การพัฒนาระบบเครือข่ายไร้สายและการเพิ่มความพร้อมในการให้บริการในเครือข่ายหลัก

IMPROVING WIRELESS COMMUNICATION NETWORKS AND PROVIDING HIGH AVAILABILITY IN CORE NETWORK

ธีรวัฒน์ นำศรีเจริญสุข

รายงานนี้เป็นส่วนหนึ่งของการจัดการศึกษารายวิชาสหกิจศึกษา
หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 1 ปีการศึกษา 2558

การพัฒนาระบบเครือข่ายไร้สายและการเพิ่มความพร้อมในการให้บริการในเครือข่ายหลัก

IMPROVING WIRELESS COMMUNICATION NETWORKS AND PROVIDING HIGH AVAILABILITY IN CORE NETWORK

โดย

ธีรวัจน์ นำศรีเจริญสุข

TEERAWAT NAMSRICHAROENSUK

อาจารย์ที่ปรึกษา

ดร. ลภัส ประดิษฐ์ทัศนีย์

รายงานนี้เป็นส่วนหนึ่งของการจัดการศึกษารายวิชาสหกิจศึกษา

หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 1 ปีการศึกษา 2558

การพัฒนาระบบเครือข่ายไร้สายและการเพิ่มความพร้อมในการให้บริการในเครือข่ายหลัก

IMPROVING WIRELESS COMMUNICATION NETWORKS AND PROVIDING HIGH AVAILABILITY IN CORE NETWORK

โดย

ธีรวัจน์ นำศรีเจริญสุข

อาจารย์ที่ปรึกษา

ดร. ลภัส ประดิษฐ์ทัศนีย์

รายงานนี้เป็นส่วนหนึ่งของการจัดการศึกษารายวิชาสหกิจศึกษา

หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 1 ปีการศึกษา 2558

IMPROVING WIRELESS COMMUNICATION NETWORKS AND PROVIDING HIGH AVAILABILITY IN CORE NETWORK

TEERAWAT NAMSRICHAROENSUK

A REPORT SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR COOPERATING EDUCATION PROGRAM
THE DEGREE OF BACHELOR OF SCIENCE PROGRAM IN
INFORMATION TECHNOLOGY
FACULTY OF INFORMATION TECNOLOGY
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
1/ 2015

ใบรับรองโครงงาน (PROJECT)

เรื่อง

การพัฒนาระบบเครือข่ายไร้สายและการเพิ่มความพร้อมในการให้บริการในเครือข่ายหลัก

IMPROVING WIRELESS COMMUNICATION NETWORKS AND PROVIDING HIGH AVAILABILITY IN CORE NETWORK

นายธีรวัจน์ นำศรีเจริญสุข รหัสนักศึกษา 55070060

ขอรับรองว่ารายงานฉบับนี้ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของการศึกษา

วิชาโครงงานหลักสูตรวิทยาศาสตรบัณฑิต (เทคโนโลยีสารสนเทศ)

ภาคเรียนที่ 1 ปีการศึกษา 2557

..... อาจารย์ที่ปรึกษา

(ดร. ลภัส ประดิษฐ์ทัศนีย์)

หัวข้อโครงงาน	การพัฒนาระบบเครือข่ายไร้สายและการเพิ่มความพร้อม ในการให้บริการในเครือข่ายหลัก
นักศึกษา	นายธีรวัจน์ นำศรีเจริญสุข รหัสนักศึกษา 55070060
ปริญญา	วิทยาศาสตรบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
ปีการศึกษา	2558
อาจารย์ที่ปรึกษา	ดร. ลภัส ประดิษฐ์ทัศนีย์

บทคัดย่อ

เนื่องจากบริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด เป็นบริษัทให้บริการเกี่ยวกับระบบต่างๆ รวมถึงดำเนินการให้บรรลุตามความต้องการของลูกค้า เช่น ออกแบบ ติดตั้ง และแก้ไขปัญหาระบบเครือข่าย โดยในรายงานฉบับนี้จะกล่าวถึงระบบที่ทางบริษัทได้รับการว่าจ้างให้ดำเนินการพัฒนาระบบเครือข่ายให้กับลูกค้า 2 รายดังต่อไปนี้

ลูกค้ารายแรกต้องการพัฒนาระบบเครือข่ายไร้สายภายในองค์กร เพื่อให้สามารถรองรับเทคโนโลยีใหม่ และเพิ่มประสิทธิภาพในการใช้งานให้มากขึ้น

ลูกค้ารายที่สองมีความต้องการที่จะติดตั้งอุปกรณ์ใหม่ ทดแทนอุปกรณ์เดิมที่มีอยู่ เพื่อเพิ่มความเสถียรและประสิทธิภาพของระบบให้เพิ่มมากขึ้น

ทั้งนี้เพื่อให้สามารถดำเนินการปรับปรุงและพัฒนาระบบให้บรรลุตามความต้องการที่ได้รับมอบหมาย จึงได้ศึกษาความรู้ในทางทฤษฎีและปฏิบัติเกี่ยวกับเทคโนโลยีดังต่อไปนี้ Lightweight Access Point (LAP), Wireless Lightweight Controller (WLC), Virtual Local Area Network (VLAN), Dynamic Host Configuration Protocol (DHCP) และ Virtual Switching System (VSS) เพื่อนำไปประยุกต์ใช้ดำเนินงานครั้งนี้

Project Title	Improving wireless communication and providing high availability in core network
Student	Teerawat Namsricharoensuk Student ID 55070060
Degree	Bachelor of Science
Program	Information Technology
Academic Year	2015
Advisor	Dr. Lapas Pradittasnee

ABSTRACT

Dimension Data's systems integration services business provides specialist IT infrastructure solutions across networking, data centre, unified communications, security, desktop, and contact centre technologies. In document refer to systems provide to two customers.

First, customer has requirement to improving wireless network technology for support new network technologies and enhance performance the network.

Second, customer has requirement to install new equipment instead of existing equipment due to existing equipment is out-of-date and not sufficient for use. The new equipment and solution will support new technologies and improving availability, reliability and tolerant to existing infrastructure.

In document will be learn in theory and technical term to archive working objective such as Lightweight Access Point (LAP), Wireless Lightweight Controller (WLC), Virtual Local Area Network (VLAN), Dynamic Host Configuration Protocol (DHCP) and Virtual Switching System (VSS) to apply on working.

