข้อมูลของผู้ใช้งานที่เชื่อมต่อเข้ากับอุปกรณ์เครือข่ายดังรูปที่ 4.22 แสดงรายละเอียดข้อมูลของผู้ใช้งานที่เชื่อมต่อเข้ากับอุปกรณ์เครือข่ายไร้สาย ทำให้ผู้ดูแลระบบสามารถทราบข้อมูลของผู้ใช้งาน สถานะการเชื่อมต่อ ความปลอดภัยในการเชื่อมต่อ และสภาพสัญญาณของเครือข่ายไร้สาย ซึ่งจะช่วยให้ผู้ดูแลระบบสามารถนำข้อมูลเหล่านี้ไปวิเคราะห์หาสาเหตุเพื่อแก้ไขปัญหาที่เกิดขึ้นกับผู้ใช้งาน ได้อย่างสะดวกและรวดเร็ว โดยไม่จำเป็นต้องเข้าไปที่ตัวอุปกรณ์เครือข่าย ดังรูปที่ 4.23 แสดงเครื่องมือที่ช่วยบริหารจัดการผู้ใช้งานบนเครือข่ายที่ระบบบริหารจัดการเครือข่ายของซิสโก้สามารถดำเนินการกับผู้ใช้งานระบบเครือข่ายได้ เช่น สั่งหยุดการทำงานของอุปกรณ์เครือข่าย สั่งวิเคราะห์ข้อมูลผู้ใช้งานเครือข่าย หรือทำการทดสอบการเชื่อมต่อของผู้ใช้งานกับอุปกรณ์เครือข่ายได้ ทำให้ผู้ดูแลระบบมีเครื่องมือที่สามารถบริหารจัดการผู้ใช้งานบนอุปกรณ์เครือข่ายจากศูนย์กลางได้อย่างสะดวกรวดเร็วและมีประสิทธิภาพ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Monitor / Monitoring Tools / Clients and Users / 34:68:95:a5:de:71

Test | Disable | Remove

Overview Location ISE Troubleshoot and Debug Clean Air Events RTTS More

Properties

General	Session	Security
User Name: PANASONIC02Parinya_Khe	Controller Name: WLC6508-B5	Security Policy Type: WPA2
IP Address: 10.84.60.29	Controller IP Address/DNS Name: 172.16.5.251	EAP Type: PEAP
MAC Address: 34:08:95:a5:de:71	AP Name: PIDTH-B5FL2-AP27021-02	On Network: Yes
Vendor: Hon	AP IP Address: 172.16.5.102	802.11 Authentication: Open System
Endpoint Type: none	AP Type: Cisco AP	Encryption Cipher: CCMP (AES)
Client Type: Regular	AP Base Radio MAC: 74:a0:2fad:63:e0	SNMP NAC State: Access
Media Type: Lightweight	802.11 State: Associated	Radius NAC State: RUN
Hostname: Data Not Available	Association ID: 1	AAA Override ACL Name: Data Not Available
EZE: Not Supported	Port: 13	AAA Override ACL Applied Status: N/A
802.11u Capable: No	Interface: pasap-vlan60	Redirect URL: Data Not Available
	SSID: PASAP-Office	ACL Name: Data Not Available
	Profile Name: PASAP-Office	ACL Applied Status: N/A
	Protocol: 802.11n(2.4GHz)	FlexConnect Local Authentication: No
	Management VLAN ID: 60	Policy Manager State: RUN

รูปที่ 4.22 แสดงรายละเอียดเชิงลึกของผู้ใช้งานบนเครือข่าย

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users Show Associated Clients

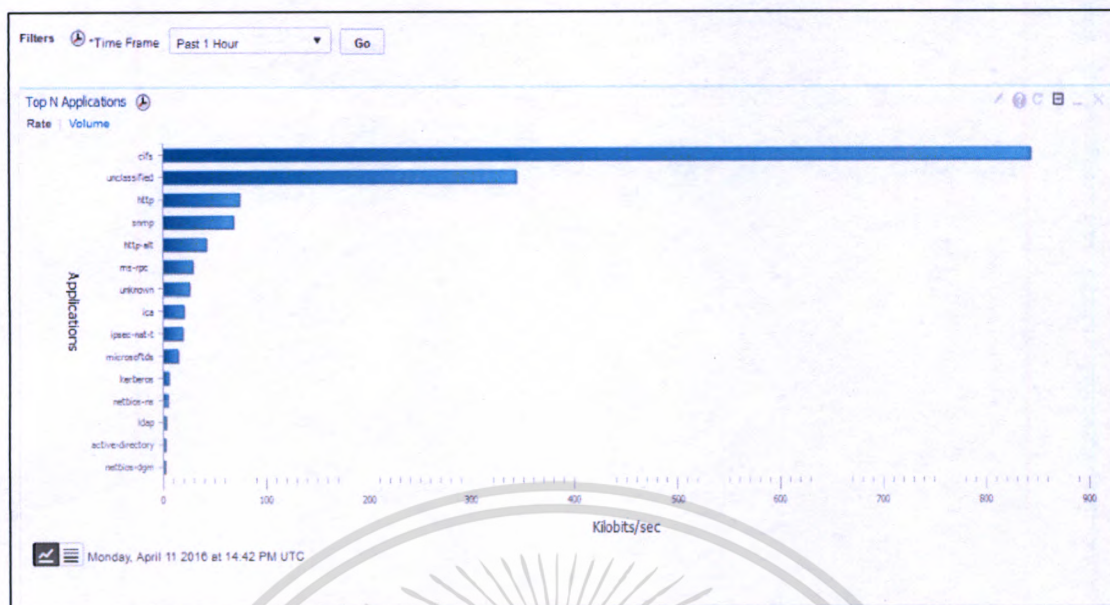
MAC Address	IP Address	IP Type	User Name	type	Vendor	Location	Device Name	Interface	VLAN	Protocol
48:e2:44:b7:2a:83		Not Det...	Unknown		Unknown	System Ca...	WLC6508-B5	pasap-via...	60	802.1
60:6d:c7:01:51:37	10.84.45.111	Dual-St...	Unknown		Unknown	System Ca...	PASAP-WLC02	production...	45	802.1
68:5d:43:02:2c:08	10.84.61.63	Dual-St...	Unknown		Intel	System Ca...	PASAP-WLC02	production...	61	802.1
84:4b:f5:b0:d2:f5	10.84.58.179	Dual-St...	Unknown		Hon Hai Pre...	System Ca...	PASAP-WLC02	office-58	58	802.1
3c77:e6:a9:80:18	10.84.3.73	Dual-St...	Unknown		Hon Hai Pre...	System Ca...	PASAP-WLC01	vlan33	33	802.1
00:23:68:cc:ef:57	192.168.106.38	IPv4	Unknown		Motorola	System Ca...	PASAP-WLC01	handheld	106	802.1
2c33:7a:69:92:bc	10.84.97.76	IPv4	PANASONIC02sucha_soo		Hon	System Ca...	WLC6508-B5	vlan97	97	802.1
54:35:30:ba:2a:3d	10.84.61.139	Dual-St...	Unknown		Hon	System Ca...	PASAP-WLC02	production...	61	802.1
34:23:87:be:45:4b	10.84.58.86	Dual-St...	Unknown		Hon Hai Pre...	System Ca...	PASAP-WLC02	office-58	58	802.1
84:4b:f5:b9:73:13	10.84.58.63	Dual-St...	Unknown		Hon Hai Pre...	System Ca...	PASAP-WLC02	office-58	58	802.1
10:08:b1:42:6c:e3	10.84.46.77	Dual-St...	Unknown		Hon	System Ca...	PASAP-WLC02	production...	46	802.1
5c:e0:c5:d2:7c:e2	10.84.60.12	IPv4	PANASONIC03harumi_tik		Intel	System Ca...	WLC6508-B5	vlan96	60	802.1
06:ed:b9:38:3e:84	10.84.46.141	Dual-St...	Unknown		Hon Hai Pre...	System Ca...	PASAP-WLC02	production...	46	802.1
84:4b:f5:b0:d4:21	10.84.61.19	Dual-St...	Unknown		Hon Hai Pre...	System Ca...	PASAP-WLC02	production...	61	802.1
18:5e:0f:25:a7:74	10.84.58.83	Dual-St...	Unknown		Unknown	System Ca...	PASAP-WLC01	office-58	58	802.1
68:94:23:33:4c:fd	10.84.58.93	Dual-St...	Unknown		Hon Hai Pre...	System Ca...	PASAP-WLC02	office-58	58	802.1
3c77:e6:a9:82:ca	10.84.3.104	Dual-St...	Unknown		Hon Hai Pre...	System Ca...	PASAP-WLC01	vlan33	33	802.1
84:4b:f5:b9:78:d5	10.84.58.116	Dual-St...	Unknown		Hon Hai Pre...	System Ca...	PASAP-WLC02	office-58	58	802.1

รูปที่ 4.23 แสดงเครื่องมือที่ช่วยบริหารจัดการผู้ใช้งานบนเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.2 แสดงข้อมูลการทำงานร่วมกับโปรโตคอลวิเคราะห์เครือข่าย

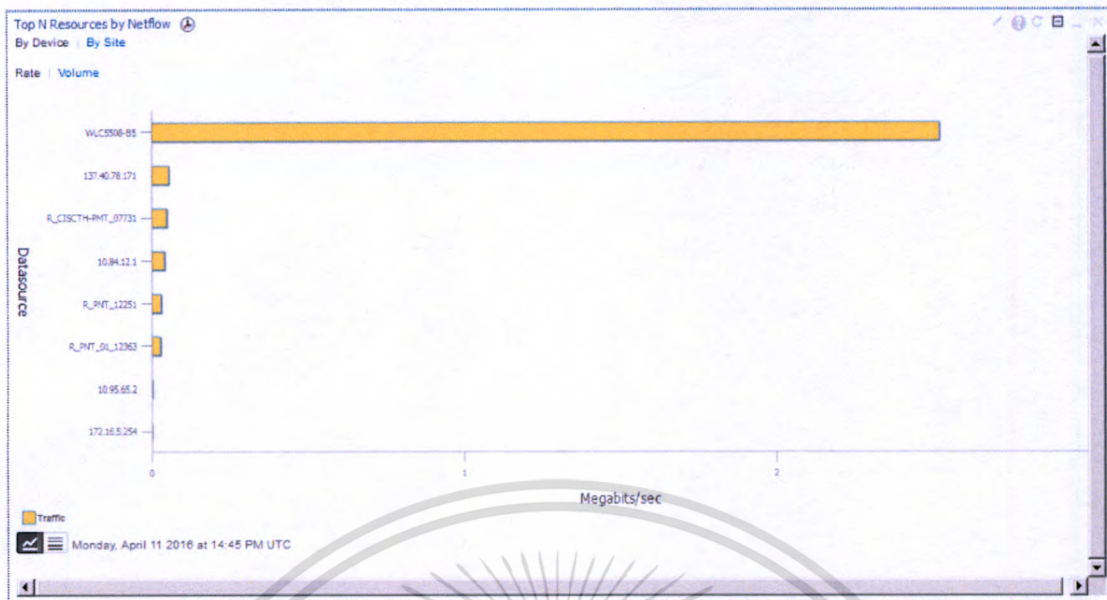
ระบบบริหารจัดการเครือข่ายของซิสโก้สามารถทำงานร่วมกับโปรโตคอลวิเคราะห์เครือข่ายที่ติดตั้งอยู่ในอุปกรณ์เครือข่ายของซิสโก้ เช่น Net-Flow, Flexible Net-Flow, NBAR2 และ Application Visibility Control (AVC) ซึ่งในการทดลองและทดสอบนี้ได้นำเอาอุปกรณ์เครือข่ายเชื่อมต่อระยะไกล หรือ เราเตอร์ ที่สนับสนุนโปรโตคอลวิเคราะห์เครือข่าย Net-Flow และอุปกรณ์ควบคุมเครือข่ายไร้สายจากศูนย์กลาง หรือ Wireless Controller ที่สนับสนุนโปรโตคอลวิเคราะห์เครือข่าย Application Visibility Control (AVC) ที่ติดตั้งใช้งานในองค์กรมาทำการทดลองและทดสอบกับระบบบริหารจัดการเครือข่ายของซิสโก้ว่าสามารถรับข้อมูลจากโปรโตคอลวิเคราะห์เครือข่ายที่ติดตั้งอยู่ในอุปกรณ์เครือข่ายของซิสโก้และนำมาแสดงผลให้กับผู้ดูแลระบบ ซึ่งจะช่วยให้ผู้ดูแลระบบสามารถทราบได้ว่ามีข้อมูลของโปรโตคอลใดบ้าง ที่ทำการรับและส่งข้อมูลผ่านบนตัวอุปกรณ์เครือข่าย และสามารถนำข้อมูลเหล่านั้นมาวิเคราะห์เพื่อใช้ในการบริหารจัดการโปรโตคอลเหล่านั้นได้อย่างถูกต้องเหมาะสม หรือสามารถนำข้อมูลมาจัดทำรายงานให้กับผู้บริการรับทราบ เพื่อดำเนินการปรับปรุงหรือขยายระบบเครือข่ายต่อไป จากปัญหาที่ผู้จัดทำได้พบในองค์กร คือ เมื่อพบว่ามีปัญหาการใช้งานช่องสัญญาณจนเต็มในระบบเครือข่าย โดยเฉพาะในระบบเครือข่ายเชื่อมต่อระยะไกลระหว่างสำนักงานใหญ่ไปที่สาขาต่างๆ ทางผู้บริหารและผู้จัดทำต้องการที่จะทราบข้อมูลว่าช่องสัญญาณเต็มเพราะสาเหตุใดและมีโปรโตคอลอะไรบ้างที่ใช้งานผ่านเครือข่ายนี้บ้าง แต่เนื่องจากไม่มีเครื่องมือที่สามารถทำงานร่วมกับโปรโตคอลวิเคราะห์เครือข่ายทำให้ไม่สามารถหาข้อมูลเหล่านี้ให้กับผู้บริหารได้ และการที่ไม่ทราบว่าโปรโตคอลอะไรบ้างที่ใช้งานผ่านเครือข่าย ทำให้ไม่สามารถบริหารจัดการโปรโตคอลที่ใช้งานผ่านเครือข่ายได้อย่างมีประสิทธิภาพ ดังนั้นการนำเอาระบบบริหารจัดการเครือข่ายของซิสโก้มาช่วยในการทำงานร่วมกับโปรโตคอลวิเคราะห์เครือข่ายที่ติดตั้งอยู่ในอุปกรณ์เครือข่ายของซิสโก้ ทำให้สามารถทราบว่าโปรโตคอลอะไรบ้างที่ใช้งานผ่านเครือข่ายดังรูปที่ 4.24 ระบบบริหารจัดการเครือข่ายของซิสโก้จะแสดงแอปพลิเคชันที่มีการใช้งานบนอุปกรณ์เครือข่าย โดยแสดงเรียงลำดับแอปพลิเคชันที่มีการใช้งานช่องสัญญาณมากที่สุดไปหาน้อยสุดบนอุปกรณ์เครือข่าย



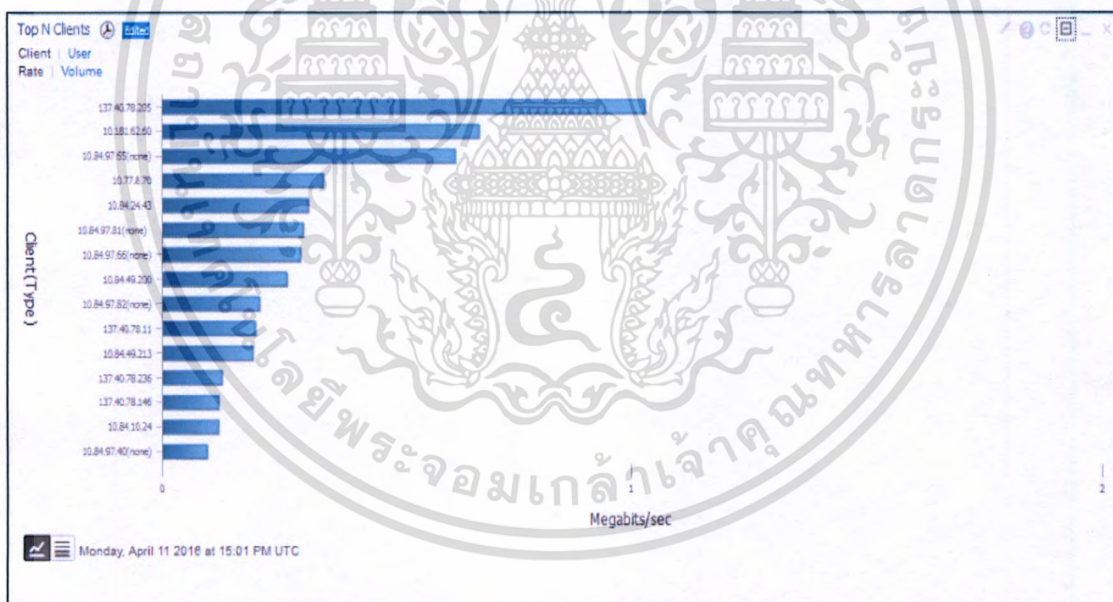
รูปที่ 4.24 แสดงแอปพลิเคชันที่มีการใช้งานบนอุปกรณ์เครือข่าย

นอกจากนั้นระบบบริหารจัดการเครือข่ายของซิสโก้ยังสามารถดูได้ว่าอุปกรณ์เครือข่ายตัวไหนมีการใช้งานทรัพยากรระบบเพื่อสนับสนุนการทำงานของแอปพลิเคชันดังรูปที่ 4.25 แสดงอุปกรณ์ควบคุมเครือข่ายไร้สายจากศูนย์กลางที่มีการใช้งานทรัพยากรระบบเพื่อสนับสนุนการทำงานของแอปพลิเคชันมากที่สุด และสามารถเข้าไปดูรายละเอียดได้ว่ามีเครื่องลูกข่ายตัวไหนเข้าใช้งานแอปพลิเคชันบนเครื่องแม่ข่ายตัวไหนมากที่สุดดังรูปที่ 4.26 และ 4.27 โดยระบบบริหารจัดการเครือข่ายของซิสโก้สามารถแสดงผลออกมาในรูปแบบแผนภูมิและเรียงตามลำดับการใช้งานจากมากไปหาน้อย ทำให้ผู้ดูแลระบบสามารถดูข้อมูลได้อย่างสะดวกและรวดเร็ว และสามารถนำข้อมูลออกมาเพื่อทำรายงานการวิเคราะห์แอปพลิเคชันที่ใช้งานบนระบบเครือข่ายให้กับผู้บริหารรับทราบและใช้ในการตัดสินใจเพื่อปรับปรุงและขยายระบบเครือข่ายต่อไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

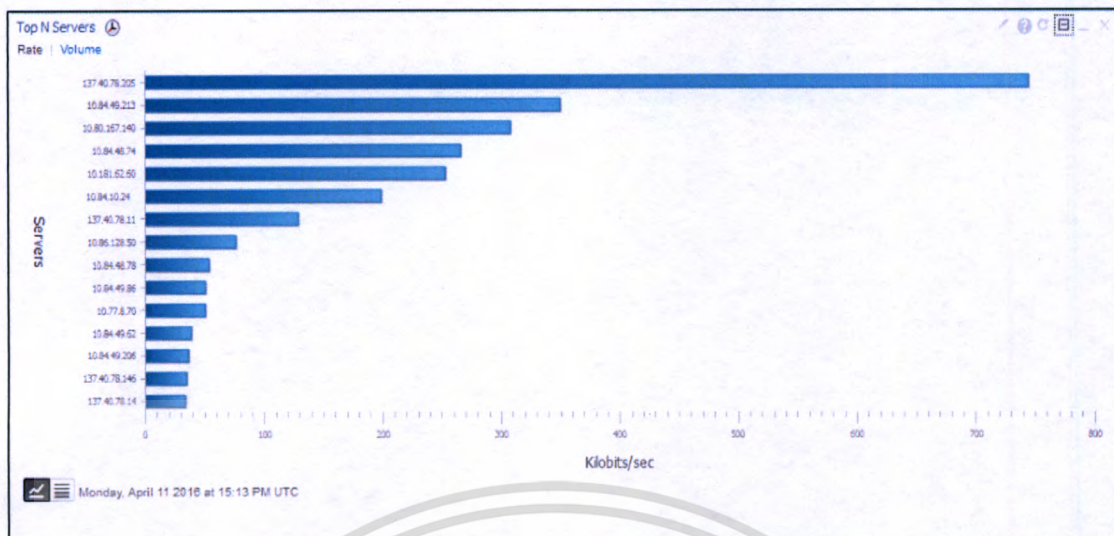


รูปที่ 4.25 แสดงอุปกรณ์ที่มีการใช้ทรัพยากรระบบเพื่อสนับสนุนการทำงานของแอปพลิเคชัน