กิตติกรรมประกาศ

การที่ข้าพเจ้าได้มาปฏิบัติงานสหกิจศึกษา ณ บริษัท ไดเมนชั่น ดาต้า จำกัด (ประเทศไทย) ในระหว่างวันที่ 3 สิงหาคม 2558 ส่งผลให้ข้าพเจ้าได้รับความรู้ ความเข้าใจ ทางด้านระบบเครือข่ายและความปลอดภัยนอกเหนือจากการเรียนรู้ภายในห้องเรียน รวมทั้งประสบการณ์ต่างๆ ที่ได้จากการทำงาน ซึ่งมีคุณค่าต่อการเรียนและการทำงานในภายภาคหน้า อีกทั้งข้าพเจ้ายังได้มีโอกาสนำความรู้จากการเรียนมาประยุกต์ใช้ในการปฏิบัติงานจริง

ซึ่งในการปฏิบัติงานสหกิจศึกษาครั้งนี้ สำเร็จลุล่วงไปได้ด้วยดี จากความร่วมมือและการชี้แนะจากพนักงานในบริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด ดังนี้

- คุณนฤดล รุ่งวีรกุลอนันต์ ตำแหน่ง Installation Manager
- คุณจุไรรัตน์ สุภาวัฒนา ตำแหน่ง Installation Manager
- คุณศิริศักดิ์ สุกิจชาญยุทธ ตำแหน่ง Client Services Engineer
- คุณสัมพันธ์ ศรจรัสสุวรรณ ตำแหน่ง Client Services Engineer
- คุณนพพล พุ่มบุตร ตำแหน่ง Client Services Engineer
- คุณณภัทร คุณานันทกิจ ตำแหน่ง Client Services Engineer
- คุณอารียา จารุภูมิ ตำแหน่ง MS Resource Manager

ข้าพเจ้าใคร่ขอขอบพระคุณทุกท่าน ที่ได้ให้ความกรุณาชี้แนะ ให้คำแนะนำ คำปรึกษา ความช่วยเหลือในเรื่องต่างๆตลอดจนให้การดูแลและให้ความเข้าใจเกี่ยวกับชีวิตในการทำงานจริง

นอกจากนี้ ข้าพเจ้าจักขอบคุณ ที่ได้แนะนำโครงการสหกิจศึกษา ซึ่งเปิดโอกาสให้นักศึกษาได้รับประสบการณ์ที่ดีในอีกด้านหนึ่ง ขอขอบคุณเจ้าหน้าที่ คุณ อารียา จารุภูมิ ที่ช่วยประสานงานในการปฏิบัติงานตามขั้นตอนสหกิจและขอขอบคุณ ผศ.ดร. ปานวิทย์ ธุวะนุติ ที่อำนวยความสะดวกในการจัดทำโครงงานเล่มนี้ ขอขอบคุณอาจารย์ที่ปรึกษา ดร. ลภัส ประดิษฐ์ทัศนีย์ ที่คอยช่วยเหลือและรับฟังปัญหาต่าง ๆ จนโครงงานเล่มนี้สำเร็จลุล่วงไปได้ด้วยดี

สารบัญ

หน้า

สารบัญ (ต่อ)

สารบัญรูป

สารบัญรูป (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญ

บริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด ได้มีโครงการสหกิจศึกษาร่วมกับทางคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยปฏิบัติงานในส่วนของทีมติดตั้งแผนก Client Service ซึ่งได้มอบหมายโครงการสหกิจศึกษาเกี่ยวกับระบบเครือข่ายไร้สายที่ประกอบไปด้วย Wireless Device และ Wireless Controller ให้นักศึกษารับผิดชอบ โดยโครงนี้เป็นการปรับปรุงเครือข่ายไร้สายที่มีอยู่เดิมของลูกค้าเพื่อให้มีประสิทธิภาพที่ดีขึ้น

1.2 ความมุ่งหมายและวัตถุประสงค์

เพื่อให้นักศึกษามีความรู้ความเข้าใจในรูปแบบการทำงานของระบบเครือข่ายไร้สายและสามารถนำความรู้ไปประยุกต์ใช้ในการปรับปรุงระบบเครือข่ายไร้สายเพื่อรองรับการใช้งานที่เพิ่มมากขึ้นและสามารถให้บริการได้อย่างมีประสิทธิภาพ โดยเป็นไปตามความต้องการของลูกค้าที่กำหนดไว้ จึงได้มอบหมายให้ทำการศึกษาเกี่ยวกับ Wireless Device, Controller และความรู้ที่เกี่ยวข้อง

1.3 ขอบเขตของโครงงาน

1. เรียนรู้พร้อมทำความเข้าใจเกี่ยวกับระบบเครือข่ายหลักและเครือข่ายไร้สาย
2. ศึกษาการทำงานของระบบเครือข่ายไร้สายในการในส่วนที่มีการนำเครือข่ายไร้สายเข้ามาใช้งานรวมไปถึงการทำงานของ Virtual Switching System (VSS) บนเครือข่ายหลัก

1.4 ขั้นตอนการพัฒนาโครงงาน

1. ศึกษาระบบและเทคโนโลยีที่บริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด กำหนดไว้ อาทิเช่น Cisco Wireless Lightweight Access Point (LAP), Cisco Wireless Lightweight Controller (WLC) และ Virtual Switching System (VSS) เพื่อใช้ในการปรับปรุงระบบเครือข่าย
2. วิเคราะห์ ระบบเครือข่ายหลักและเครือข่ายไร้สาย
3. ศึกษาการออกแบบและติดตั้งระบบเครือข่ายหลักและไร้สาย ให้สามารถใช้งานได้ดีตามที่ออกแบบไว้ โดยใช้ความรู้และความเข้าใจที่ได้ศึกษามาประยุกต์ใช้ในการดำเนินงาน
4. ทดสอบใช้งานระบบเครือข่ายหลักและไร้สาย
5. วิเคราะห์และแก้ไขปัญหาที่อาจเกิดขึ้น
6. เสนอแนวทางการเพิ่มประสิทธิภาพอันเป็นประโยชน์แก่บริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด เพื่อใช้ในการปรับปรุงระบบเครือข่ายไร้สายให้กับสถาบันการศึกษาซึ่งเป็นลูกค้า
7. สรุปผล

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้รับเข้ารู้และความเข้าใจเกี่ยวกับการทำงานของ Cisco LAP ร่วมกับ Cisco WLC และระบบ VSS
2. ทางบริษัทฯ ได้รับแนวทางในการเพิ่มประสิทธิภาพให้กับสถาบันการศึกษา ซึ่งเป็นลูกค้า

บทที่ 2
การทบทวนวรรณกรรมที่เกี่ยวข้อง

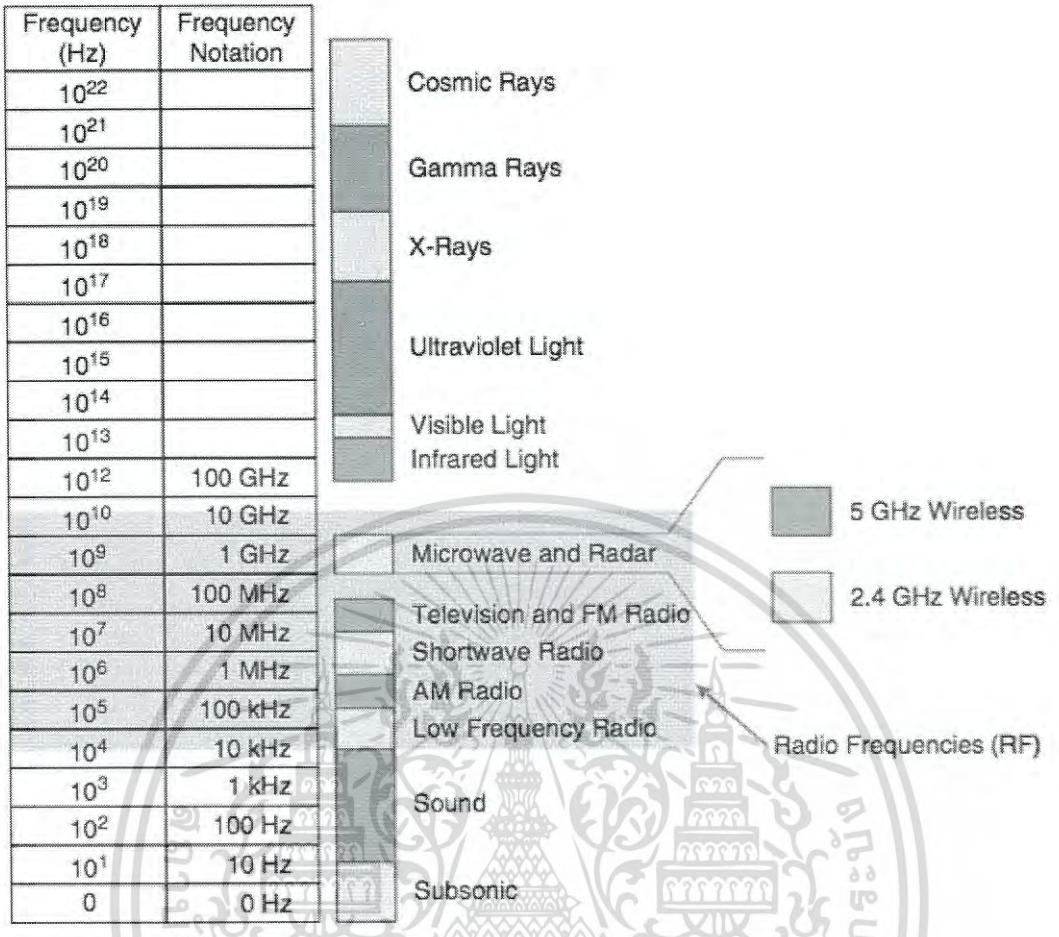
2.1 ทบทวนวรรณกรรมของระบบ Wireless LAN

2.1.1 IEEE 802.11 Standards

IEEE 802.11 ในมาตรฐานที่กำหนดกลไกต่างๆที่อุปกรณ์สามารถนำไปใช้สื่อสารแบบไร้สายกับอุปกรณ์อื่นๆ โดยทีข้อกำหนดสำคัญต่างๆ เช่น การสัญญาณวิทยุ, การมอดูเลต, การเข้ารหัส , ควบคุมขนาดและความถี่ของช่องสัญญาณ และอัตราการรับส่งข้อมูล

2.1.1.1 Frequency bands

การทำงานของระบบเครือข่ายไร้สายภายใต้มาตรฐาน IEEE 802.11 นั้นจะทำงานอยู่ในช่วงความถี่ 2.4-GHz และ 5-GHz โดยย่านสัญญาณความถี่ 2.4-GHz ใช้ช่วงสัญญาณความถี่ระหว่าง 2.400 ถึง 2.4835-GHz และย่านสัญญาณความถี่ 5-GHz ใช้ช่วงสัญญาณระหว่าง 5.150 ถึง 5.825-GHz

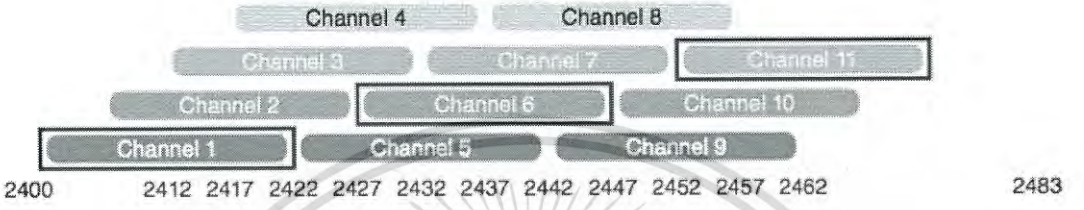


รูปที่ 2.1 ภาพแสดงคลื่นความถี่ที่ Wireless ใช้งาน

ช่วงความยาวคลื่น 2.4-GHz ถูกแบ่งออกเป็น 14 ช่องสัญญาณ ช่องสัญญาณละ 5-MHz จากมาตรฐาน IEEE 802.11 สามารถใช้การมอดูเลตแบบ Direct-Sequence Spread Spectrum (DSSS) หรือ Orthogonal Frequency-Division Multiplexing (OFDM) ได้ในย่านความถี่ 2.4-GHz

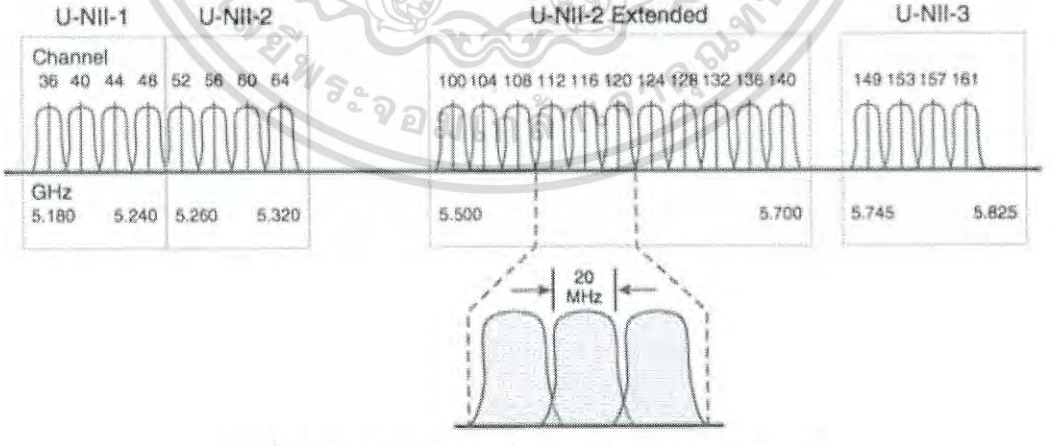
โดยสัญญาณที่มีการมอดูเลตแบบ DSSS มีความต้องการใช้ช่องสัญญาณที่มีความกว้าง 22 MHz ต่อช่องสัญญาณ ส่วนสัญญาณที่มีการมอดูเลตแบบ OFDM ต้องการใช้ช่องสัญญาณที่มีความกว้าง 20-MHz ต่อช่องสัญญาณ