รูปที่ 4.26 แสดงเครื่องลูกข่ายที่มีเข้าใช้งานมากที่สุดบนเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.27 แสดงเครื่องแม่ข่ายที่ถูกเข้าใช้งานมากสุดบนเครือข่าย

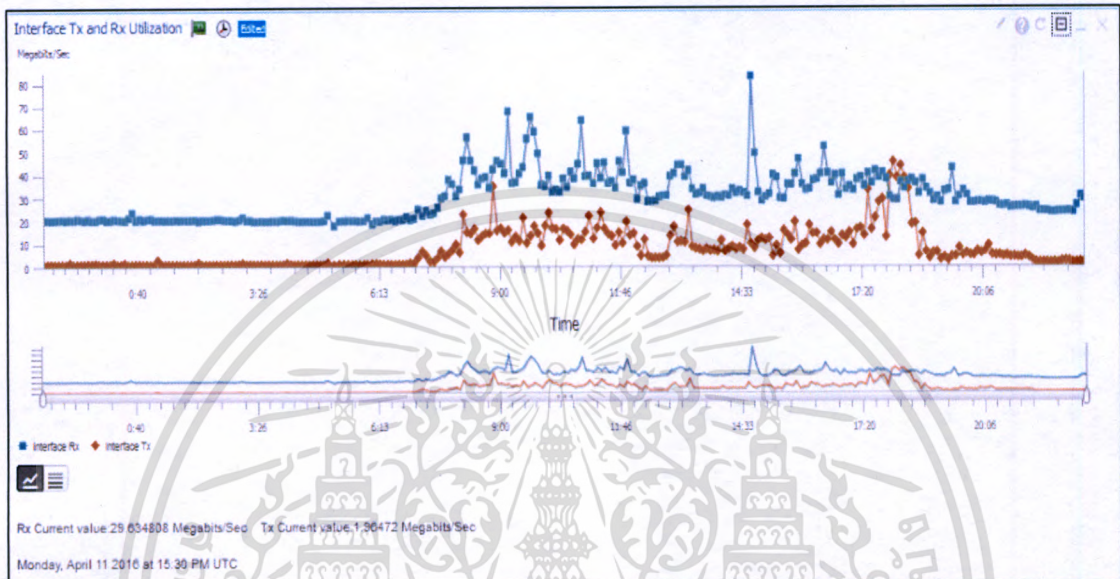
4.4 การจัดการประสิทธิภาพ (Performance Management)

ในการบริหารจัดการเครือข่ายจะต้องมีเครื่องมือที่ช่วยบริหารจัดการเกี่ยวกับประสิทธิภาพการทำงานของเครือข่าย โดยต้องสามารถตรวจวัดข้อมูลการจราจรในระบบเครือข่าย มาแสดงผลให้ผู้ดูแลระบบเครือข่ายทราบ เพื่อนำข้อมูลที่ได้ไปใช้ในการตัดสินใจ วางแผน และจัดเตรียมความพร้อมของทรัพยากรในระบบเครือข่ายให้สอดคล้องกับความต้องการใช้งานเครือข่ายในปัจจุบัน จากปัญหาที่พบในระบบเครือข่ายขององค์กรของผู้จัดทำคือ ไม่มีเครื่องมือที่ช่วยในการวัดประสิทธิภาพการทำงานของอุปกรณ์เครือข่ายและระบบเครือข่าย ทำให้ไม่สามารถรับทราบข้อมูลว่าโดยอุปกรณ์เครือข่ายและระบบเครือข่ายทำงานได้เต็มประสิทธิภาพหรือไม่ รวมทั้งไม่สามารถรับทราบปัญหาถ้าหากอุปกรณ์เครือข่ายและระบบเครือข่ายทำงานจนเกินประสิทธิภาพซึ่งอาจส่งผลกระทบต่อตัวอุปกรณ์และระบบเครือข่ายโดยรวมได้ ดังนั้นทางผู้จัดทำจึงได้ทำการทดลองและทดสอบระบบบริหารจัดการเครือข่ายของซิสโก้ในการบริหารจัดการเกี่ยวกับประสิทธิภาพของเครือข่ายดังนี้

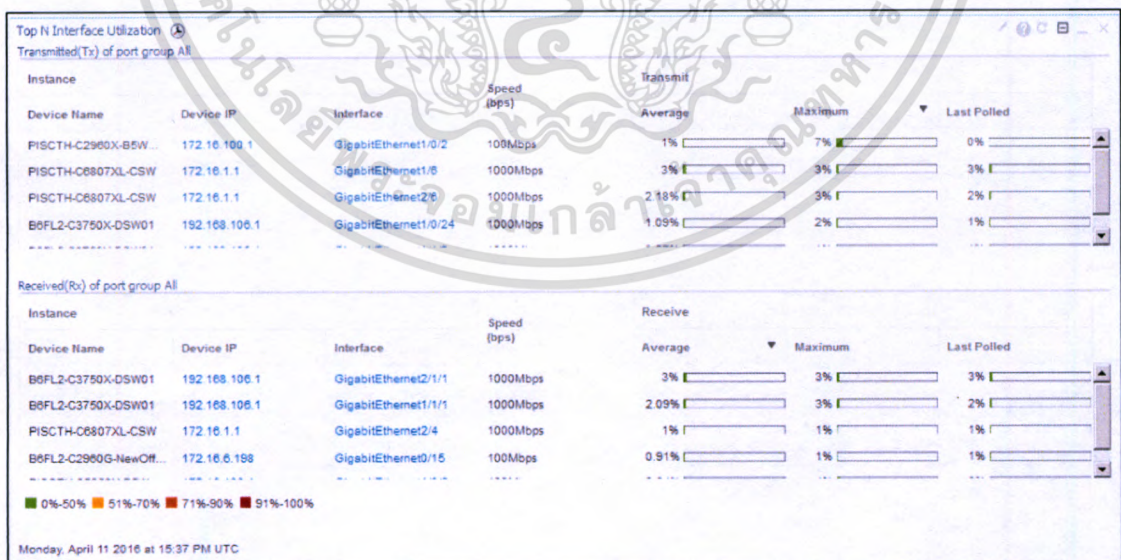
4.4.1 การแสดงรายงานการใช้ทรัพยากรบนอุปกรณ์เครือข่าย

ระบบบริหารจัดการเครือข่ายของซิสโก้สามารถทำการรวบรวมข้อมูลการทำงาน การเชื่อมต่อและการส่งผ่านข้อมูลของอุปกรณ์เครือข่าย ในทุกช่วงเวลาและทำการวัดประสิทธิภาพการให้บริการของอุปกรณ์เครือข่าย เช่น เวลาการตอบสนอง (Response Time), การละทิ้งแพคเกจ (Package Drop), การสูญหายของแพคเกจ (Package Loss), สภาพพร้อมใช้งานตลอดเวลา (Availability), และอัตราความผิดพลาดการรับ-ส่งข้อมูล (Error Rate) ดังรูปที่ 4.28 , 4.29 และ 4.30

ระบบบริหารจัดการเครือข่ายของซิสโก้จะแสดงข้อมูลประสิทธิภาพการให้บริการของแต่ละอินเทอร์เฟซบนแต่ละอุปกรณ์เครือข่ายที่มีการเชื่อมต่อ ทำให้ผู้ดูแลระบบเครือข่ายสามารถตรวจสอบประสิทธิภาพการให้บริการของเครือข่ายได้อย่างสะดวก รวดเร็วและทำให้สามารถบริหารจัดการเครือข่ายมีประสิทธิภาพมากขึ้น

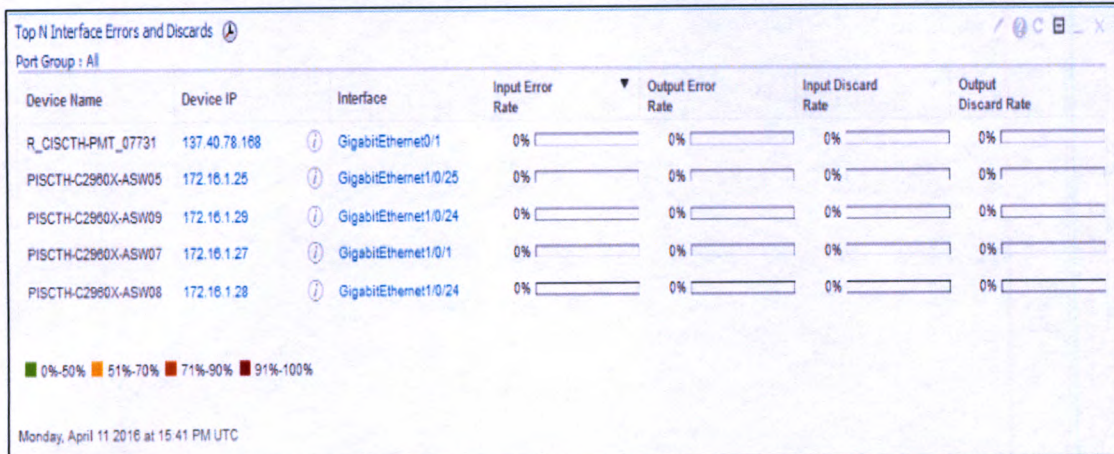


รูปที่ 4.28 แสดงการวัดประสิทธิภาพบนอินเทอร์เฟซของอุปกรณ์เครือข่าย



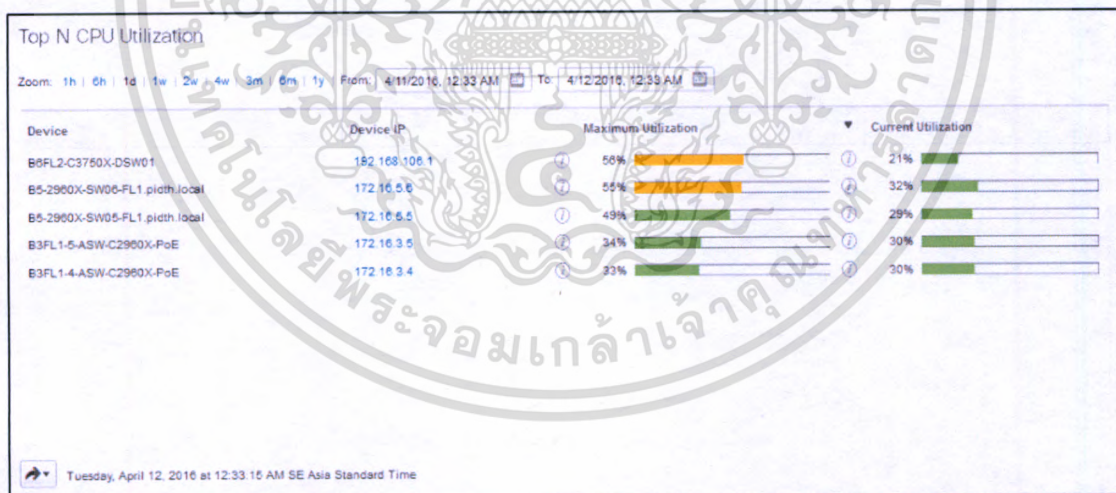
รูปที่ 4.29 แสดงอินเทอร์เฟซของอุปกรณ์เครือข่ายที่มีการใช้งานมาก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



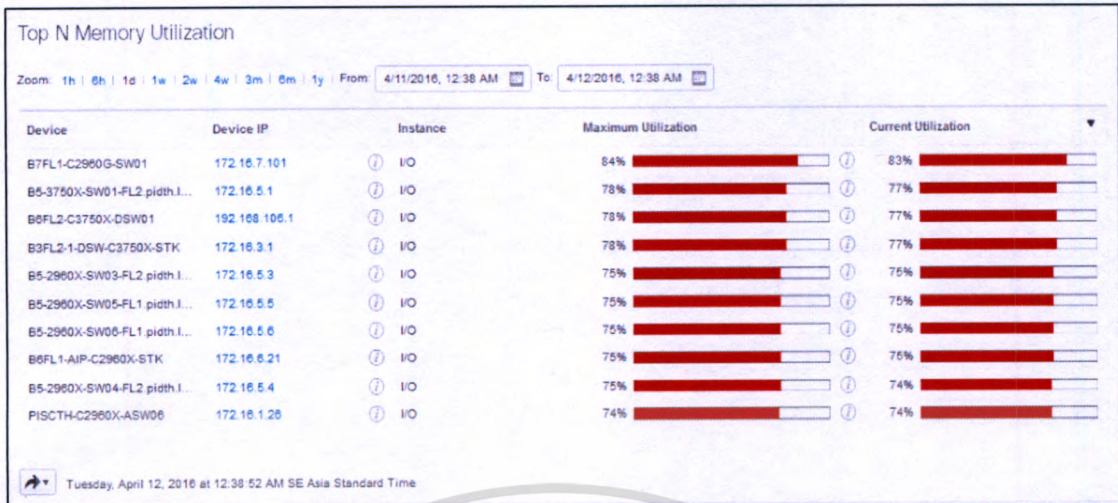
รูปที่ 4.30 แสดงการละทิ้งแพคเกจและอัตราความผิดพลาดในการรับ-ส่งข้อมูล

ระบบบริหารจัดการเครือข่ายของซิสโก้สามารถการแสดงผลงานการใช้ทรัพยากรบนอุปกรณ์เครือข่าย เช่น หน่วยประมวลผล หน่วยความจำ ทำให้ผู้ดูแลระบบเครือข่ายสามารถรับทราบข้อมูลภาพรวมการใช้ทรัพยากรบนอุปกรณ์เครือข่าย และสามารถนำข้อมูลไปวิเคราะห์หาสาเหตุ เพื่อแก้ไขปัญหาในกรณีที่อุปกรณ์เครือข่ายมีการใช้ทรัพยากรบนอุปกรณ์เครือข่ายผิดปกติ ดังรูปที่ 4.31 และรูปที่ 4.32



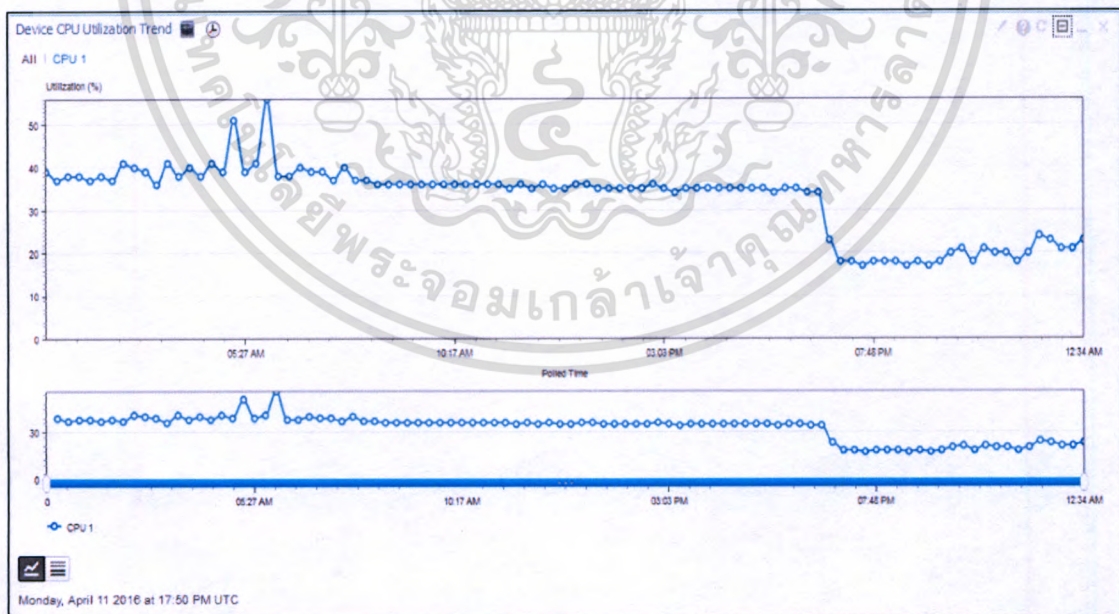
รูปที่ 4.31 แสดงรายการอุปกรณ์เครือข่ายที่มีการใช้งานหน่วยประมวลผลสูง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



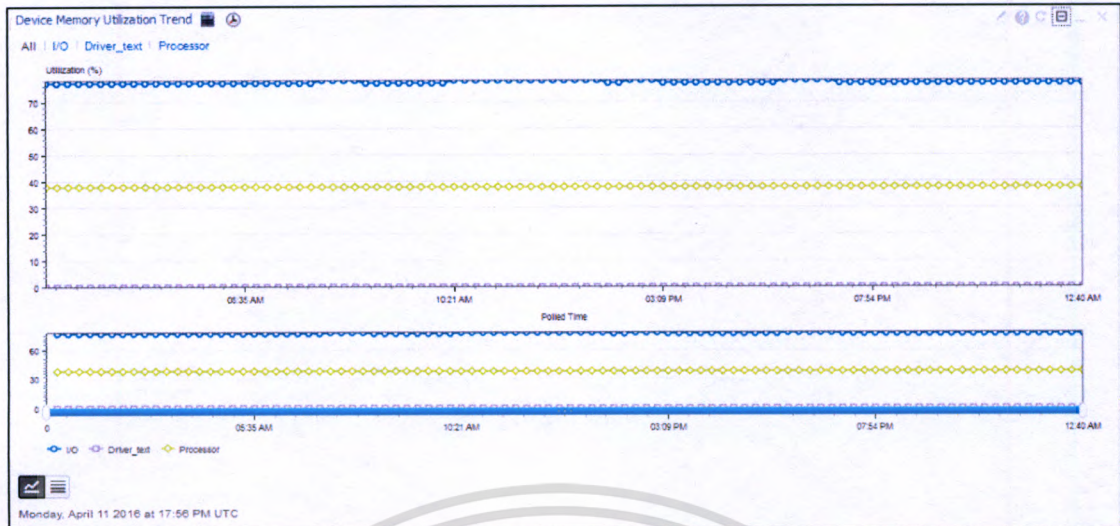
รูปที่ 4.32 แสดงรายการอุปกรณ์เครือข่ายที่มีการใช้งานหน่วยความจำสูง

นอกจากนี้ระบบบริหารจัดการเครือข่ายของซิสโก้ยังสามารถแสดงรายละเอียดการใช้ทรัพยากรหน่วยประมวลผลและหน่วยความจำบนอุปกรณ์เครือข่ายแต่ละตัว โดยสามารถเลือกแสดงตามช่วงเวลาที่กำหนด เพื่อให้ผู้ดูแลระบบสามารถทราบช่วงเวลาที่ถูกอุปกรณ์เครือข่ายมีการใช้ทรัพยากรบนอุปกรณ์เครือข่ายผิดปกติ ดังรูปที่ 4.33 และรูปที่ 4.34



รูปที่ 4.33 แสดงการใช้งานหน่วยประมวลผลของอุปกรณ์เครือข่ายตามช่วงเวลา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.34 แสดงการใช้งานหน่วยความจำของอุปกรณ์เครือข่ายตามช่วงเวลา

4.4.2 การแสดงข้อมูลพื้นฐานของอุปกรณ์เครือข่าย

ระบบบริหารจัดการเครือข่ายของซิสโก้สามารถแสดงข้อมูลพื้นฐานและรายละเอียดของอุปกรณ์เครือข่ายของซิสโก้ชนิดต่างๆ ได้ เช่น สภาพแวดล้อมของอุปกรณ์เครือข่าย เฟิร์มแวร์ที่ใช้งานอยู่ การแสดงรายการรายละเอียดและส่วนประกอบภายในอุปกรณ์เครือข่าย ทำให้ผู้ดูแลระบบทราบข้อมูลของอุปกรณ์เครือข่ายได้อย่างครบถ้วนและสะดวกรวดเร็ว เพราะไม่ต้องเข้าดูข้อมูลผ่านทางคอมมานด์ไลน์ ดังรูปที่ 4.35 แสดงค่าอุณหภูมิของอุปกรณ์เครือข่ายที่มีแนวโน้มค่อนข้างสูง ที่ผู้ดูแลระบบควรจะไปตรวจสอบหาสาเหตุและทำการแก้ไข

Figure 4.35 is a table titled "Top N Environmental Temperature". It shows the average, maximum, and minimum temperatures for five devices. The temperatures are in Celsius. The table also includes the device name, device IP, and the last polled time.