จากที่กล่าวไปข้างต้นในการใช้งานเครือข่ายไร้สายในสภาพแวดล้อมจริงบนคลื่นความถี่ 2.4 GHz ช่องสัญญาณที่ดีที่สุดที่ควรเลือกใช้งานคือ ช่องสัญญาณที่ 1, 6 และ 11 ซึ่งการเลือกใช้ 3 ช่องสัญญาณนี้จะทำให้ไม่เกิดการรบกวนกันของช่องสัญญาณที่ซ้อนทับกัน ดังรูป



รูปที่ 2.2 ภาพแสดงการใช้ช่องสัญญาณที่ไม่ซ้อนทับกัน

ส่วนการใช้งานคลื่นความถี่ 5 GHz จะมีการแบ่งเป็นช่วงความถี่ที่ใช้งานได้เป็น 4 ช่วง ได้แก่ U-NII-1, U-NII-2, U-NII-2 Extended และ U-NII-3 โดยแบ่งช่วงเป็นช่วงคลื่นละ 20 MHz ที่ไม่ซ้อนทับกันและมีการมอดูเลตแบบ Orthogonal Frequency-Division Multiplexing (OFDM) ดังรูป



รูปที่ 2.3 แสดงรูปแบบคลื่นความถี่ 5-GHz ช่วง U-NII

2.1.1.2 มาตรฐาน 802.11-1997

มาตรฐานแรกที่มีการกำหนดขึ้นเป็นต้นฉบับที่กำหนดมาตรฐานการรับส่งสัญญาณแบบไร้สาย โดยสามารถเลือกใช้วิธีการรับส่งข้อมูลได้ทั้ง Frequency Hopping Spread Spectrum (FHSS) และ Direct Sequence Spread Spectrum (DSSS) บนคลื่นสัญญาณ 2.4-GHz โดยตามทฤษฎีมีอัตรารับส่งข้อมูลอยู่ที่ 1 ถึง 2 Mbps โดยอัตรารับส่งข้อมูลที่ 1 Mbps ใช้การมอดูเลตแบบ Differential Binary Phase Shift Keying (DBPSK) และอัตราการรับส่งข้อมูลที่ 2 Mbps ใช้การมอดูเลตแบบ Differential Quadrature Phase Shift Keying (DQPSK)

2.1.1.3 มาตรฐาน 802.11b

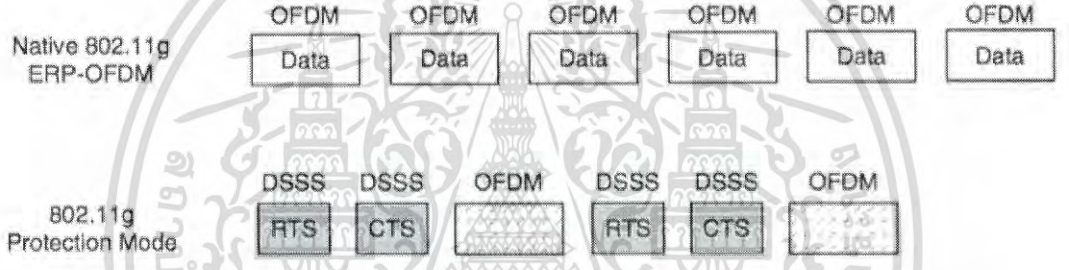
เพิ่มอัตราการรับส่งข้อมูลสูงสุดให้มากขึ้นจากมาตรฐาน 802.11-1997 ซึ่งอัตราการรับส่งข้อมูลอยู่ที่ 5.5 และ11 Mbps โดยใช้การมอดูเลตแบบ Complementary Code Keying (CCK) เพราะว่า 802.11b อยู่บนพื้นฐานของ DSSS และถูกใช้โดยคลื่นความถี่ 2.4-GHz อีกทั้งยังรองรับมาตรฐานก่อนหน้านี้คือมาตรฐาน 802.11-1997 ดังนั้นอุปกรณ์สามารถเลือกอัตราในการรับส่งข้อมูลที่ 1, 2, 5.5 หรือ 11 Mbps ได้ จากการปรับเปลี่ยนวิธีการมอดูเลตและเข้ารหัส

2.1.1.4 มาตรฐาน 802.11g

เนื่องจาก 802.11b มีรูปแบบการรับส่งข้อมูลแบบ DSSS ถูกจำกัดอัตราการรับส่งข้อมูลอยู่ที่ 11 Mbps และเพื่อที่จะเพิ่มอัตราการส่งข้อมูลจึงต้องใช้รูปแบบการส่งข้อมูลที่แตกต่างออกไป ซึ่งในมาตรฐาน 802.11g ได้แก้ไขโดยการนำเทคนิค Orthogonal Frequency-Division Multiplexing (OFDM) หรืออาจเรียกแทนว่า Extended Rate PHY-OFDM หรือ ERP-OFDM ซึ่งเทคนิค OFDM ยังคงทำงานที่ช่วงคลื่นความถี่ 2.4-GHz มีรูปแบบการรับส่งข้อมูลแบบ ERP-OFDM และอัตราการรับส่งข้อมูลอยู่ที่ 6, 9, 12, 18, 24, 36, 48 และ 54 Mbps โดยมีการมอดูเลตที่แตกต่างกันออกไปตามลำดับคือ BPSK 1/2, BPSK 3/4, QPSK 1/2, QPSK 3/4, 16-QAM 1/2, 16-QAM 3/4, 64-QAM 2/3 และ 64-QAM 3/4 โดยอัตราการรับส่งข้อมูลและเลือกวิธีการมอดูเลตจะสัมพันธ์กับ Signal-to-Noise Ratio (SNR) ซึ่งการจะใช้อัตราความเร็วที่มากสุดได้ ต่อเมื่อสัดส่วนของสัญญาณและสัญญาณรบกวน Signal-to-Noise Ratio (SNR) มีค่าอยู่ในระดับที่เหมาะสม

อีกทั้งมาตรฐาน 802.11g ถูกออกแบบมาให้รองรับการใช้งานร่วมกับ 802.11b ความหมายคือ อุปกรณ์ที่ใช้ 802.11g และ OFDM ได้จะสามารถกลับไปใช้และเข้าใจการสื่อสารของมาตรฐาน 802.11b โดยอุปกรณ์ในมาตรฐาน 802.11g จะใช้เทคนิคการเข้ารหัสของ 802.11b ในช่วงอัตรารับส่งข้อมูล 1 ถึง 5.5 Mbps ที่เป็นตามมาตรฐาน 802.11b