Device Name	Device IP	Temperature			Last Polled
		Average	Maximum	Minimum	
B3FL1-6-ASW-...	172.16.3.6	46	46	46	46
B3FL1-5-ASW-...	172.16.3.5	45	45	45	45
B3FL1-4-ASW-...	172.16.3.4	45	45	45	45
B3FL2-3-ASW-...	172.16.3.3	44	44	44	44
B3FL1-12-AS-...	172.16.3.12	43	43	43	43

รูปที่ 4.35 แสดงค่าอุณหภูมิของอุปกรณ์เครือข่ายที่มีแนวโน้มค่อนข้างสูง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบบริหารจัดการเครือข่ายของซิสโก้สามารถแสดงรายละเอียดของอุปกรณ์เครือข่ายของซิสโก้ โดยมีรูปจำลองของอุปกรณ์เครือข่ายนั้นดังรูปที่ 4.36 แสดงรายละเอียดอุปกรณ์เครือข่ายสวิตช์ของซิสโก้ ส่วนรูปที่ 4.37 แสดงข้อมูลรายละเอียดเชิงลึกของอุปกรณ์เครือข่ายของซิสโก้ และรูปที่ 4.38 แสดงรายละเอียดอุปกรณ์เครือข่ายไร้สายของซิสโก้ โดยระบบบริหารจัดการเครือข่ายของซิสโก้สามารถแสดงสถานะของอินเตอร์เฟซที่ถูกใช้งานในรูปแบบของภาพสี ซึ่งช่วยทำให้ผู้ดูแลระบบเครือข่ายไม่จำเป็นต้องไปดูที่ตัวอุปกรณ์เครือข่ายจริงๆทำให้สะดวกรวดเร็วในการบริหารจัดการตัวอุปกรณ์เครือข่าย นอกจากนี้ระบบบริหารจัดการเครือข่ายของซิสโก้สามารถแสดงรายละเอียดข้อมูลอื่นๆของอุปกรณ์เครือข่ายของซิสโก้ได้อีก เช่น หมายเลขเครื่องของอุปกรณ์เครือข่าย รุ่นของเฟิร์มแวร์ที่ใช้งานอยู่ จำนวนอินเตอร์เฟซที่ถูกใช้งานและไม่ได้ถูกใช้งาน ระยะเวลาที่อุปกรณ์เครือข่ายทำงานอยู่ เป็นต้น ทำผู้ดูแลระบบเครือข่ายสามารถทราบข้อมูลของอุปกรณ์เครือข่ายได้อย่างครบถ้วน สะดวกและรวดเร็ว เพราะระบบบริหารจัดการเครือข่ายของซิสโก้จะแสดงผลออกมาในรูปของกราฟิก ทำให้ดูได้ สะดวกรวดเร็วและง่ายกว่าแบบคอมมานด์ไลน์

The screenshot displays the Cisco Prime Network Manager interface for a switch configuration page. The page is titled "Summary" and shows the following details:

- System:** Summary, CLI Sessions, CDP Neighbors, Environment, Location, Memory, Modules, Physical Ports, Sensor, Stacks, User Defined Field, WLANs.
- Summary:** Status bar showing interface status (green/red).
- General:**
 - IP Address/DNS Name: 172.16.0.1
 - Device Name: B1FL1-C3850-DSW01
 - Device Type: Cisco Catalyst3850 stackable ethernet switch
 - Up Time: 38 days 11 hrs 19 mins 10 secs
 - Reachability Status: Reachable
- Unique Device Identifier (UDI):**
 - Name: Switch 1
 - Description: WS-C3850-48T-S
 - Product ID: WS-C3850-48T-S
 - Version ID: V08
 - Serial Number: FCW1950C19U
- Inventory:**
 - Software Version: 03.07.02E
 - Model No.: WS-C3850-48T-S
 - Burned-in MAC Address: 00:0a:55:13:87:00
 - Number of APs Supported: 0
- Other Fields:**
 - Location: (empty)
 - Contact: (empty)
 - Current ICMP Latency: 2 Secs
 - Cisco Identity Capable: No
 - Location Capable: Yes

รูปที่ 4.36 แสดงรายละเอียดอุปกรณ์เครือข่ายสวิตช์ของซิสโก้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

General		Unique Device Identifier (UDI)	
IP Address/DNS Name	172.16.8.1	Name	Switch 1
Device Name	B1FL1-C3850-DSW01	Description	WS-C3850-48T-S
Device Type	Cisco Catalyst38xx stack-able ethernet switch	Product ID	WS-C3850-48T-S
Up Time	39 days 11 hrs 18 mins 15 secs	Version ID	V06
Reachability Status	Reachable	Serial Number	FCW1950C19U
Location		Inventory	
Contact		Software Version	03.07.02E
Current ICMP Latency	2 Secs	Model No.	WS-C3850-48T-S
Cisco Identity Capable	No	Burned-in MAC Address	00:da:55:f3:87:00
Location Capable	Yes	Number of APs Supported	0
Internal Temperature	48C	Port Summary	
Total Client Count	0	Number of Ports Up	34
Power Supply One	Present, Operational	Number of Ports Down	64
Power Supply Two	Present, Operational		

รูปที่ 4.37 แสดงข้อมูลรายละเอียดอุปกรณ์เครือข่ายสวิตช์ของซิสโก้

Summary

Alarms Events Access Point # 67

General		Unique Device Identifier (UDI)	
IP Address/DNS Name	172.16.5.251	Name	Chassis
Name	WLC5508-B5	Description	Cisco 5500 Series Wireless LAN Controller
Device Type	5500	Product ID	AIR-CT5508-K9
Uptime	275 days 10 hrs 27 mins 29 secs	Version ID	V04
System Time	2016-Apr-11, 19:58:55 UTC	Serial Number	FCW1904B4FM
Internal Temperature	43C	CPU Utilization	
Location		Zoom:	1h 6h 1d 1w 2w 4w 3m 6m 1y
Contact		View History	
Current ICMP Latency	2005 Secs	From:	To:
Total Client Count	20	Avg. CPU Utilization(%)	
Current CAPWAP Transport Mode	Layer3		

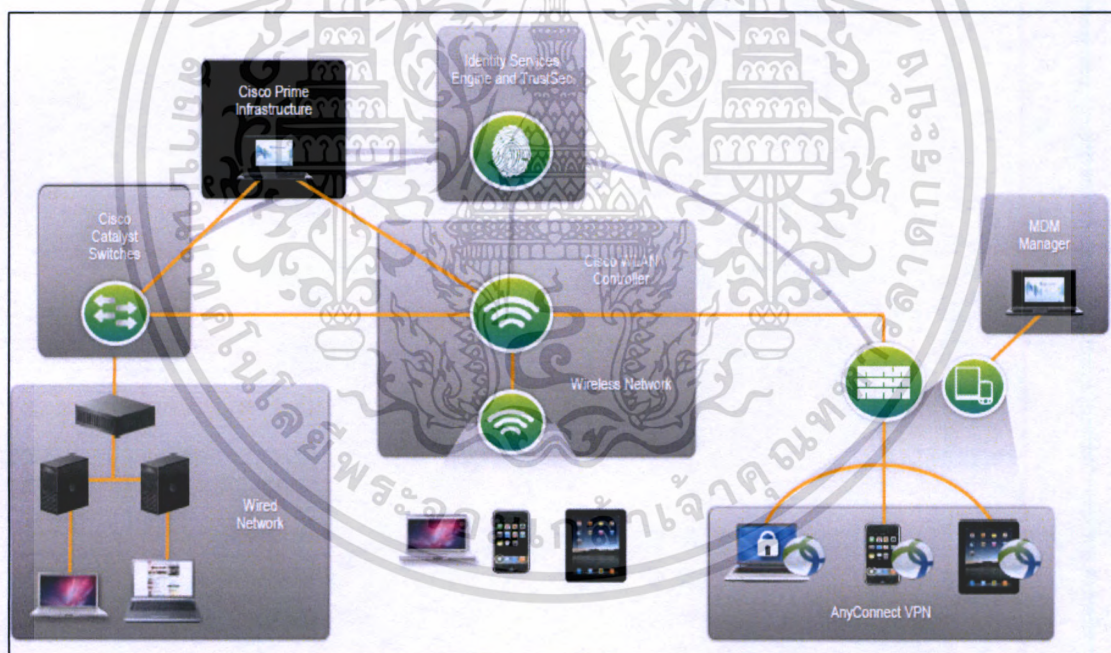
Inventory

รูปที่ 4.38 แสดงรายละเอียดอุปกรณ์เครือข่ายไร้สายของซิสโก้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.5 การจัดการด้านความปลอดภัย (Security Management)

ปัญหาของระบบเครือข่ายในด้านความมั่นคงปลอดภัย คือ การถูกบุกรุกหรือถูกโจมตีจากผู้ประสงค์ร้ายจากภายในและนอกองค์กร การเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาตและสร้างความเสียหายกับข้อมูลขององค์กร จึงมีความจำเป็นที่จะต้องมีการจัดการด้านความมั่นคงปลอดภัยให้กับระบบเครือข่ายภายในองค์กร โดยระบบบริหารจัดการเครือข่ายจะต้องมีเครื่องมือเพื่อช่วยผู้ดูแลระบบเครือข่ายในการตรวจสอบ, ควบคุมดูแลการเข้าถึงระบบเครือข่ายและอุปกรณ์เครือข่ายได้อย่างมีประสิทธิภาพ มีการเก็บข้อมูลการสื่อสารรับส่งข้อมูลของผู้ใช้งานเครือข่าย แสดงข้อมูลวิเคราะห์การใช้งานของผู้ใช้งานเครือข่ายและเก็บบันทึกข้อมูลจากเหตุการณ์ที่เกิดขึ้นบนอุปกรณ์และเครือข่าย โดยระบบบริหารจัดการเครือข่ายของซิสโก้สามารถทำงานร่วมกับซอฟต์แวร์ด้านความปลอดภัยของทางซิสโก้ได้ เช่น สามารถทำงานร่วมกับ Identity Services Engine หรือ (ISE) ซึ่งเป็นซอฟต์แวร์ด้านความปลอดภัยของทางซิสโก้ที่ใช้ในการยืนยันตัวตนของผู้ใช้งานที่จะเชื่อมต่อเข้าสู่ระบบเครือข่าย ดังรูปที่ 4.39



รูปที่ 4.39 แสดงแผนภาพการทำงานร่วมกับซอฟต์แวร์ด้านความปลอดภัยของทางซิสโก้

โดยระบบบริหารจัดการเครือข่ายของซิสโก้จะทำหน้าที่เป็นศูนย์กลางในการบริหารจัดการอุปกรณ์เครือข่ายของซิสโก้ชนิดต่างๆในระบบเครือข่าย โดยแต่ละอุปกรณ์เครือข่ายต้องมีการตั้งค่าให้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สามารถทำงานร่วมกับ Identity Services Engine หรือ (ISE) ซึ่งเป็นซอฟต์แวร์ด้านความปลอดภัยของทางซิสโก้ โดยซอฟต์แวร์ด้านความปลอดภัยของทางซิสโก้จะเป็นตัวกำหนดวิธีการยืนยันตัวตน นโยบายและสิทธิในการเข้าใช้งานเครือข่ายให้กับผู้ใช้งาน เมื่อผู้ใช้งานมีการเชื่อมต่อเข้ากับระบบเครือข่ายทั้งแบบใช้สายและไร้สาย จะต้องทำการยืนยันตัวตน รับนโยบายและสิทธิในการเข้าใช้งานเครือข่ายที่ทางผู้ดูแลระบบกำหนดขึ้นในซอฟต์แวร์ด้านความปลอดภัยของทางซิสโก้ โดยระบบบริหารจัดการเครือข่ายของซิสโก้จะช่วยในเรื่องของการบริหารจัดการค่าการติดตั้งด้านความปลอดภัยให้กับทุกๆ อุปกรณ์เครือข่ายของซิสโก้จากศูนย์กลางและเป็นตัวดึงข้อมูลการยืนยันตัวตนและสถานะของผู้ใช้งานจากซอฟต์แวร์ด้านความปลอดภัยของทางซิสโก้มาแสดงผลให้กับผู้ดูแลระบบรับทราบข้อมูล และเนื่องจากระบบเครือข่ายในองค์กรของผู้จัดทำยังไม่มีการติดตั้งและใช้งานซอฟต์แวร์ด้านความปลอดภัยของทางซิสโก้จึงไม่สามารถแสดงข้อมูลในส่วนนี้ได้ แต่ได้ทำการทดลองและทดสอบระบบบริหารจัดการเครือข่ายของซิสโก้ในด้านการจัดการด้านความปลอดภัย โดยระบบบริหารจัดการเครือข่ายของซิสโก้สามารถแสดงผลจากข้อมูลด้านความปลอดภัยที่ส่งมาจากอุปกรณ์เครือข่ายได้ ในรูปที่ 4.40 ระบบบริหารจัดการเครือข่ายของซิสโก้สามารถแสดงข้อมูลการเชื่อมต่อระหว่างผู้ใช้งานกับอุปกรณ์เครือข่ายไร้สาย ทำให้ผู้ดูแลระบบสามารถค้นหาผู้ใช้งานที่มีการเชื่อมต่อเข้าใช้งานในระบบเครือข่ายได้ ทำให้ง่ายต่อการตรวจสอบข้อมูลด้านความปลอดภัยของผู้ใช้งาน ในการใช้งานเครือข่ายได้อย่างสะดวกและรวดเร็ว

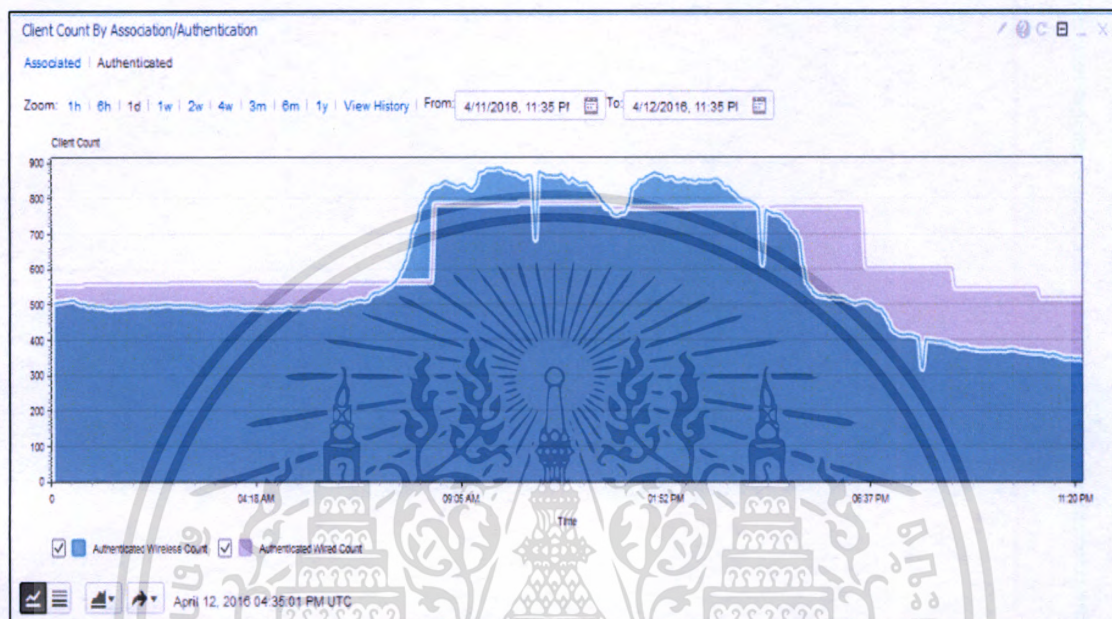
The screenshot displays the Cisco ISE Client Attributes page. At the top, there are navigation tabs: Overview, Location, ISE, Troubleshoot and Debug, Clean Air, Events, RTTS, and More. Below the tabs, there is a 'Client Attributes Summary' section with a diagram showing a client (00:23:68:e8:a9:ef) connected to an AP (AP-206), which is connected to a controller (FASAP-WLC01). Below this is the 'Client Attributes' section with a 'Refresh from Device' button. The main content is divided into three columns: General, Session, and Security.

General	Session	Security
User Name: Unknown	Controller Name: FASAP-WLC01	Security Policy Type: WPA2
IP Address: 192.168.106.48	Controller IP Address/DNS Name: 137.40.76.80	EAP Type: Unknown
MAC Address: 00:23:68:e8:a9:ef	AP Name: AP-206	On Network: Yes
Vendor: Motorola	AP IP Address: 172.16.6.206	802.11 Authentication: Open System
Endpoint Type: none	AP Type: Cisco AP	Encryption Cipher: COMP (AES)
Client Type: Regular	AP Base Radio MAC: 20:3a:07:97:ce:c0	SNMP IAC State: Access
Media Type: Lightweight	802.11 State: Associated	Radius IAC State: RUN

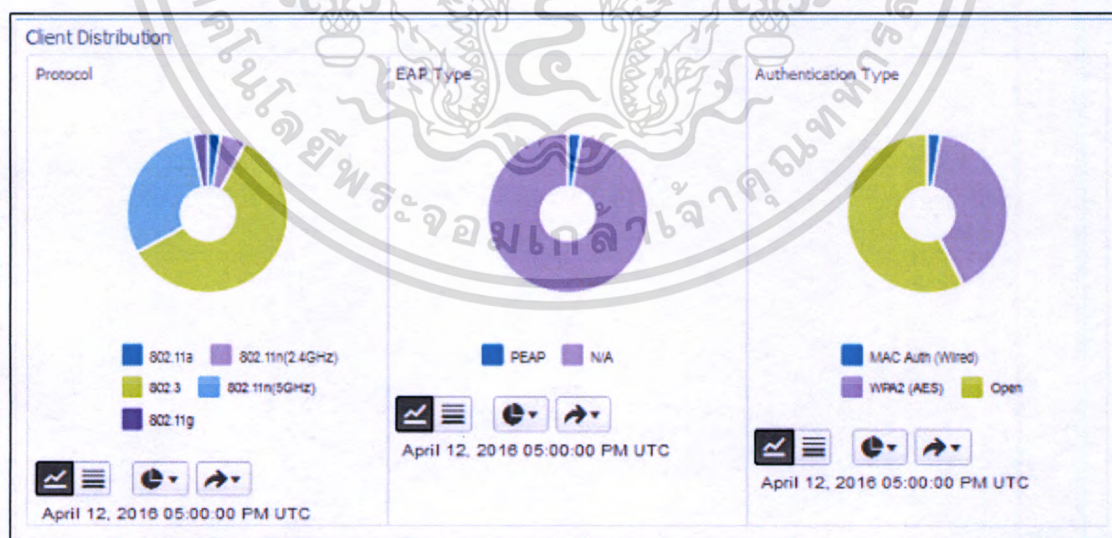
รูปที่ 4.40 แสดงแผนภูมิการเชื่อมต่อระหว่างผู้ใช้งานกับอุปกรณ์เครือข่ายไร้สาย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบบริหารจัดการเครือข่ายของซิสโก้สามารถแสดงปริมาณผู้ใช้งานที่มีการยืนยันตัวตนเข้าสู่เครือข่ายดังรูปที่ 4.41 และสามารถจัดประเภทตามชนิดของการยืนยันตัวตนเข้าสู่เครือข่ายดังรูปที่ 4.42



รูปที่ 4.41 แสดงปริมาณผู้ใช้งานที่มีการยืนยันตัวตนเข้าสู่เครือข่าย



รูปที่ 4.42 แสดงการจัดประเภทตามชนิดของการยืนยันตัวตนเข้าสู่เครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

นอกจากนี้ระบบบริหารจัดการเครือข่ายของซิสโก้ยังสามารถเก็บรวบรวมข้อมูลเหตุการณ์ที่เกิดขึ้นบนตัวอุปกรณ์เครือข่ายที่เกี่ยวข้องกับความมั่นคงปลอดภัยในระบบเครือข่าย โดยสามารถแสดงผลเป็นภาพรวมเหตุการณ์ที่เกิดขึ้นตามช่วงเวลาที่เกิดขึ้นดังรูปที่ 4.43 ทำให้ผู้ดูแลระบบสามารถเข้าไปตรวจสอบเหตุการณ์ที่เกิดขึ้นได้ดังรูปที่ 4.44 รวมถึงมีความสามารถในการตรวจสอบค่าการติดตั้งใช้งานที่อาจส่งผลให้เกิดความผิดพลาดด้านความปลอดภัยบนตัวอุปกรณ์เครือข่าย ดังรูปที่ 4.45 แสดงการตรวจสอบค่าการติดตั้งใช้งานที่อาจส่งผลให้เกิดความผิดพลาดด้านความปลอดภัยบนอุปกรณ์ควบคุมเครือข่ายไร้สายจากศูนย์กลาง

Attacks Detected	Last Hour	24 Hours	Total Active
Consolidated wIPS Alerts			
None detected			
wIPS Denial of Service Attacks			
Auth flood	0	14	0
Denauth flood	0	0	1
Broadcast Probe flood	0	2	0
wIPS Security Penetration Attacks			
None detected			
Performance Violation: Channel and Device Overload			
None detected			
User Authentication and Encryption			
None detected			
Custom Signature Events			
None detected			

รูปที่ 4.43 แสดงภาพรวมเหตุการณ์ด้านความปลอดภัยที่เกิดขึ้นตามช่วงเวลา

Description	Failure Source	Timestamp	Severity	Category	Condition
▶ 'Network User' 'host/CSW745.PANASONIC.CO.TH' faile...	User/host/CSW745.P...	April 12, 2016 9:27:2...	Information	Security	User auth...
▶ 'Network User' 'host/CSW745.PANASONIC.CO.TH' faile...	User/host/CSW745.P...	April 12, 2016 9:27:3...	Information	Security	User auth...
▶ 'Network User' 'host/CSW745.PANASONIC.CO.TH' faile...	User/host/CSW745.P...	April 12, 2016 9:27:3...	Information	Security	User auth...
▶ Client '2c33:7a:69:95:e2 (PANASONIC)02Thitima_so...	Trap for Client 2c33...	April 12, 2016 9:27:3...	Minor	Security	Client exc...
▶ Security-risk Interferer 'WiFi Inverted' is detected by 'A...	AP PIDTH-B5FL2-AP...	April 12, 2016 9:30:1...	Critical	Security	Interferer ...
▶ 'Network User' 'host/CSW796.PANASONIC.CO.TH' faile...	User/host/CSW796.P...	April 12, 2016 9:30:4...	Information	Security	User auth...
▶ 'Network User' 'host/CSW796.PANASONIC.CO.TH' faile...	User/host/CSW796.P...	April 12, 2016 9:30:4...	Information	Security	User auth...
▶ 'Network User' 'host/CSW796.PANASONIC.CO.TH' faile...	User/host/CSW796.P...	April 12, 2016 9:30:4...	Information	Security	User auth...
▶ Client '3c77:e9:a9:84:7d (PANASONIC)02Niparat_Mu...	Trap for Client 3c77...	April 12, 2016 9:30:4...	Minor	Security	Client exc...
▶ 'Network User' 'host/CSW724.PANASONIC.CO.TH' faile...	User/host/CSW724.P...	April 12, 2016 9:31:1...	Information	Security	User auth...
▶ 'Network User' 'host/CSW742.PANASONIC.CO.TH' faile...	User/host/CSW742.P...	April 12, 2016 9:31:5...	Information	Security	User auth...
▶ 'Network User' 'host/CSW735.PANASONIC.CO.TH' faile...	User/host/CSW735.P...	April 12, 2016 9:31:5...	Information	Security	User auth...
▶ 'Network User' '00fe1e2f16b3' failed authentication on ...	User/00fe1e2f16b3	April 12, 2016 9:32:0...	Information	Security	User auth...

รูปที่ 4.44 แสดงเหตุการณ์ด้านความปลอดภัยที่เกิดขึ้นบนอุปกรณ์เครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีกรณีนำไปใช้

... / Security / Security Index / View All / Security Index Detailed Report

- Select a command - Go

Entries 1 - 56 of 57
1 2 >>>>

IP Address	Device Name	Device Type	Device Security Issue	Security Solution	Acknowledged
137.40.78.29	PASAP-WLC02	Controller	WLAN SSID PASAP-RD-Guest on the controller has no key management methods (applicable only for WPA+WPA2) configured.	Configure at least one key management methods such as CC/M.	No
137.40.78.29	PASAP-WLC02	Controller	WLAN SSID PASAP-RD-Guest on the controller has "MFP Client Protection" set to "Optional".	Set "MFP Client Protection" to "Required" to protect against clients connecting to a rogue AP.	No
137.40.78.29	PASAP-WLC02	Controller	WLAN SSID PASAP-RD-Office on the controller has "MFP Client Protection" set to "Optional".	Set "MFP Client Protection" to "Required" to protect against clients connecting to a rogue AP.	No
137.40.78.29	PASAP-WLC02	Controller	WLAN SSID PASAP-RD-Guest on the controller has no encryption configured.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.	No
172.16.5.251	WLC5508-B5	Controller	WLAN SSID PASAPW44 on the controller has "MFP Client Protection" set to "Optional".	Set "MFP Client Protection" to "Required" to protect against clients connecting to a rogue AP.	No
172.16.5.251	WLC5508-B5	Controller	WLAN SSID PIDTH-WiFi3 on the controller has "MFP Client Protection" set to "Optional".	Set "MFP Client Protection" to "Required" to protect against clients connecting to a rogue AP.	No
172.16.5.251	WLC5508-B5	Controller	WLAN SSID PIDTH-WiFi2 on the controller has "MFP Client Protection" set to "Optional".	Set "MFP Client Protection" to "Required" to protect against clients connecting to a rogue AP.	No
172.16.5.251	WLC5508-B5	Controller	WLAN SSID PIDTH-Guest1 on the controller has "MFP Client Protection" set to "Optional".	Set "MFP Client Protection" to "Required" to protect against clients connecting to a rogue AP.	No
172.16.5.251	WLC5508-B5	Controller	WLAN SSID PIDTH-WiFi4 on the controller has "MFP Client Protection" set to "Optional".	Set "MFP Client Protection" to "Required" to protect against clients connecting to a rogue AP.	No
172.16.5.251	WLC5508-B5	Controller	WLAN SSID PIDTH-WiFi on the controller has "MFP Client Protection" set to "Optional".	Set "MFP Client Protection" to "Required" to protect against clients connecting to a rogue AP.	No
172.16.5.251	WLC5508-B5	Controller	"Protection Type" is set to "None" on the controller.	Set "Protection Type" to "Management Frame Protection (MFP)" on the controller.	No
172.16.5.251	WLC5508-B5	Controller	No CIDS Sensor configured on the controller.	Configure at least one CIDS Sensor on the controller.	No
172.16.5.251	WLC5508-B5	Controller	Telnet is enabled on the controller.	Disable telnet on the controller.	No
137.40.78.80	PASAP-WLC01	Controller	WLAN SSID PASAPW46 on the controller has "MFP Client Protection" set to "Optional".	Set "MFP Client Protection" to "Required" to protect against clients connecting to a rogue AP.	No
137.40.78.80	PASAP-WLC01	Controller	WLAN SSID PASAP-Guest on the controller has "MFP Client Protection" set to "Optional".	Set "MFP Client Protection" to "Required" to protect against clients connecting to a rogue AP.	No
137.40.78.80	PASAP-WLC01	Controller	WLAN SSID PASAPW45 on the controller has "MFP Client Protection" set to "Optional".	Set "MFP Client Protection" to "Required" to protect against clients connecting to a rogue AP.	No
137.40.78.80	PASAP-WLC01	Controller	WLAN SSID PASAP-Handheld on the controller has "MFP Client Protection" set to "Optional".	Set "MFP Client Protection" to "Required" to protect against clients connecting to a rogue AP.	No

รูปที่ 4.45 แสดงค่าการติดตั้งใช้งานที่อาจส่งผลให้เกิดความผิดพลาดด้านความปลอดภัย

4.6 ความสามารถในการบริหารจัดการเครือข่ายด้านอื่นๆ

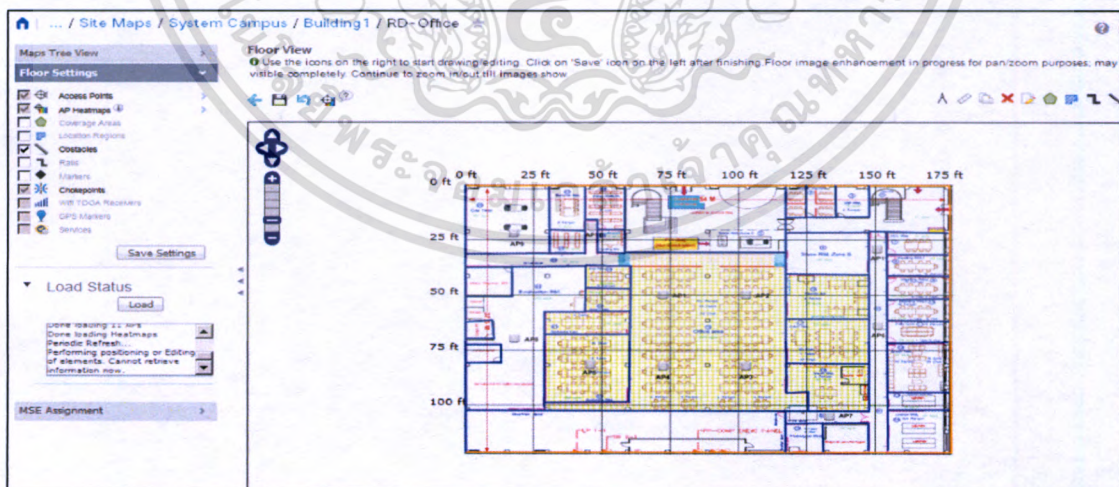
ระบบบริหารจัดการเครือข่ายของซิสโก้มีความสามารถในการบริหารจัดการเครือข่ายด้านอื่นๆอีกที่นอกเหนือจากโมเดลมาตรฐานด้านการบริหารจัดการเครือข่าย (FCAPS Model) และมีเครื่องมือที่สามารถช่วยอำนวยความสะดวกในการบริหารจัดการเครือข่ายให้ด้านอื่นๆให้กับผู้ดูแลระบบเครือข่ายอีกด้วย ดังนี้

4.6.1 การทำแผนภาพแสดงสัญญาณคลื่นวิทยุของอุปกรณ์เครือข่ายไร้สาย

ระบบบริหารจัดการเครือข่ายของซิสโก้มีเครื่องมือที่ช่วยในการจัดทำแผนภาพจำลองแสดงสัญญาณคลื่นวิทยุของอุปกรณ์เครือข่ายไร้สายที่ติดตั้งใช้งานตามพื้นที่ต่างๆ ซึ่งเครื่องมือนี้มีประโยชน์อย่างมากเพราะช่วยให้ผู้ดูแลระบบเครือข่ายสามารถออกแบบระบบเครือข่ายไร้สายได้อย่างสะดวกและใกล้เคียงกับความเป็นจริง เพราะการออกแบบระบบเครือข่ายไร้สายจะแตกต่างจากการออกแบบระบบเครือข่ายแบบใช้สาย เนื่องจากระบบเครือข่ายไร้สายใช้สัญญาณคลื่นวิทยุซึ่งไม่สามารถมองเห็นได้ด้วยตาเปล่า ดังนั้นการจะออกแบบระบบเครือข่ายไร้สายให้ครอบคลุมพื้นที่ในการให้บริการนั้นจึงเป็นเรื่องยากหากไม่มีเครื่องมือนี้ ซึ่งอาจส่งผลทำให้การออกแบบระบบเครือข่ายไร้สายเกิดความผิดพลาดขึ้น เช่น ทำให้ออกแบบระบบเครือข่ายไร้สายที่มีสัญญาณไม่ครอบคลุมพื้นที่การให้บริการเนื่องจากจำนวนตัวส่งสัญญาณมีจำนวนน้อยเกินไปหรือติดตั้งในตำแหน่งที่ไม่เหมาะสมทำให้ลดประสิทธิภาพในการกระจายสัญญาณ หรือทำให้ออกแบบระบบ

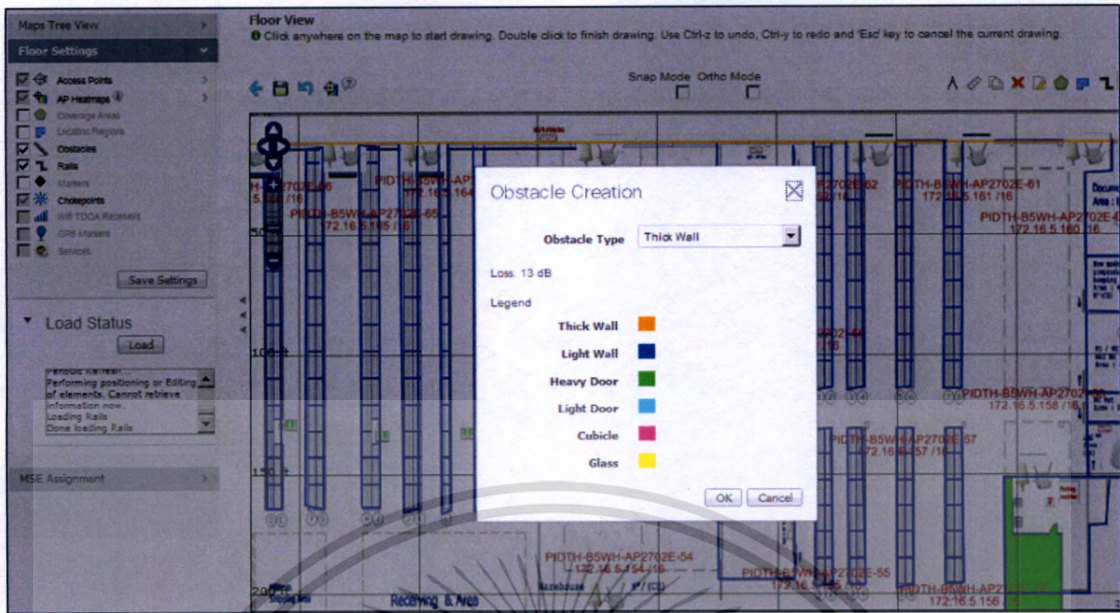
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เครือข่ายไร้สายที่มีจำนวนตัวส่งสัญญาณมากเกินไปทำให้งบประมาณในการดำเนินงานสูงเกินกว่าความเป็นจริง ซึ่งปัญหาที่เกิดขึ้นได้เกิดขึ้นกับผู้จัดทำมาแล้ว ดังนั้นจึงได้มีการทดลองและทดสอบเครื่องมือออกแบบจำลองการกระจายสัญญาณคลื่นวิทยุของอุปกรณ์เครือข่ายไร้สายที่มีในระบบบริหารจัดการเครือข่ายของซิสโก้ โดยขั้นตอนการออกแบบจำลองการกระจายสัญญาณคลื่นวิทยุของอุปกรณ์เครือข่ายไร้สาย สามารถทำได้โดยนำเอารูปของพื้นที่ใช้งานจริงที่จะทำการติดตั้งระบบเครือข่ายไร้สายเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้ดังรูปที่ 4.46 จากนั้นทำการใส่ข้อมูลขนาดของพื้นที่ เช่น ขนาดความกว้าง ยาวและความสูงของพื้นที่ ลักษณะและชนิดของผนังหรือสิ่งกีดขวางสัญญาณวิทยุในพื้นที่ติดตั้งจริงดังรูปที่ 4.47 จากนั้นทำการเลือกชนิดของตัวส่งสัญญาณซึ่งระบบบริหารจัดการเครือข่ายของซิสโก้จะมีข้อมูลรุ่นของตัวส่งสัญญาณของซิสโก้ให้เลือกตามที่เราต้องการจะใช้ดังรูปที่ 4.48 เมื่อทำการเลือกชนิดของตัวส่งสัญญาณเรียบร้อยแล้ว ชนิดของตัวส่งสัญญาณเป็นแบบที่สามารถเปลี่ยนแปลงเสาส่งสัญญาณได้ ระบบบริหารจัดการเครือข่ายของซิสโก้จะมีข้อมูลรุ่นของเสาส่งสัญญาณของซิสโก้ให้เลือกดังรูปที่ 4.49 ควรเลือกตัวส่งสัญญาณและเสาส่งสัญญาณให้ถูกต้องและตามความเป็นจริงเพราะจะมีผลต่อการออกแบบจำลองการกระจายสัญญาณคลื่นวิทยุของอุปกรณ์เครือข่ายไร้สาย เมื่อใส่ข้อมูลครบถ้วนระบบบริหารจัดการเครือข่ายของซิสโก้จะทำการสร้างแบบจำลองการกระจายสัญญาณคลื่นวิทยุของอุปกรณ์เครือข่ายไร้สายบนพื้นที่ที่เราต้องการจะติดตั้งจริงดังรูปที่ 4.50 ทำให้ผู้ดูแลระบบสามารถสร้างแบบจำลองการกระจายสัญญาณคลื่นวิทยุของอุปกรณ์เครือข่ายไร้สายเพื่อให้เหมาะสมกับการใช้งานจริง และลดความผิดพลาดในการออกแบบระบบเครือข่ายไร้สายได้อีกด้วย