นอกจากนี้การใช้งานร่วมกันระหว่างอุปกรณ์ 802.11b แหละ 802.11g ยังต้องคำนึงถึงการทำงานของ RTS/CTS โดย 802.11g ต้องมีกลไกการป้องกัน โดยมีแนวคิดคือการส่งข้อมูลตามมาตรฐาน 802.11g OFDM ร่วมกับ DSSS flags เพื่อให้อุปกรณ์ที่ใช้มาตรฐาน 802.11b สามารถเข้าใจได้ เมื่อกลไกการป้องกันถูกเปิดใช้งาน อุปกรณ์ที่ใช้มาตรฐาน 802.11g จะเริ่มส่งข้อมูลในโหมดป้องกัน โดยขั้นแรกส่งข้อมูล Request-to-Sent (RTS) และ Clear-to-Send (CTS) ด้วยการส่งแบบ DSSS ไปหามาตรฐาน 802.11b ทุกอุปกรณ์ที่ OFDM จะส่งข้อมูลไปหา อุปกรณ์ที่เป็นมาตรฐาน 802.11b ใดๆ ที่ได้รับข้อมูลนั้นจะหยุดเพื่อรอจนกว่าการส่งข้อมูลจะเสร็จสิ้น เพราะการส่งข้อมูลแบบ OFDM นั้นอุปกรณ์ที่เป็น 802.11b ไม่สามารถเข้าใจได้ ดังนั้นรูปแบบการส่งข้อมูลจึงเป็นดังรูป



รูปที่ 2.4 ภาพเปรียบเทียบระหว่าง 802.11g Native และการส่งข้อมูลในโหมด Protected

ข้อด้วยในการทำงานของมาตรฐาน 802.11g อาจสามารถแบ่งได้เป็น 2 หัวข้อหลักๆดังนี้

- ถ้าหากใช้ในย่านความถี่ 2.4-GHz จะสามารถใช้งานได้ 3 ช่องสัญญาณที่ไม่เกิดการทับซ้อนกันของสัญญาณ
- อุปกรณ์ที่ใช้ OFDM ถูกจำกัดกำลังส่งของสัญญาณที่ 15-dBm แย่กว่าการใช้ DSSS ที่มีกำลังส่งอยู่ที่ 20-dBm โดยกำลังส่งที่มากกว่าจะทำให้การแพร่กระจายของสัญญาณมีรัศมีที่กว้างกว่าการส่งข้อมูลที่มีกำลังส่งน้อยกว่า

2.1.1.5 มาตรฐาน 802.11a

มาตรฐาน 802.11a ได้ถูกพัฒนาขึ้นเพื่อแก้ไขปัญหาของบนคลื่นความถี่ 2.4-GHz ซึ่งสามารถใช้งานได้ 3 ช่องสัญญาณที่ไม่ซ้อนทับกันเท่านั้น ทำให้มีช่องสัญญาณที่น้อยเกินไป และไม่สามารถรองรับผู้ใช้งานจำนวนมากได้อย่างมีประสิทธิภาพ

ทำให้ในมาตรฐาน 802.11a ได้แก้ไขให้มีการเริ่มใช้งานสัญญาณช่วงความถี่ 5-GHz ดังนั้น โอกาสสำหรับคลื่นที่ไม่ใช่ 802.11 จะมีการรบกวนสัญญาณน้อยมาก เพราะว่าหนึ่งช่องสัญญาณบนความถี่ 5-GHz มีความกว้าง 20-MHz ทำให้สามารถใช้งานได้ 1 ช่องต่อการรับส่งข้อมูลพอดี อีกทั้งจำนวนช่องสัญญาณที่มีจำนวนมากบนความถี่ 5-GHz จึงสามารถรองรับผู้ใช้งานได้จำนวนมากขึ้น

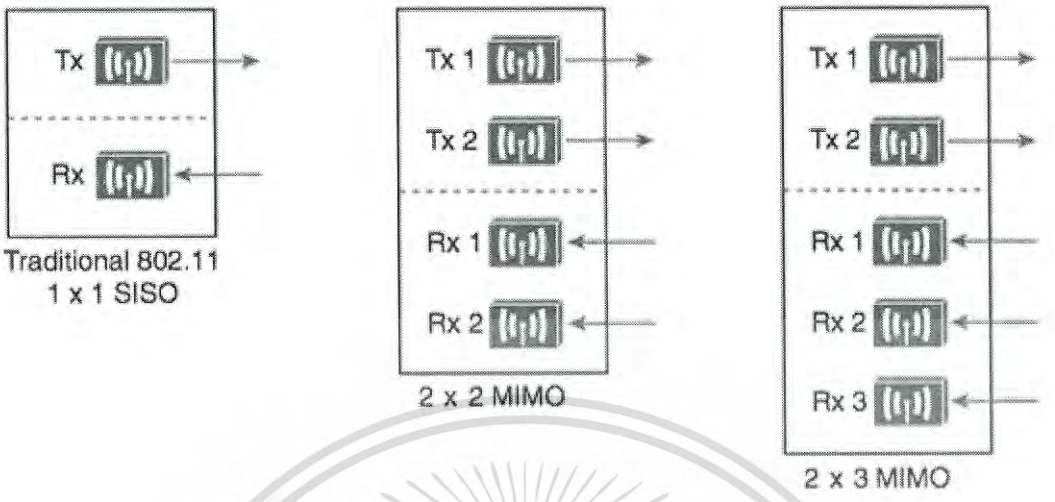
โดยในรูปแบบการส่งข้อมูลจะใช้เป็นแบบ OFDM เท่านั้น และไม่ได้ถูกออกแบบมาเพื่อรองรับการใช้งานเทคโนโลยี 802.11b และ 802.11-1997 รวมไปถึงไม่รองรับการรับส่งข้อมูลที่ต่ำกว่า 6 Mbps

อุปกรณ์เครือข่ายไร้สายสามารถเลือก 1 ใน 8 ของเทคนิคการมอดูเลต ได้แก่ 6, 9, 12, 18, 24, 36, 48 หรือ 54 Mbps แต่ละช่องสัญญาณที่ใช้รูปแบบการรับส่งข้อมูลแบบ OFDM มีความกว้างของช่องสัญญาณเท่ากับ 20-MHz และเนื่องจากความกว้างแต่ละช่องสัญญาณบนย่านความถี่ 5-GHz ที่มีช่องละ 20-MHz พอดี ทำให้มีการซ้อนทับกันของสัญญาณเล็กน้อย เพราะฉะนั้นมาตรฐาน 802.11a ได้แนะนำให้เครื่องส่งสัญญาณที่อยู่ในพื้นที่เดียวกัน ควรจะใช้ช่องสัญญาณห่างกัน 1 ช่องสัญญาณ อาทิเช่น เครื่องส่งสัญญาณตัวที่หนึ่งอาจใช้ช่องสัญญาณที่ 36 แต่เครื่องส่งสัญญาณเครื่องที่สองที่อยู่ในพื้นที่เดียวกันควรจะใช้ช่องสัญญาณที่ 44 (เว้นหนึ่งช่องสัญญาณ) ซึ่งจะทำให้ได้ประสิทธิภาพที่ดีกว่าใช้ช่องสัญญาณที่ 40 โดยอ้างอิงจาก (รูปที่ 2.3)