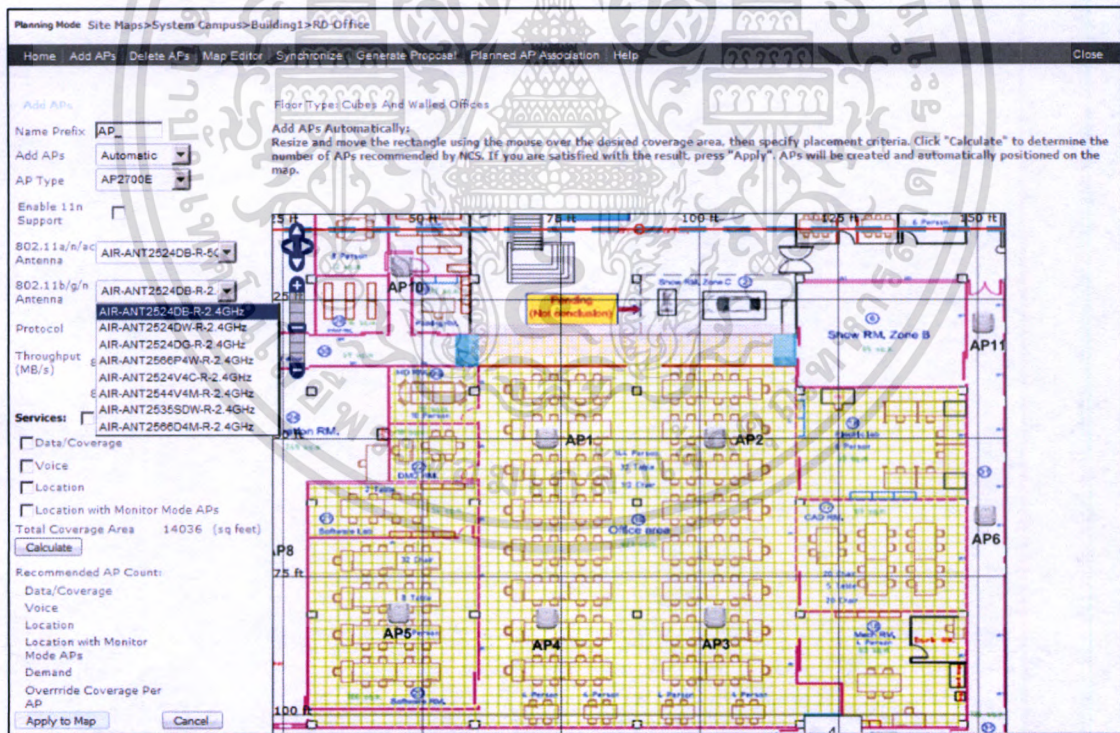


รูปที่ 4.46 การออกแบบจำลองเครือข่ายไร้สายจากพื้นที่ใช้งานจริง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

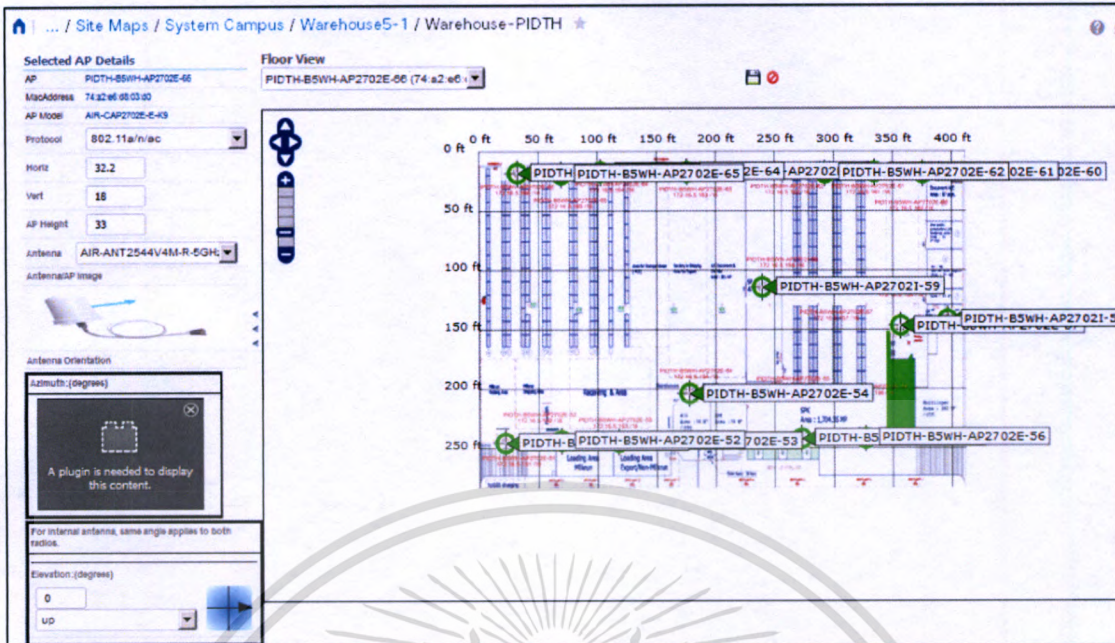


รูปที่ 4.47 การกำหนดชนิดของผนังหรือสิ่งกีดขวางสัญญาณวิทยุตามพื้นที่ใช้งานจริง

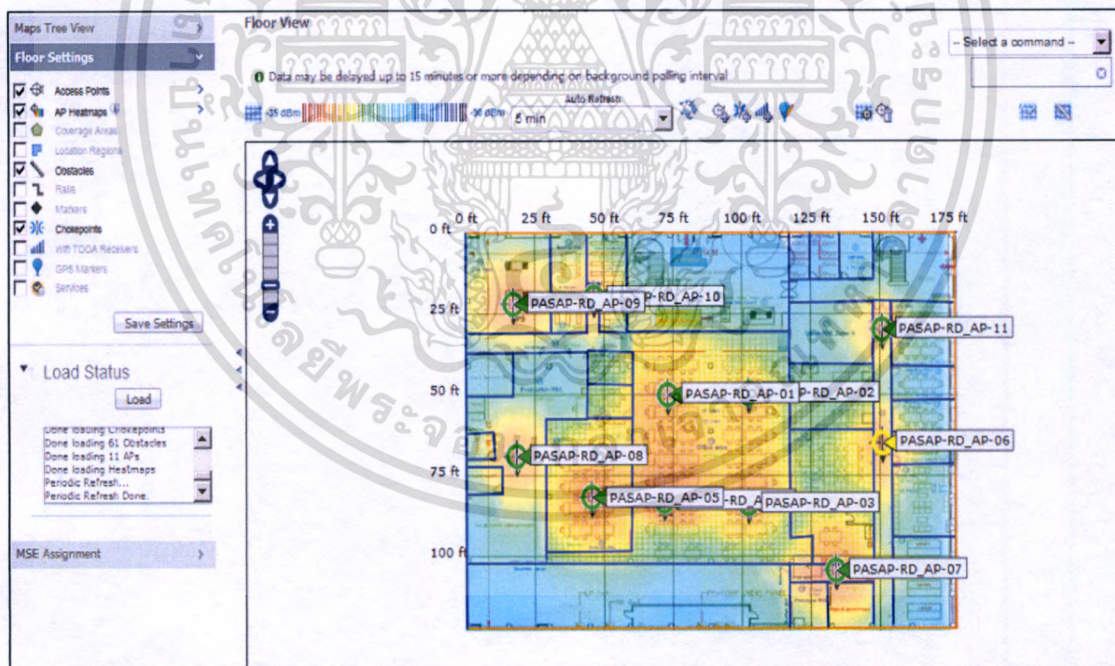


รูปที่ 4.48 การกำหนดชนิดของตัวส่งสัญญาณวิทยุตามพื้นที่ใช้งานจริง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีกรนำไปใช้



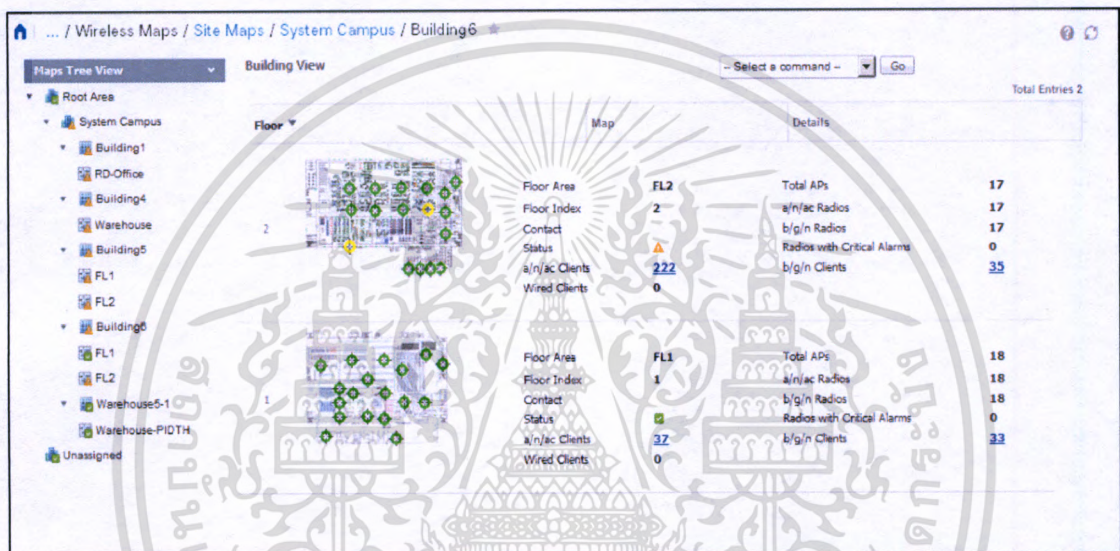
รูปที่ 4.49 การกำหนดชนิดของเสาส่งสัญญาณวิทยุตามพื้นที่ใช้งานจริง



รูปที่ 4.50 แสดงแบบจำลองการกระจายสัญญาณวิทยุตามพื้นที่ใช้งานจริง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

นอกจากระบบบริหารจัดการเครือข่ายของซิสโก้จะมีเครื่องมือที่ช่วยในการจัดทำแผนภาพจำลอง แสดงสัญญาณคลื่นวิทยุของอุปกรณ์เครือข่ายไร้สายก่อนที่จะมีการติดตั้งใช้งานจริงตามพื้นที่ต่างๆ แล้ว ระบบบริหารจัดการเครือข่ายของซิสโก้ยังสามารถแสดงแบบจำลองการกระจายสัญญาณวิทยุตามพื้นที่ใช้งานจริงที่มีการติดตั้งอุปกรณ์เครือข่ายไร้สายไปแล้วดังรูปที่ 4.51 โดยระบบบริหารจัดการเครือข่ายของซิสโก้จะแสดงรายละเอียดการใช้งานระบบเครือข่ายไร้สายในแต่ละพื้นที่ดังรูปที่ 4.52 ทำให้ผู้ดูแลระบบสามารถนำข้อมูลไปใช้ในการบริหารจัดการระบบเครือข่ายไร้สายได้อย่างมีประสิทธิภาพ



รูปที่ 4.51 แสดงการติดตั้งใช้งานอุปกรณ์เครือข่ายไร้สายในแต่ละพื้นที่

Coverage Area | View Maps

Total APs not yet assigned to maps - Unified: 0 | Autonomous: 0

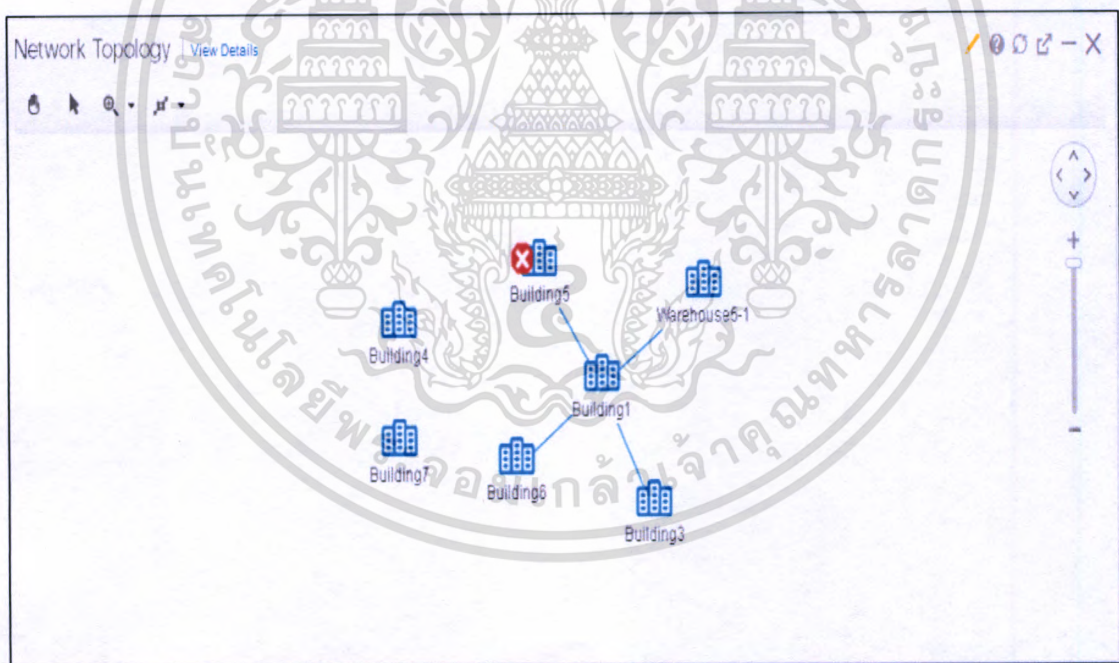
Name	Total APs	Radios			Alarms	Clients	
		5 GHz	2.4 GHz	Wireless		Wired	
Building6	35	35	35	0	325	0	
Building5	35	35	35	0	2	0	
Building4	21	21	21	0	8	0	
Warehouse5-1	16	16	16	0	0	0	
Building1	11	11	11	0	2	0	

รูปที่ 4.52 แสดงการใช้งานบนอุปกรณ์เครือข่ายไร้สายในแต่ละพื้นที่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับกรใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

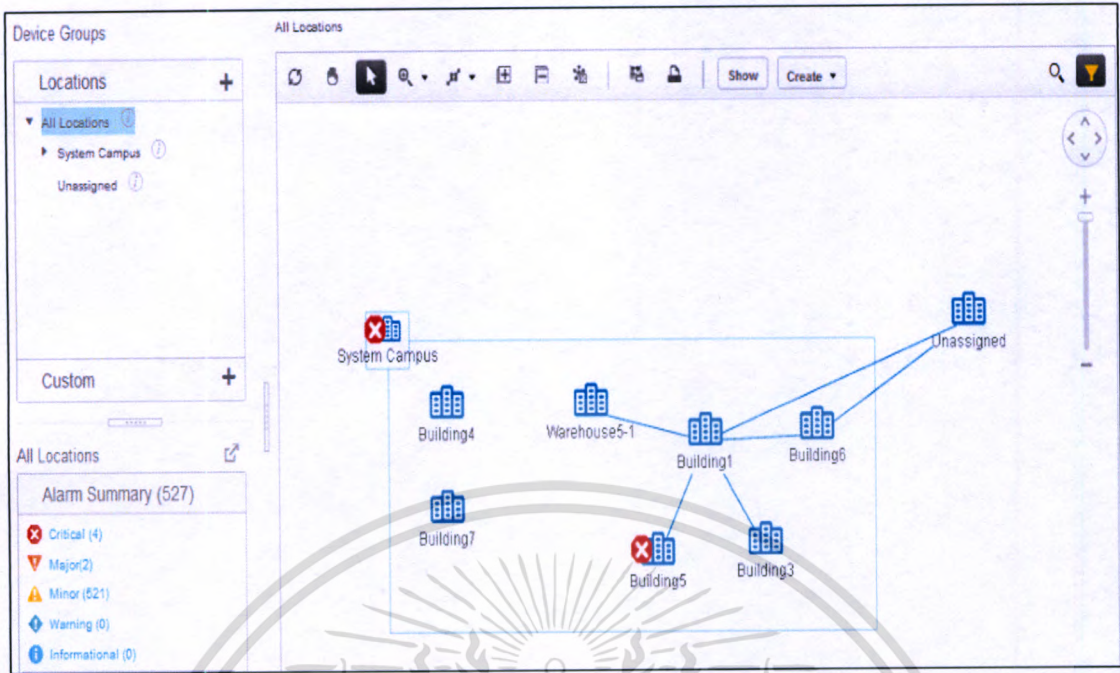
4.6.2 การแสดงแผนภูมิการเชื่อมต่อของอุปกรณ์เครือข่าย

ระบบบริหารจัดการเครือข่ายของซิสโก้มีเครื่องมือที่ช่วยในการจัดทำแผนภาพการเชื่อมต่อของอุปกรณ์ต่างๆในระบบเครือข่าย ทำให้ผู้ดูแลระบบสามารถมองเห็นภาพรวมในการเชื่อมต่ออุปกรณ์ต่างๆในระบบเครือข่าย โดยระบบบริหารจัดการเครือข่ายของซิสโก้จะใช้โปรโตคอลที่มีชื่อว่า Cisco Discovery Protocol หรือ (CDP) ซึ่งถูกออกแบบและพัฒนาโดยบริษัทซิสโก้ ในการแสดงการเชื่อมต่อของอุปกรณ์เครือข่ายต่างๆในระบบเครือข่ายดังรูปที่ 4.53 โดยโปรโตคอล CDP ที่อยู่บนตัวอุปกรณ์เครือข่ายและมีการเปิดใช้งาน โปรโตคอลนี้ จะทำการส่งข้อมูลการเชื่อมต่อให้กับระบบบริหารจัดการเครือข่ายของซิสโก้เพื่อใช้ในการสร้างแผนภาพการเชื่อมต่อของอุปกรณ์เครือข่ายต่างๆในระบบเครือข่าย โดยระบบบริหารจัดการเครือข่ายของซิสโก้จะสามารถทำการแยกกลุ่มของอุปกรณ์เครือข่ายตามพื้นที่ที่ติดตั้งใช้งาน ซึ่งจะถูกกำหนดโดยผู้ดูแลระบบเครือข่ายดังรูปที่ 4.54 ส่วนโปรโตคอล CDP จะแสดงข้อมูลการเชื่อมต่อระหว่างอุปกรณ์เครือข่ายที่มีการเชื่อมต่อกันโดยตรงเท่านั้นดังรูปที่ 4.55 ทำให้ผู้ดูแลระบบมองเห็นภาพรวมในการเชื่อมต่ออุปกรณ์ต่างๆในระบบเครือข่ายและสามารถทำการบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

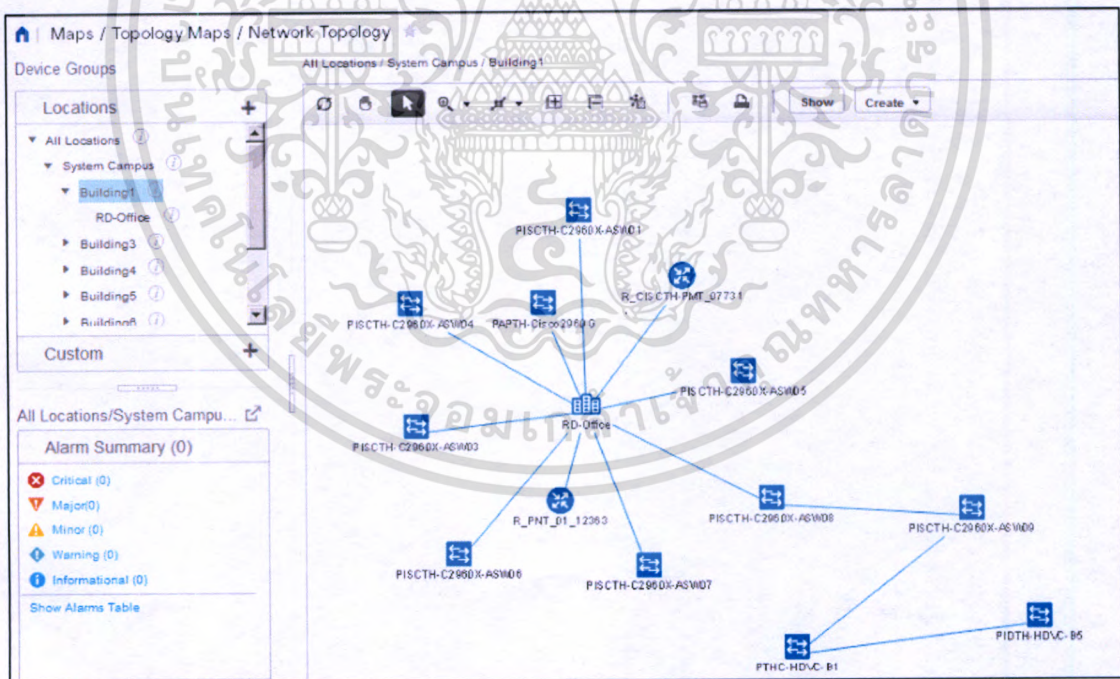


รูปที่ 4.53 แสดงภาพรวมในการเชื่อมต่ออุปกรณ์ต่างๆในระบบเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.54 แสดงการเชื่อมต่อตามกลุ่มพื้นที่ที่ติดตั้งใช้งานของอุปกรณ์เครือข่าย



รูปที่ 4.55 แสดงการเชื่อมต่อของอุปกรณ์เครือข่ายที่ใช้โปรโตคอล CDP

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.6.3 การสร้างรูปแบบรายงานและแสดงผลรายงาน

งานที่ผู้ดูแลระบบเครือข่ายต้องดำเนินการในการบริหารจัดการเครือข่ายอีกอย่างคือ การสร้างรูปแบบรายงานและแสดงผลรายงานสถานะของอุปกรณ์เครือข่ายหรือภาพรวมของระบบเครือข่าย เพื่อรายงานข้อมูลให้กับผู้บริหารหรือผู้ตรวจสอบระบบได้ทราบข้อมูลการทำงานและการบริหารจัดการเครือข่ายของผู้ดูแลระบบเครือข่าย เช่น รายการจำนวนของอุปกรณ์เครือข่ายทั้งหมดที่ติดตั้ง หรือรายการจำนวนของอุปกรณ์เครือข่ายแยกตามชนิดของอุปกรณ์เครือข่าย เป็นต้น จากปัญหาที่ผู้จัดทำพบในองค์กรคือ ต้องมีการสร้างรูปแบบรายงานและแสดงผลรายงานสถานะของอุปกรณ์เครือข่ายหรือภาพรวมของระบบเครือข่าย เพื่อรายงานให้กับผู้บริหารหรือผู้ตรวจสอบระบบได้ทราบข้อมูลในทุกๆเดือน ยกตัวอย่างรายงานที่ต้องส่งให้กับบริหารและผู้ตรวจสอบระบบ เช่น รายการจำนวนของอุปกรณ์เครือข่ายทั้งหมด ซึ่งต้องใช้เวลาในการจัดทำและต้องมีการปรับปรุงเปลี่ยนแปลงอยู่ตลอดเพราะมีการเพิ่มและปรับเปลี่ยนอุปกรณ์ในระบบเครือข่ายอยู่เสมอ ถ้าไม่มีเครื่องมือที่ช่วยในการดำเนินงานสร้างรูปแบบและแสดงผลรายงานจะทำให้เพิ่มภาระการทำงานให้กับผู้ดูแลระบบอย่างมาก และในบางครั้งอาจเกิดความผิดพลาดขึ้นในการแสดงผลรายงานอันเนื่องมาจากการจัดทำข้อมูลที่ผิดพลาดของผู้ดูแลระบบ จากการทดลองและทดสอบระบบบริหารจัดการเครือข่ายของซิสโก้ในด้านกรสร้างรูปแบบรายงานและแสดงผลรายงานสถานะของอุปกรณ์เครือข่ายหรือภาพรวมของระบบเครือข่าย ระบบบริหารจัดการเครือข่ายของซิสโก้ มีเครื่องมือที่ช่วยอำนวยความสะดวกในการจัดทำรายงานในการบริหารจัดการเครือข่าย โดยระบบบริหารจัดการเครือข่ายของซิสโก้จะมีรูปแบบรายงานที่ใช้จัดทำรายงานในการบริหารจัดการเครือข่ายให้ผู้ดูแลระบบเครือข่ายสามารถได้เลือกใช้ ดังรูปที่ 4.56 ทำให้ผู้ดูแลระบบเครือข่ายเลือกใช้รูปแบบและสามารถจัดทำรายงานได้อย่างสะดวกและรวดเร็ว ทำให้ช่วยภาระการทำงานและลดเวลาที่ต้องเสียไปในการจัดทำรายงาน ให้กับผู้บริหารหรือผู้ตรวจสอบระบบได้ทราบข้อมูลในทุกๆเดือน



รูปที่ 4.56 แสดงรูปแบบรายงานที่ใช้จัดทำรายงานในระบบบริหารจัดการเครือข่ายของซิสโก้

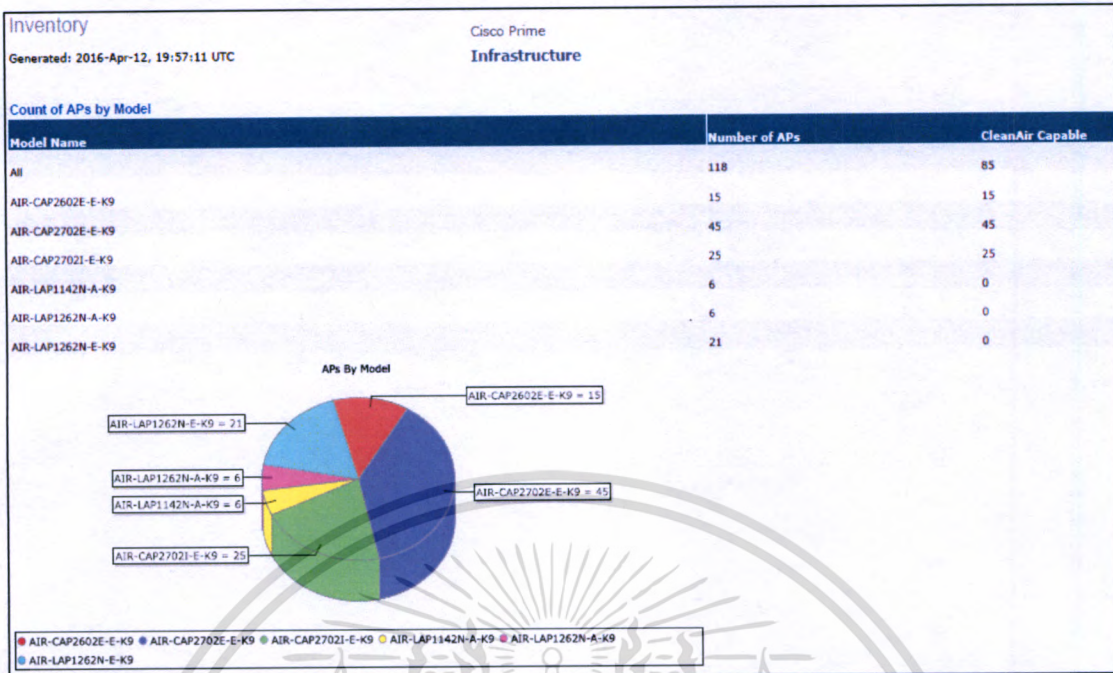
นอกจากระบบบริหารจัดการเครือข่ายของซิสโก้จะมีเครื่องมือที่สามารถทำการสร้างรายงานให้กับผู้ดูแลระบบแล้ว ระบบบริหารจัดการเครือข่ายของซิสโก้ยังสามารถตั้งเวลาในการจัดส่งรายงานให้กับผู้ดูแลระบบได้โดยอัตโนมัติตามช่วงเวลาที่กำหนด โดยผู้ดูแลระบบสามารถเข้าไปปรับแต่งค่าต่างๆเพื่อสร้างรูปแบบรายงานและกำหนดเวลาในการจัดส่งรายงานบนระบบบริหารจัดการเครือข่ายของซิสโก้ได้ เช่น สามารถเลือกข้อมูลที่จะแสดงในรายงานได้ หรือเลือกชนิดของไฟล์รายงานที่จะให้แสดงผลโดยระบบบริหารจัดการเครือข่ายของซิสโก้สามารถเลือกชนิดของไฟล์รายงานที่จะให้แสดงผลได้เป็น 2 แบบคือ ไฟล์ PDF และไฟล์ CSV ดังรูปที่ 4.57 นอกจากนี้ระบบบริหารจัดการเครือข่ายของซิสโก้ยังสามารถเลือกได้ว่าจะให้ระบบบริหารจัดการเครือข่ายของซิสโก้ทำการส่งรายงานไปให้ผู้ดูแลระบบผ่านทางอีเมลด้วยหรือไม่ เพราะนอกจากระบบบริหารจัดการเครือข่ายของซิสโก้จะสามารถสร้างรายงานให้กับผู้ดูแลระบบได้โดยอัตโนมัติตามช่วงเวลาที่ผู้ดูแลระบบกำหนดแล้วยังสามารถส่งอีเมลรายงานให้กับผู้ดูแลระบบหรือผู้ที่เกี่ยวข้องที่ต้องการรายงานให้โดยอัตโนมัติ ดังรูปที่ 4.58 ซึ่งตัวอย่างรูปแบบรายงานของระบบบริหารจัดการเครือข่ายของซิสโก้จะแสดงในรูปที่ 4.59 และ 4.60

รูปที่ 4.57 แสดงการสร้างรายงานให้กับผู้ดูแลระบบอัตโนมัติตามช่วงเวลาที่กำหนด

Report Title	Report Type	Scheduled	Virtual Domain	Run Now	Total Entries
AP Inventory	Inventory	Enabled	ROOT-DOMAIN	✓	2
Inventory	Inventory	Enabled	ROOT-DOMAIN	✓	2

รูปที่ 4.58 แสดงสถานะการสร้างรายงานอัตโนมัติตามที่ผู้ดูแลระบบกำหนด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีกรนำมาไปใช้



รูปที่ 4.59 แสดงรูปแบบรายงานของระบบบริหารจัดการเครือข่ายของซิสโก้

AP Inventory

AP Name	Model	Serial Number	AP IP Address	Map Location	Software Version	Primary Controller Name	Secondary Controller Name
AP-201	AIR-LAP1142N-A-K9	FGL1512S2PU	172.16.6.201	System Campus > Building6 > FL2	8.0.121.0	PASAP-WLC02	PASAP-WLC01
AP-202	AIR-LAP1142N-A-K9	FGL1512S2PR	172.16.6.202	System Campus > Building6 > FL2	8.0.121.0	PASAP-WLC02	PASAP-WLC01
AP-203	AIR-LAP1142N-A-K9	FGL1512S2PP	172.16.6.203	System Campus > Building6 > FL2	8.0.121.0	PASAP-WLC02	PASAP-WLC01
AP-204	AIR-LAP1142N-A-K9	FGL1512S2PN	172.16.6.204	System Campus > Building6 > FL2	8.0.121.0	PASAP-WLC02	PASAP-WLC01
AP-205	AIR-LAP1142N-A-K9	FGL1512S2PT	172.16.6.205	System Campus > Building6 > FL1	8.0.121.0	PASAP-WLC01	PASAP-WLC02
AP-206	AIR-LAP1262N-E-K9	FGL16345QA	172.16.6.206	System Campus > Building6 > FL1	8.0.121.0	PASAP-WLC01	PASAP-WLC02
AP-207	AIR-LAP1142N-A-K9	FGL1512S2PS	172.16.6.207	System Campus > Building6 > FL1	8.0.121.0	PASAP-WLC01	PASAP-WLC02
AP-208	AIR-LAP1262N-A-K9	FGL1512S2QS	172.16.6.208	System Campus > Building6 > FL2	8.0.121.0	PASAP-WLC02	PASAP-WLC01
AP-209	AIR-LAP1262N-A-K9	FGL1512S2QY	172.16.6.209	System Campus > Building6 > FL2	8.0.121.0	PASAP-WLC02	PASAP-WLC01
AP-210	AIR-LAP1262N-A-K9	FGL1512S2QR	172.16.6.210	System Campus > Building6 > FL2	8.0.121.0	PASAP-WLC02	PASAP-WLC01
AP-211	AIR-LAP1262N-A-K9	FGL1512S2QN	172.16.6.211	System Campus > Building6 > FL1	8.0.121.0	PASAP-WLC01	PASAP-WLC02
AP-212	AIR-CAP2602E-E-K9	FGL1806XNA	172.16.6.212	System Campus > Building6 > FL1	8.0.121.0	PASAP-WLC01	PASAP-WLC02
AP-213	AIR-LAP1262N-A-K9	FGL1512S2QP	172.16.6.213	System Campus > Building6 > FL2	8.0.121.0	PASAP-WLC02	PASAP-WLC01
AP-214	AIR-LAP1262N-E-K9	FGL16345QB	172.16.6.214	System Campus > Building6 > FL1	8.0.121.0	PASAP-WLC01	PASAP-WLC02

รูปที่ 4.60 แสดงรายละเอียดของข้อมูลในรายงาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5

บทสรุป

5.1 สรุปผลการทดลองและทดสอบระบบ

จากการศึกษา ทดลองและทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) โดยใช้โมเดลมาตรฐานในการบริหารจัดการเครือข่าย หรือ FCAPS Model ทั้ง 5 ด้าน คือ การจัดการด้านความผิดพลาด การจัดการค่าที่ติดตั้งไว้ การจัดการบัญชีผู้ใช้งาน การจัดการด้านประสิทธิภาพ และการจัดการด้านความปลอดภัย มาใช้เป็นเกณฑ์ในการวัดผล ด้านการบริหารจัดการระบบเครือข่ายของซอฟต์แวร์และแวร์ระบบบริหารจัดการเครือข่ายของซิสโก้โดยได้ใช้สภาพแวดล้อมในระบบเครือข่ายขององค์กรที่ใช้งานอยู่จริงในการทดลองและทดสอบระบบ รวมถึงได้ทำการทดลองและทดสอบความสามารถของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ในการแก้ไขปัญหาที่เกิดจากการทำงานจริงในระบบเครือข่ายขององค์กร พบว่าซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ มีคุณสมบัติเหมาะสมและตรงต่อความต้องการในการใช้งานด้านการบริหารจัดการเครือข่าย รวมทั้งสามารถรองรับการทำงานกับทุกอุปกรณ์เครือข่ายของซิสโก้ที่ติดตั้งใช้งานอยู่จริงในระบบเครือข่ายขององค์กร นอกจากนี้ยังมีเครื่องมือที่ช่วยแก้ไขปัญหาและอำนวยความสะดวกในการทำงานให้กับผู้ดูแลระบบเครือข่าย ทำให้สามารถลดภาระการทำงานที่เคยทำอยู่เดิม ลดเวลาในการดำเนินการ และช่วยเพิ่มประสิทธิภาพในการบริหารจัดการเครือข่ายให้กับผู้ดูแลระบบเครือข่าย

ผลที่ได้จากการศึกษา ทดลองและทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้บนสภาพแวดล้อมของระบบเครือข่ายที่ใช้งานอยู่จริงในองค์กร ทำให้สามารถทราบข้อมูลคุณสมบัติ ประสิทธิภาพในการบริหารจัดการเครือข่ายและความสามารถในการช่วยเหลือผู้ดูแลระบบเครือข่ายแก้ไขปัญหาที่เกิดขึ้นในระบบเครือข่าย ของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ ก่อนที่จะดำเนินการจัดซื้อและติดตั้งใช้งานจริง และสามารถนำผลที่ได้จากการศึกษา ทดลองและทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ มานำเสนอกับผู้บริหารเพื่อใช้ในการตัดสินใจและเลือกใช้ระบบบริหารจัดการเครือข่ายภายในองค์กร โดยผู้บริหารได้ทำการตัดสินใจและเลือกใช้ระบบบริหารจัดการเครือข่ายของซิสโก้ บนระบบเครือข่ายในองค์กรเป็นที่เรียบร้อยแล้ว ซึ่งตอนนี้อยู่ในระหว่างรอดำเนินการซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ เพื่อติดตั้งใช้งานจริงในองค์กร

5.2 ปัญหาและข้อจำกัด

ปัญหาที่พบจากการศึกษา ทดลองและทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure) บนระบบเครือข่ายในองค์กรที่ใช้งานอยู่จริง คือ เกิดจากฟังก์ชันบนตัวซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ที่มีความสามารถและสนับสนุนการทำงานที่หลากหลายด้านการบริหารจัดการเครือข่าย ทำให้มีความผิดพลาดและการทำงานไม่สมบูรณ์ในบางฟังก์ชัน เช่น ปัญหาไม่สามารถลบข้อมูลของอุปกรณ์เครือข่ายที่ไม่ต้องการออกจากตัวซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ แต่หลังจากที่ได้ทำการแจ้งปัญหาไปยังฝ่ายบริการและสนับสนุนของบริษัทซิสโก้ ทางบริษัทซิสโก้ได้ดำเนินการแก้ไข โดยได้ออกซอฟต์แวร์เสริมเพื่อใช้ปรับปรุงซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้และสามารถแก้ไขปัญหานั้นได้

ข้อจำกัดที่พบบนตัวซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ หลังจากได้ทำการศึกษา ทดลองและทดสอบใช้งาน คือ ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้จะทำงานได้เต็มประสิทธิภาพเมื่อทำงานร่วมกับอุปกรณ์เครือข่ายของซิสโก้เท่านั้น ถึงแม้ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้จะสามารถทำงานร่วมกับอุปกรณ์เครือข่ายของบริษัทอื่นได้ แต่ก็ไม่ได้เต็มประสิทธิภาพ และในบางอุปกรณ์เครือข่ายที่เป็นของบริษัทอื่นซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้จะไม่สามารถทำงานร่วมกันได้ แต่เนื่องจากในระบบเครือข่ายขององค์กร อุปกรณ์เครือข่ายส่วนใหญ่เป็นของบริษัทซิสโก้และได้มีแผนที่จะทำการเปลี่ยนอุปกรณ์เครือข่ายของบริษัทอื่นให้เป็นอุปกรณ์เครือข่ายของบริษัทซิสโก้อยู่แล้ว ทำให้สามารถแก้ไขปัญหของข้อจำกัดนี้ได้ นอกจากนี้ยังพบข้อจำกัดบนตัวซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ในด้านฟังก์ชันการทำงาน เช่น การแก้ไขค่าการติดตั้งบนตัวอุปกรณ์เครือข่ายของซิสโก้ในรุ่นเก่าๆ บางรุ่น ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้จะไม่สามารถทำการแก้ไขค่าการติดตั้งได้เต็มประสิทธิภาพ โดยทำได้แค่เพียงบางส่วนและยังต้องทำการใช้งานผ่านคอมพิวเตอร์ไคลน์ในการแก้ไขค่าการติดตั้งบนตัวอุปกรณ์เครือข่ายแบบเดิมอยู่

5.3 ข้อเสนอแนะและแนวทางการพัฒนาในอนาคต

เนื่องจากต้องมีการใช้ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ในการบริหารจัดการเครือข่ายในองค์กร และจากการดำเนินงานที่ผ่านมาเป็นการศึกษา ทดลองและทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ เพื่อให้สามารถทราบข้อมูลคุณสมบัติ การทำงานและประสิทธิภาพในการบริหารจัดการเครือข่ายของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ ก่อนที่จะดำเนินการจัดซื้อและติดตั้งใช้งานจริง ดังนั้นจึงควรทำการศึกษางานของ

ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ให้เข้าใจ เพื่อที่จะใช้ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ให้เต็มประสิทธิภาพ และควรเตรียมแนวทางการพัฒนาระบบในอนาคต หลังจากทำการติดตั้งใช้งานซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ในองค์กรแล้ว โดยจะต้องจัดเตรียมแผนในการดูแลรักษาซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ในด้านต่างๆ เช่น การขยายตัวของระบบในอนาคต การดูแลเรื่องของการจัดเก็บและสำรองค่าที่ตั้งไว้บนซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ แผนสำรองเมื่อซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ไม่สามารถใช้งานได้ แผนในการกู้คืนระบบเมื่อระบบเกิดความเสียหาย และสามารถทำให้ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ทำงานร่วมกับระบบต่างๆ ได้อย่างมีประสิทธิภาพ