2.1.1.6 มาตรฐาน 802.11n

ภายใต้ตัวเลือกที่ดีที่สุด ทั้งมาตรฐาน 802.11g และ 802.11a ต่างก็มีอัตราการส่งข้อมูลสูงสุดที่ 54 Mbps แต่อุปกรณ์ใช้สาย Ethernet ที่มีความเร็วได้ถึง 10 - 1000 Mbps ทำให้เมื่อมีการใช้งานร่วมกันระหว่าง Ethernet กับ Wireless มีปัญหาคอขวด (Bottleneck) จึงต้องมีการปรับปรุงมาตรฐานให้รองรับอัตรารับส่งข้อมูลที่สูงขึ้นได้ถึง 600 Mbps โดยเรียกเทคนิคนี้ว่า High Throughput (HT) ซึ่งเทคนิคนี้สามารถปรับใช้ได้กับทั้งสองคลื่นความถี่คือ ความถี่ช่วง 2.4-GHz และ 5 GHz โดยที่มาตรฐาน 802.11n ได้ออกแบบให้สามารถทำงานร่วมกับมาตรฐาน 802.11b, 802.11g และ 802.11a ได้

ในมาตรฐานก่อนหน้า 802.11n เสาอากาศที่ถูกใช้ในอุปกรณ์จะเป็นการใช้หนึ่งเสาส่งสัญญาณ และหนึ่งเสารับสัญญาณ หรือที่เรียกกันว่า Single-in, Single-out (SISO) system ในมาตรฐาน 802.11n ได้มีการพัฒนาระบบ Multiple-input, Multiple-output (MIMO) system ซึ่งมีหลายเสาส่งสัญญาณ และหลายเสารับสัญญาณโดยการรับ-ส่งสัญญาณของอุปกรณ์เป็นดังรูป



รูปที่ 2.5 ภาพแสดงตัวอย่างอุปกรณ์ SISO และ MIMO

อุปกรณ์ 802.11n ที่ใช้งานเทคนิค MIMO ในการรับส่งข้อมูล สามารถอธิบายได้ในรูปแบบ TxR โดย T คือจำนวนของเสาส่งสัญญาณ และ R คือจำนวนของเสารับสัญญาณ โดยมาตรฐาน 802.11n มีความต้องการในการใช้งานต่ำสุดคือ 2x2 MIMO และสูงสุดที่ 4x4 MIMO

จากการทำงานแบบ MIMO ทำให้มีเทคนิคมากมายในการทำให้การสื่อสารแบบไร้สายมีประสิทธิภาพมากยิ่งขึ้น โดยมีการพัฒนาเทคนิคต่างๆเพื่อเพิ่มอัตราการรับส่งข้อมูลและเพิ่มระดับความน่าเชื่อถือในการรับส่งข้อมูล ดังนี้

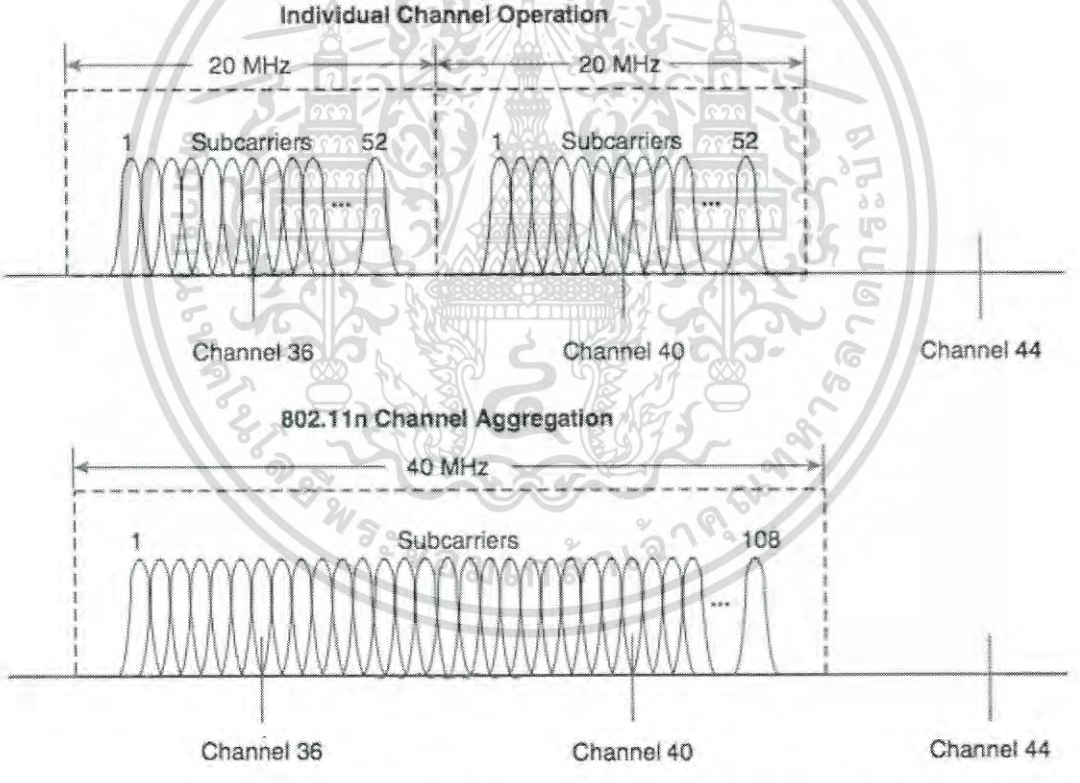
- Channel aggregation : เป็นเทคนิคการรวมช่องสัญญาณเพื่อเพิ่มช่องทางในการรับข้อมูลให้มีมากขึ้น
- Spatial multiplexing (SM) : เป็นเทคนิคในการแยกเสาสัญญาณในการเข้ารหัสและส่งข้อมูลเรียกว่าการสตรีมข้อมูล จากวิธีการนี้ทำให้ข้อมูลถูกส่งหาผู้ใช้ได้รวดเร็วยิ่งขึ้น
- MAC layer efficiency : เป็นการปรับปรุงและพัฒนา MAC protocol เพื่อลด overhead ที่เกิดขึ้นในการส่งข้อมูล
- Transmit beam forming (T×BF) : เป็นเทคนิคการใช้เสาหลายสัญญาณเพื่อเพิ่มความเข้มและระยะทางของสัญญาณที่แพร่ออกไป ส่งผลให้ไม่ให้เกิดการสูญหายของข้อมูลที่ส่งทำให้มีความน่าเชื่อถือในการใช้งานมากยิ่งขึ้น

- Maximal-ratio combining (MRC) : เป็นเทคนิคการรับข้อมูลเดียวกันจากหลายเสาสัญญาณเพื่อปรับปรุง SNR ให้ดีขึ้นและเพิ่มความถูกต้องของข้อมูลที่ได้รับ