บรรณานุกรม

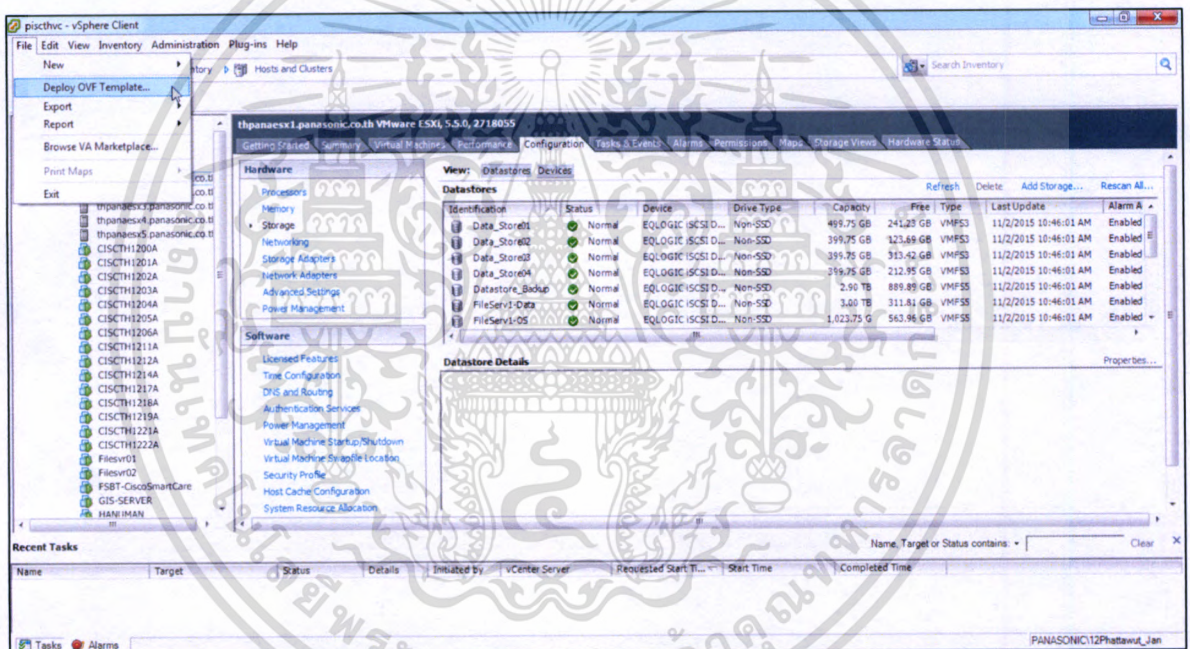
- Cisco Prime Infrastructure 3.0 Data Sheet. 2015. September. [Online]. Available:
<http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-infrastructure/datasheet-c78-735696.html>
- Douglas Bruey. 2005. December. “**SNMP: Simple Network Management Protocol**” Rane Corporation. [Online]. Available: <http://www.rane.com/note161.html>
- Douglas R. Mauro and Kevin J. Schmidt 2001. July. “**Essential SNMP**” [Online]. Available:
http://docstore.mik.ua/oreilly/networking_2ndEd/snmp/ch02_05.htm
- FCAPS. [Online]. Available: <https://en.wikipedia.org/wiki/FCAPS>
- Peng Gao and Rui Zhao. 1999. November. “**An Introduction to Network Management**” [Online]. Available: <http://www.tml.tkk.fi/Studies/Tik110.300/1999/Essays/management.html>
- Simple Network Management Protocol Introduction. [Online]. Available:
http://www.snmpsharpnet.com/?page_id=30
- SNMP. 2016. March. [Online]. Available: <http://ittransformers.net/content/snmp>
- Terry Vinson. 2012. June. “**SNMP Theory and Operation**” [Online]. Available:
<http://blog.ipexpert.com/snmp-theory-and-operation/>
- White Paper. “**Network Management Systems Architectural Leading Practice**” Cisco Systems Inc. [Online]. Available:
http://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aec806bfb4c.html

ภาคผนวก

ขั้นตอนในการติดตั้งระบบบริหารจัดการเครือข่ายของซิสโก้ (Cisco Prime Infrastructure)

เนื่องจากการทดลองและทดสอบระบบบริการจัดการเครือข่ายซิสโก้ จะใช้ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ที่อยู่ในรูปแบบของไฟล์ Open Virtualization Archive (OVA) ทำให้สามารถติดตั้งใช้งานบนระบบ VMware ESXi ที่มีใช้งานอยู่ได้ทันที โดยมีวิธีการดำเนินการติดตั้งดังนี้

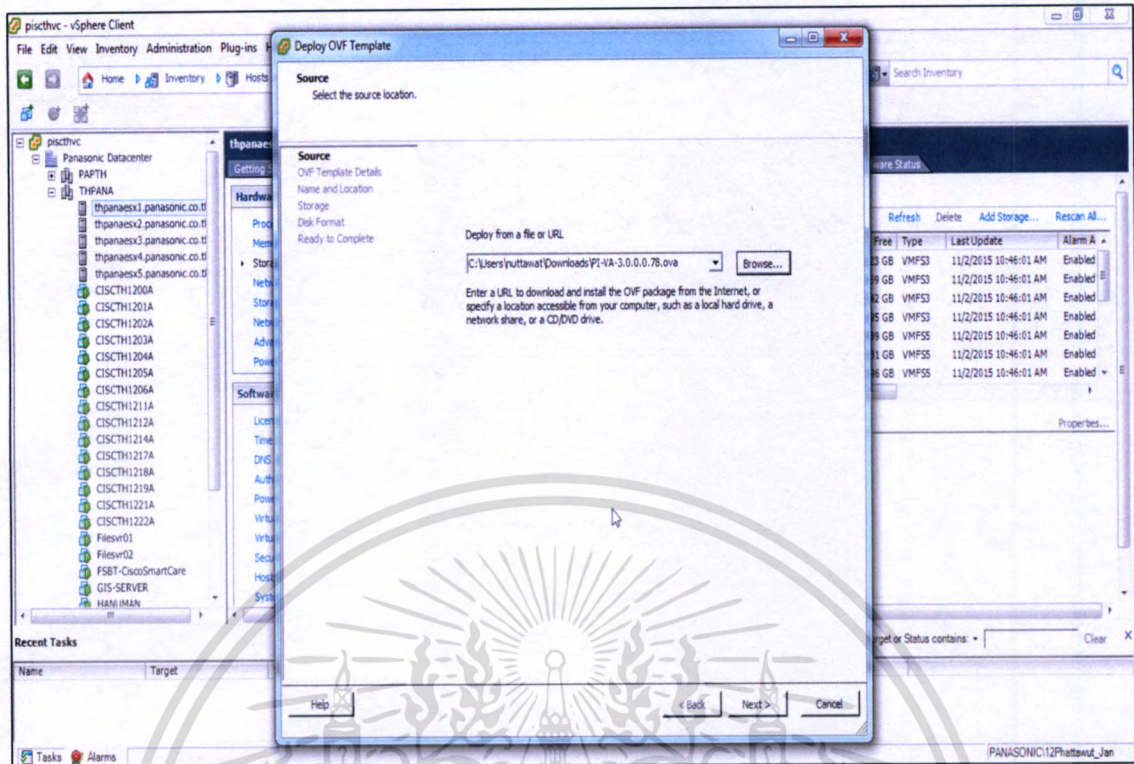
1. ทำการเพิ่มซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ที่อยู่ในรูปแบบของไฟล์ OVA เข้าสู่ระบบ VMware ESXi ผ่านทางซอฟต์แวร์ vSphere ของ VMware ตามรูปที่ 1.



รูปที่ 1. การเพิ่มไฟล์ OVA เข้าสู่ระบบ VMware ESXi ผ่านทางซอฟต์แวร์ vSphere

2. ซอฟต์แวร์ vSphere ทำการค้นหาไฟล์ OVA ของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ที่อยู่ในเครื่องคอมพิวเตอร์ของผู้ดูแลระบบ เข้าสู่ระบบ VMware ESXi ตามรูปที่ 2. ซึ่งไฟล์ OVA ของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้สามารถดาวน์โหลดได้ที่เว็บไซต์ของซิสโก้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้拿去ไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

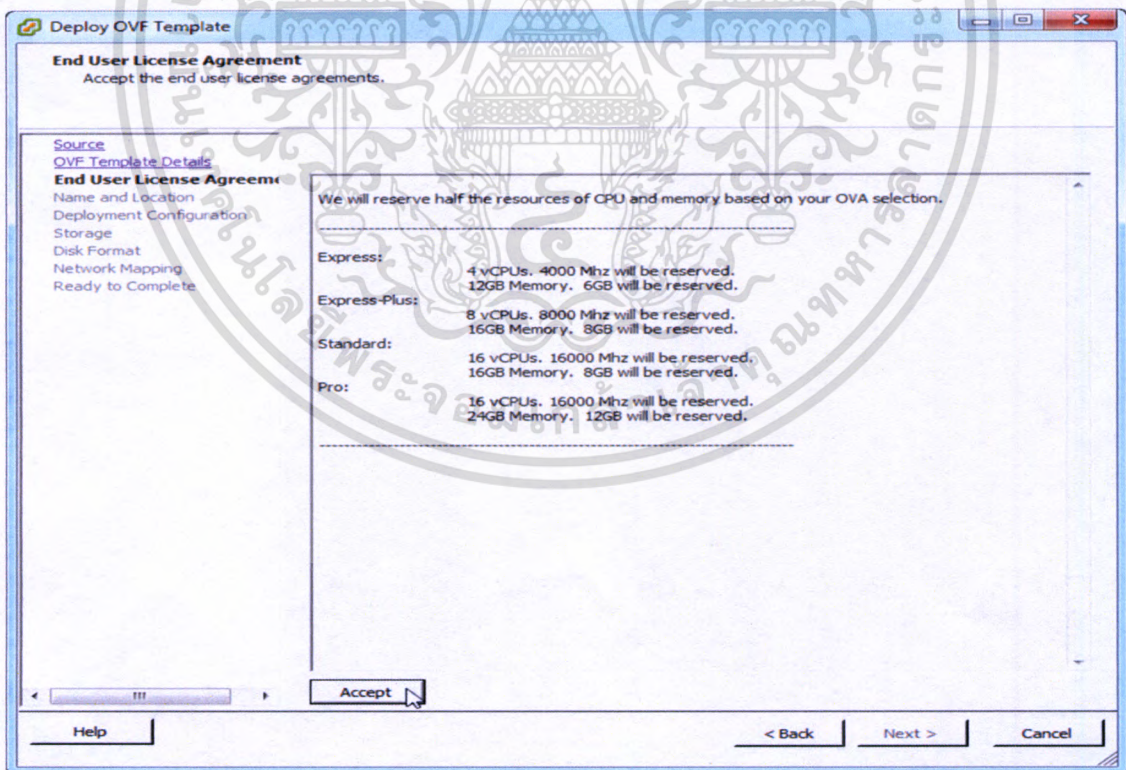


รูปที่ 2: การค้นหาไฟล์ OVA ผ่านทางซอฟต์แวร์ vSphere

3. ก่อนทำการเพิ่มไฟล์ OVA ของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ที่เข้าสู่ระบบ VMware ESXi ตัวซอฟต์แวร์ vSphere จะแสดงรายละเอียดของไฟล์ OVA ของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ดังรูปที่ 3. และ 4. โดยจะบอกรายละเอียดเกี่ยวกับขนาดของไฟล์ และบอกความต้องการในการใช้ทรัพยากรระบบของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ในแต่ละรุ่น ขึ้นอยู่กับผู้ใช้งานว่าต้องการจะใช้ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้รุ่นไหน โดยจะมีให้เลือก 3 รุ่นคือ Express , Express-Plus , Standard และ Pro ในการทดลองและทดสอบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้รุ่นนี้ ได้ทำการเลือกใช้ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้รุ่น Express ดังรูปที่ 5.

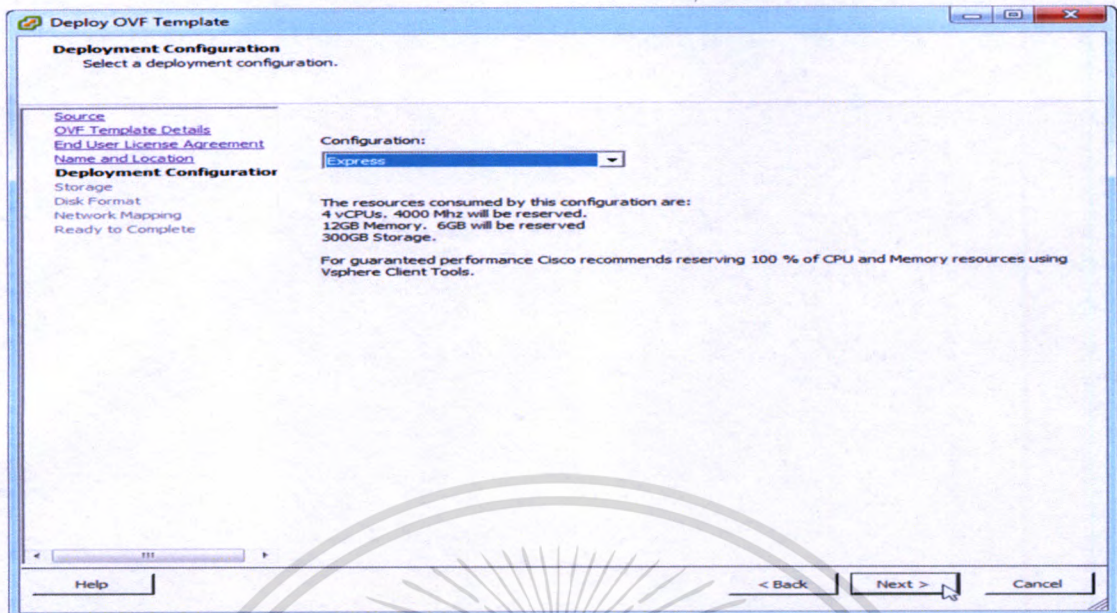


รูปที่ 3. แสดงรายละเอียดของไฟล์ OVA



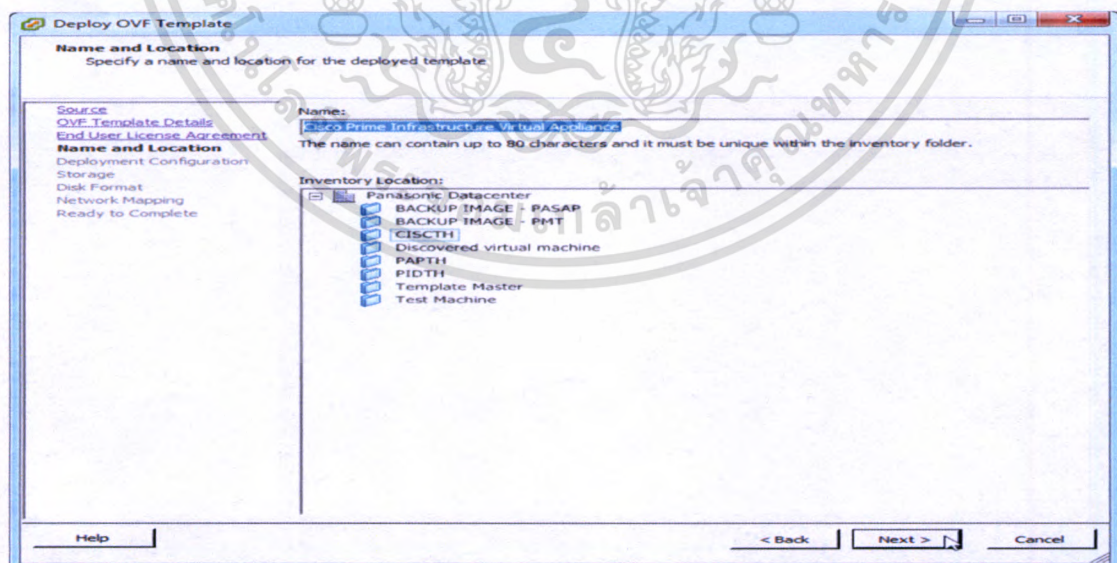
รูปที่ 4. แสดงรายละเอียดแต่ละรุ่นของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีกรนำไปใช้



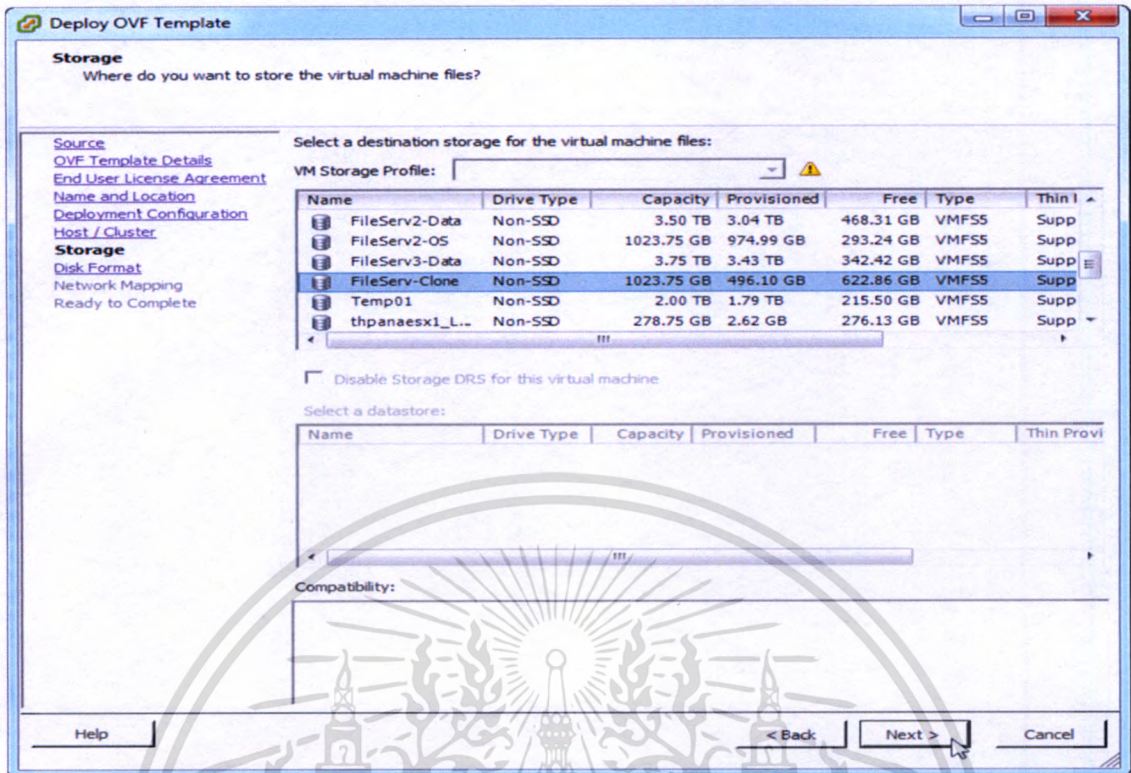
รูปที่ 5. แสดงการเลือกรุ่นซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ที่จะติดตั้ง

4. เมื่อทำการเลือกรุ่นซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ที่ต้องการติดตั้งเรียบร้อยแล้ว ขั้นตอนต่อไปจะต้องเลือกกลุ่มของ VMware ที่จะติดตั้ง โดยสิ่งที่ควรระวังในขั้นตอนนี้ คือ ต้องดูว่ากลุ่มของ VMware ที่จะติดตั้งมีทรัพยากรระบบเพียงพอหรือไม่ ดังรูปที่ 6. จากนั้นต้องทำการเลือกชุดอุปกรณ์จัดเก็บข้อมูลของระบบ VMware ดังรูปที่ 7.