โดยปกติอุปกรณ์เครือข่ายไร้สายมาตรฐาน 802.11a หรือ 802.11g จะมีตัวรับ-ส่งสัญญาณตัวเดียว กล่าวคือมีช่องสัญญาณขนาด 20-MHz เพียงช่องเดียว ณ.เวลานั้นๆ

ในมาตรฐาน 802.11n ได้ปรับปรุงให้เพิ่มช่องสัญญาณ 20-MHz ในการส่งผ่านข้อมูลโดยเพิ่มจำนวนของการแบ่งช่องสัญญาณย่อยของข้อมูลถึง 52 ช่อง

นอกจากนี้ยังสามารถทำงานซึ่งใช้ช่องสัญญาณ 20-MHz ช่องเดียว หรือ 40-MHz ช่องเดียวโดยเพิ่มความกว้างของช่องสัญญาณสองเท่าเป็น 40-MHz ทำให้ส่งผ่านข้อมูลได้เป็นสองเท่า



รูปที่ 2.6 ภาพเปรียบเทียบช่องสัญญาณ 20-MHz และ 40-MHz

เมื่อถูกรวมช่องสัญญาณจำนวนช่องสัญญาณที่ว่างก็จะลดน้อยลง อาทิเช่น คลื่นความถี่ 5 GHz มี 23 ช่องสัญญาณที่ไม่ซ้อนทับกันในความกว้างช่องละ 20-MHz ถ้าถูกรวมช่องสัญญาณเป็น 40 MHz จะมีเพียง 11 ช่องสัญญาณที่ไม่ซ้อนทับกัน แต่ก็ยังให้ช่องสัญญาณที่มากพอต่อการใช้งาน

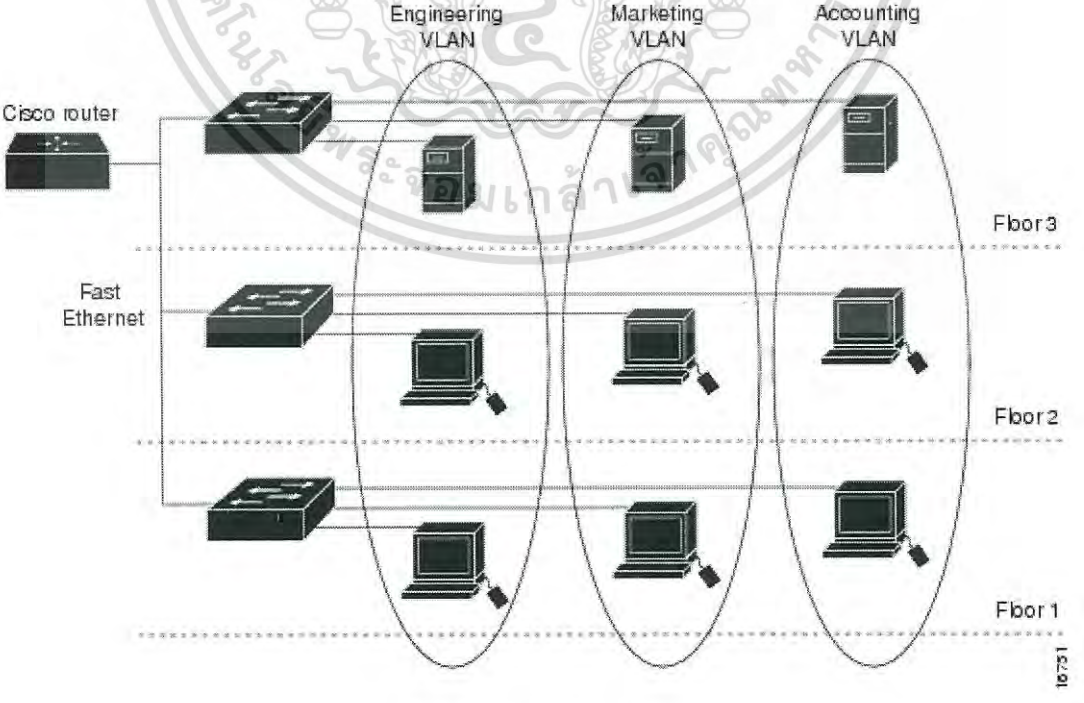
พิจารณาช่องคลื่น 2.4-GHz ซึ่งมีเพียง 3 ช่องสัญญาณที่ไม่ซ้อนทับกัน ที่ไม่สามารถที่จะพยายามรวมช่องสัญญาณเข้าไปในช่องสัญญาณ 40-MHz ดังนั้นการรวมช่องสัญญาณไม่แนะนำและไม่พยายามทำการใดๆในช่อง 2.4-GHz

2.2 Virtual Local Area Network (VLAN)

เป็นการนำเทคโนโลยีเสมือน (Virtualization) มาใช้กับระบบเครือข่าย (LAN) ทำให้มีหลายเครือข่ายบนเครือข่ายหลักที่ใช้ร่วมกัน โดยเทคโนโลยีนี้ทำงานบนชั้นที่ 2 ของ OSI model

ซึ่งแต่ก่อนอุปกรณ์ทุกตัวจะเชื่อมต่อกันบนเครือข่ายเดียวกันทั้งหมด ส่งผลให้เกิด overhead จำนวนมากบนเครือข่ายจากการส่ง Broadcast สื่อสารกันจากตัวอุปกรณ์

ดังนั้นเพื่อลด overhead จึงนำ VLAN มาช่วยในการลดจำนวนของข้อมูล Broadcast บนเครือข่าย โดยการแบ่งอุปกรณ์ต่างๆบนเครือข่ายหลักออกเป็นเครือข่ายย่อย ทำให้ขนาดของเครือข่ายลดลง และส่งผลให้ Broadcast domain เล็กลงเช่นกัน เพราะข้อมูล Broadcast จะไม่ถูกส่งข้าม VLAN หรืออุปกรณ์ที่ทำงานบนชั้นที่ 3 โดยการสื่อสารข้าม VLAN ของแต่ละกลุ่มอุปกรณ์สามารถทำได้โดยใช้อุปกรณ์ชั้นที่ 3 อาทิเช่น Router เพื่อให้ข้อมูลที่อยู่ต่าง VLAN กันสามารถสื่อการกันได้



รูปที่ 2.7 แสดงตัวอย่าง VLANs

2.3 Dynamic Host Configuration Protocol (DHCP)

2.3.1 กลไกและขั้นตอนการทำงานของ DHCP

DHCP ให้บริการการกำหนดค่าที่ใช้ในระบบเครือข่ายให้กับอุปกรณ์ (Host) เช่น หมายเลข IP address, Subnet mask, Default gateway เป็นต้น โดยประกอบไปด้วย 2 องค์ประกอบ คือ โปรโตคอลสำหรับจัดสรรค่าของตัวแปรต่างๆจากเซิร์ฟเวอร์ส่งให้กับอุปกรณ์ และกลไกการจองที่อยู่บนเครือข่ายให้กับอุปกรณ์