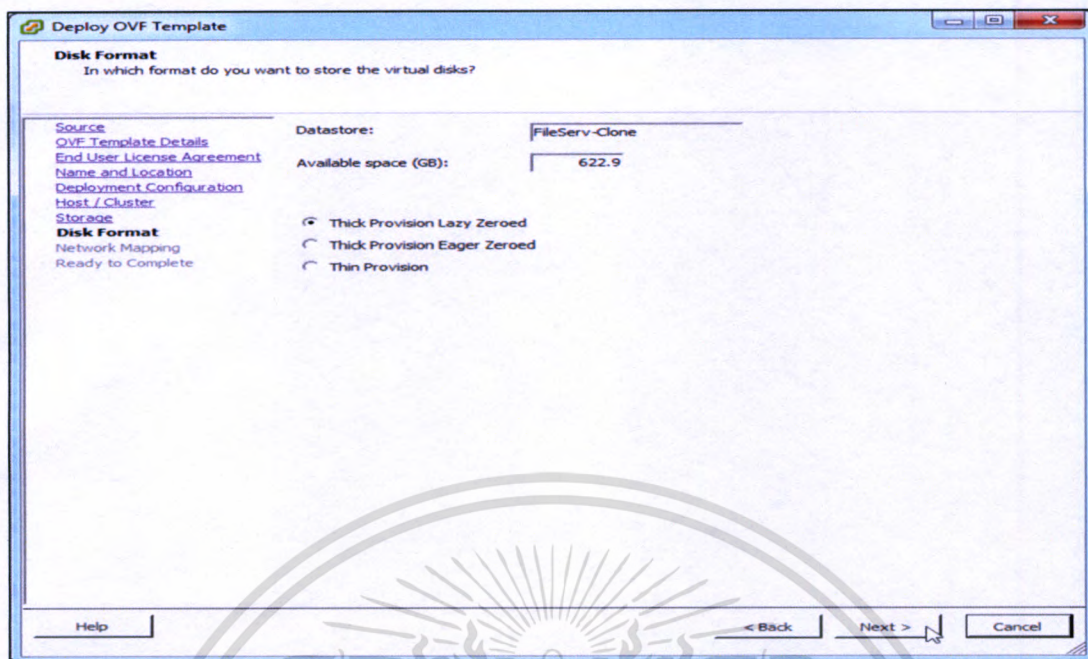
รูปที่ 6. การเลือกกลุ่มที่จะติดตั้งซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

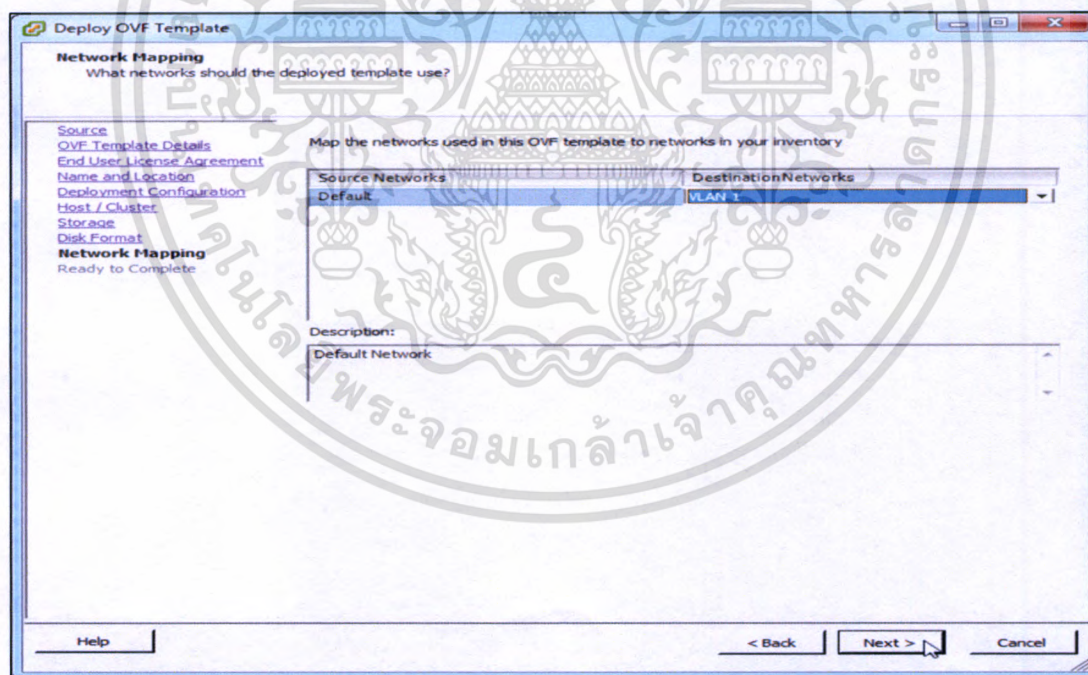


รูปที่ 7. แสดงที่เก็บข้อมูลในการติดตั้งซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้

5. เมื่อการเลือกชุดอุปกรณ์จัดเก็บข้อมูลของระบบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้เรียบร้อยแล้ว ระบบ VMware จะบอกขนาดของพื้นที่เก็บข้อมูลที่เหลือจากการใช้ไปของระบบซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ให้ผู้ตั้งทราบ ดังรูปที่ 8. ขั้นตอนต่อไปคือการเลือกระบบเครือข่ายให้กับซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ ดังรูปที่ 9. โดยระบบ VMware จะมีตัวเลือกระบบเครือข่ายตามหมายเลข VLAN ที่อ้างอิงมาจากบนระบบเครือข่ายที่ใช้งานอยู่ให้ผู้ที่ตั้งเลือกใช้ โดยผู้ติดตั้งควรเลือกหมายเลข VLAN ให้ตรงกับหมายเลขเครือข่ายที่จะตั้งค่าให้กับซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ จากนั้น vSphere จะแสดงข้อมูลสรุปการตั้งค่าการติดตั้งทั้งหมดของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ ดังรูปที่ 10.

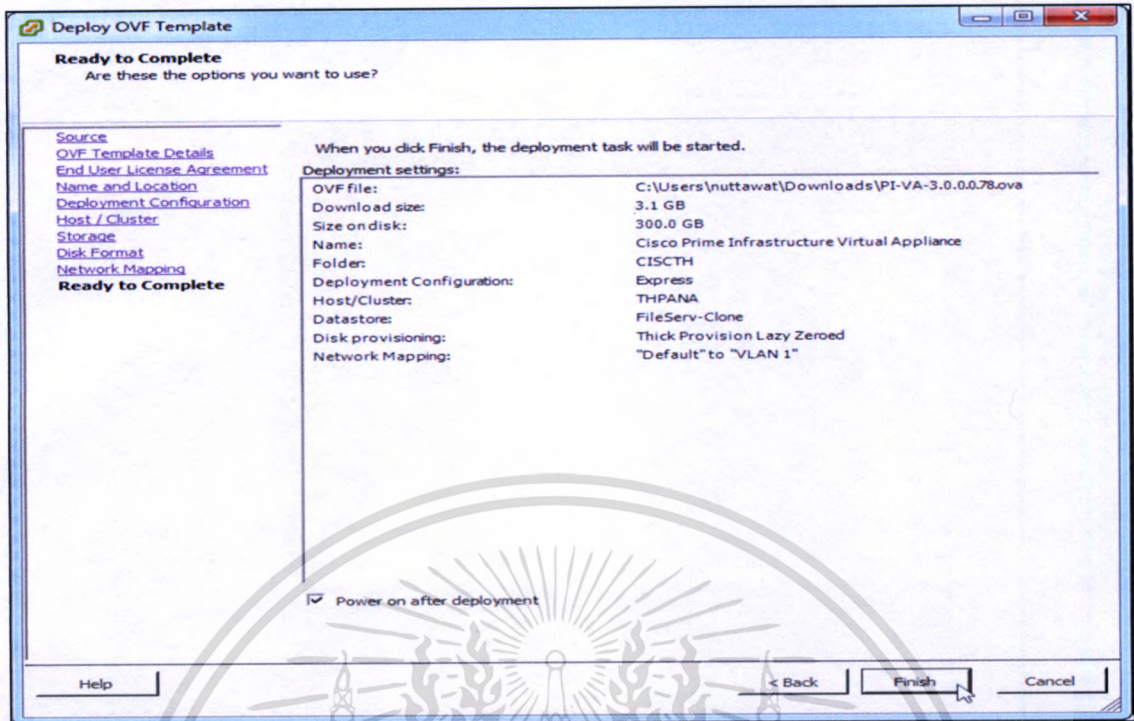


รูปที่ 8. แสดงขนาดที่เก็บข้อมูลที่เหลือหลังจากการติดตั้ง



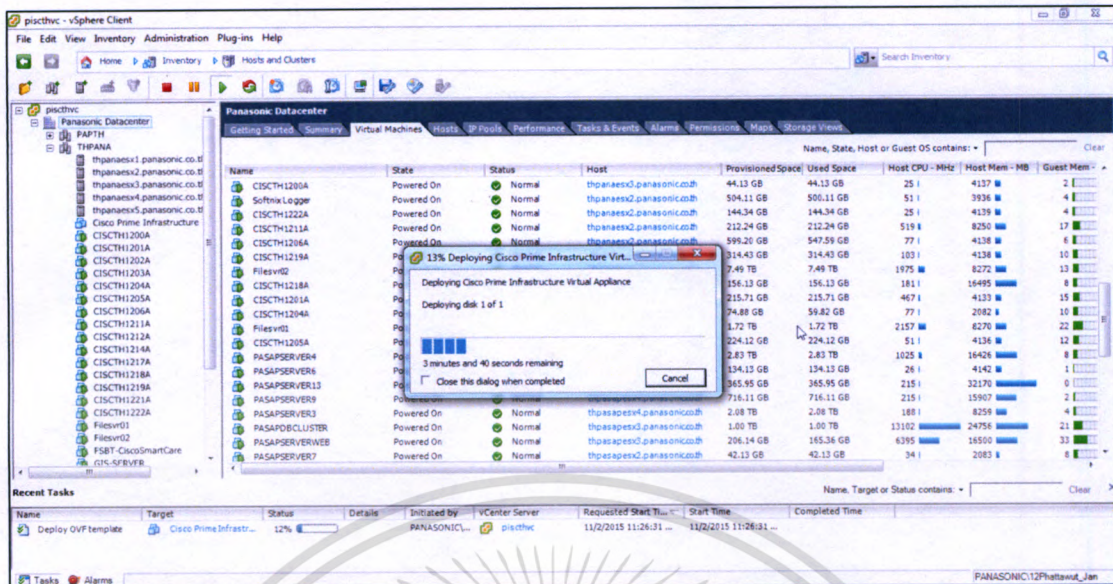
รูปที่ 9. แสดงตัวเลือกระบบเครือข่ายตามหมายเลข VLAN

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

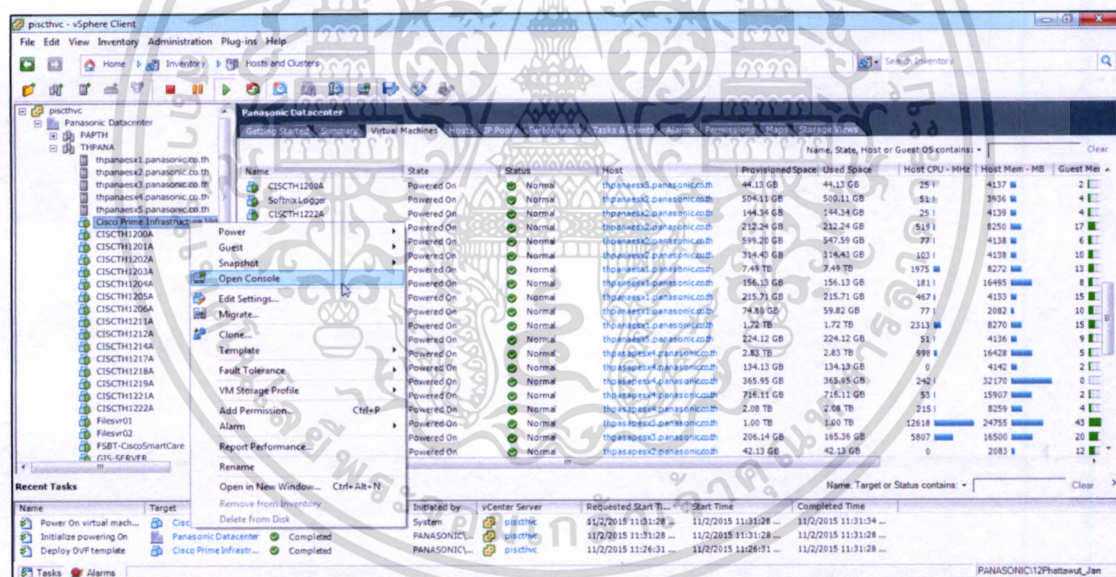


รูปที่ 10. แสดงข้อมูลสรุปการติดตั้งซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้

6. เมื่อทำการตั้งค่าต่างๆเสร็จเรียบร้อยแล้ว vSphere จะทำการโหลดไฟล์ OVA ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้เข้าสู่ระบบ VMware ดังรูปที่ 11. เมื่อการโหลดไฟล์ OVA ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้เข้าสู่ระบบ VMware เรียบร้อย ผู้ติดตั้งจะสามารถเปิดการทำงานของซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ได้ ดังรูปที่ 12.



รูปที่ 11. การโหลดไฟล์ซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้เข้าสู่ระบบ Vmware

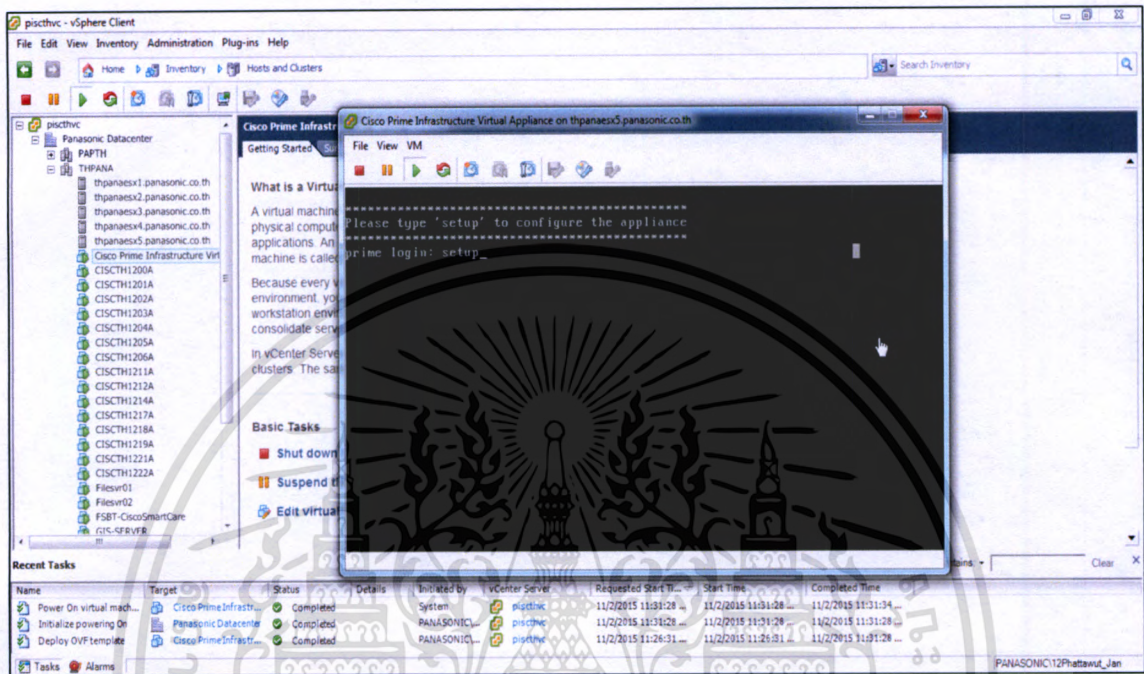


รูปที่ 12. การเปิดระบบบริหารจัดการเครือข่ายของซิสโก้บน Vmware

7. เมื่อทำการติดตั้งซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้บนระบบ Vmware เป็นครั้งแรก จะต้องเข้าไปตั้งค่าต่างๆ ให้กับซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ผ่านทางหน้าจอบริการออนไลน์ โดยจะต้องทำการยืนยันตัวตนเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้ โดยใช้บัญชีรายชื่อว่า Setup ดังรูปที่ 13. เพื่อเข้าไปทำการตั้งค่าต่างๆ ให้กับซอฟต์แวร์ระบบบริหาร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จัดการเครือข่ายของซิสโก้ โดยค่าที่ต้องทำการติดตั้งให้กับตั้งค่าต่างๆให้กับซอฟต์แวร์ระบบบริหารจัดการเครือข่ายของซิสโก้ในตอนเริ่มต้นการทำงาน เช่น ชื่อของตัวระบบบริหารจัดการเครือข่ายของซิสโก้ ชื่อโดเมน หมายเลขเครือข่าย วันและเวลา เป็นต้น ดังรูปที่ 14.



รูปที่ 13. การยืนยันตัวตนเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้ในครั้งแรก

โดยในขั้นตอนสุดท้าย ระบบบริหารจัดการเครือข่ายของซิสโก้จะให้ผู้ติดตั้งทำการตั้งค่าบัญชีผู้ใช้งานและรหัส ที่จะเป็นผู้ดูแลระบบบริหารจัดการเครือข่ายของซิสโก้ขึ้นมาใหม่ เมื่อเสร็จขั้นตอนนี้ ระบบบริหารจัดการเครือข่ายของซิสโก้จะดำเนินการติดตั้งและประมวลผลค่าที่ผู้ติดตั้งทำการตั้งค่าไว้ โดยอาจใช้เวลาในการดำเนินการประมาณ 30 นาที และหลังจากระบบบริหารจัดการเครือข่ายของซิสโก้จะดำเนินการติดตั้งและประมวลผลค่าที่ผู้ติดตั้งทำการตั้งค่าไว้เสร็จ ผู้ใช้งานสามารถเข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้ได้ผ่านทางเว็บไซต์ดังรูปที่ 15.

```

Cisco Prime Infrastructure Virtual Appliance on thpanaex5.panasonic.co.th
File View VM
Press 'Ctrl-C' to abort setup
Enter hostname[]: PISCTH
Enter IP address[]: 137.48.78.198
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 137.48.78.26
Enter default DNS domain[]: panasonic.co.th
Enter primary nameserver[]: 137.48.78.5
Add/Edit another nameserver? Y/N : y
Enter secondary nameserver[]: 137.48.78.2
Add/Edit another nameserver? Y/N : n
Enter primary NTP server[time.nist.gov]: 137.48.78.5
Add/Edit secondary NTP server? Y/N : n
Enter system timezone[UTC]: UTC
Current system clock time : 2015-11-02 04:35:55 UTC
Change system clock time? Y/N : y
Enter system clock time[2015-11-02 04:36]: 2015-11-02 11:36
System clock time changed
Current system clock time : 2015-11-02 11:35:59 UTC
Change system clock time? Y/N : n
Enter username[admin]:
Enter password:
Enter password again:
Bringing up network interface ...

```

รูปที่ 14. การประมวลค่าที่ตั้งไว้บนระบบบริหารจัดการเครือข่ายของซิสโก้



รูปที่ 15. แสดงหน้าจอ login เข้าสู่ระบบบริหารจัดการเครือข่ายของซิสโก้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประวัติผู้เขียน

ชื่อผู้เขียน	นายภัทรวิช จันทรสุเทพ
วันเดือนปีเกิด	12 สิงหาคม 2523
สถานที่เกิด	40 ตำบลอุทัยใหม่ อำเภอเมือง จังหวัดอุทัยธานี
วุฒิการศึกษาระดับปริญญาตรี	วิศวกรรมศาสตรบัณฑิต สาขา คอมพิวเตอร์
สถานที่สำเร็จการศึกษา	มหาวิทยาลัยนเรศวร
ปีที่สำเร็จการศึกษา	2545
การทำงาน	วิศวกรเครือข่าย บริษัทพานาโซนิค ประเทศไทย



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้