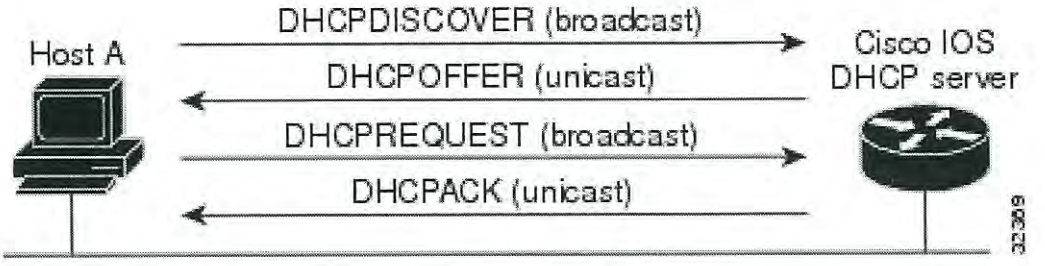
DHCP ถูกสร้างขึ้นบนรูปแบบการสื่อสารแบบ Client/Server โดยที่เซิร์ฟเวอร์ DHCP กำหนดและจัดสรรที่อยู่บนเครือข่าย และส่งการตั้งค่าต่างๆให้กับอุปกรณ์แบบไดนามิก

DHCP รองรับ 3 กลไกสำหรับการจองหมายเลขไอพีดังนี้

- Automatic allocation : DHCP จะกำหนดหมายเลขไอพีถาวรให้กับไคลเอนต์
- Dynamic allocation : DHCP จะกำหนดหมายเลขไอพีที่มีช่วงเวลาหมดอายุ ให้กับไคลเอนต์
- Manual allocation : ผู้ดูแลระบบเป็นผู้กำหนดหมายเลขไอพีให้กับไคลเอนต์ แล้วใช้ DHCP เพื่อตั้งค่าไคลเอนต์ให้มีหมายเลขไอพีตามที่ได้กำหนดไว้

โดยต่อไปจะเป็นการแสดงขั้นตอนที่เกิดขึ้นเมื่อ DHCP Client ร้องขอหมายเลขไอพีจาก DHCP Server

- ไคลเอนต์ส่ง DHCPDISCOVER broadcast message ไปยัง DHCP server ที่กำหนดไว้
- DHCP server เสนอพารามิเตอร์ของการตั้งค่า เช่น หมายเลขไอพี, หมายเลข MAC, ชื่อโดเมน และค่าต่างๆที่กำหนดไว้ให้กับไคลเอนต์ใน DHCP unicast message
- ไคลเอนต์ส่ง DHCPREQUEST broadcast message ไปหา DHCP server เพื่อขอข้อมูลที่ได้เสนอมาให้
- DHCP server ตอบกลับ โดยให้รายละเอียดข้อมูลที่ไคลเอนต์ได้ร้องขอมา



รูปที่ 2.8 ภาพแสดงการร้องขอหมายเลขไอพีจาก DHCP Server

2.3.2 DHCP Option 43 (Vendor Specific DHCP Options)

โดยปกติการใช้งาน Lightweight access point (LAP) จะต้องทำงานร่วมกับ Wireless LAN controller (WLC) เพราะว่าอุปกรณ์โหมดที่เป็น LAP ในส่วนของการควบคุม (Control plane) จะอยู่ที่อุปกรณ์ WLC ต่างจาก Access point (AP) ทั่วไปที่มี Control plane และส่วนของข้อมูล (Data plane) อยู่ในอุปกรณ์เดียวกัน

ดังนั้นจึงต้องตั้งค่า LAP ใช้งาน DHCP เพื่อรับหมายเลขไอพีมาจากอุปกรณ์ที่ให้บริการ DHCP เช่น DHCP Server เป็นต้น ซึ่งการใช้งานทั่วไป DHCP Server จะให้บริการข้อมูลพื้นฐาน เช่น หมายเลขไอพี, หมายเลข MAC, หมายเลข Gateway เป็นต้น แต่สำหรับ LAP จำเป็นต้องใช้หมายเลขไอพีเฉพาะ เพื่อให้ LAP ดึงข้อมูลต่างๆที่จำเป็นต่อการใช้งาน ซึ่งส่วนนั้นคือ DHCP Option 43 ที่ต้องเพิ่มเติมเข้าไปในการตั้งค่า DHCP Server ที่ทำหน้าที่ให้บริการในส่วนนี้

การทำงานร่วมกับ LAP จะต้องมีกระบวนการกำหนดค่าเพิ่มเติม เพื่อให้ LAP สามารถดาวน์โหลดเฟิร์มแวร์ และข้อมูลต่างๆจาก WLC ได้ โดยใช้ DHCP Option 43 (Vendor Specific DHCP Options) ซึ่ง DHCP Option 43 มีความสัมพันธ์กับ DHCP Option 60 เนื่องจาก DHCP Option 60 คือ vendor class identifier (VCI) ทำหน้าที่บ่งบอกประเภทของผู้ผลิต (อ้างอิงตาม RFC 2131) ใช้ระบุหมวดหมู่ของผู้ผลิตในการแลกเปลี่ยนข้อมูล vendor-specific ระหว่าง Server และ Client

เพื่อระบุข้อมูลต่างๆที่แต่ละผู้ผลิตจำเป็นในการใช้งานผลิตภัณฑ์ เช่น ผลิตภัณฑ์ Cisco Aironet 2700 Series ต้องระบุ VCI ข้อความว่า “Cisco AP c2700” จากนั้นกำหนด type-length-value (TLV) blocks ลงไปใน DHCP offer ของ DHCP Option 43 โดยมี sub-option ของ TLV block ดังนี้

1. Type - 0xf1 (decimal 241)
2. Length – (จำนวนไอพีของ WLC) * 4
3. Value - รายการอินเตอร์เฟสควบคุม WLC ซึ่งอยู่ในรูปของค่าตัวเลขฐาน 16

ในการใช้งานจะมีการกำหนด Option 43 Vendor Specific Info บน DHCP Server โดยจำเป็นต้องใส่ค่าซึ่งอยู่ในรูปแบบของ Type-Length-Value (TLV) และเป็นฐาน 16 โดยระบบจะอ่านค่าเรียงลำดับจากหน้าไปหลัง ในปกติ Type จะมีค่าเป็น 0xf1 เสมอ ส่วน Length จะเกิดจากการจำนวนชุดของไอพี WLC คูณด้วย 4 และสุดท้าย Value คือการนำหมายเลขไอพีของ WLC แปลงเป็นฐาน 16 อาทิเช่น ในการใช้งานมี WLC จำนวน 2 เครื่อง ได้แก่หมายเลขไอพี 192.168.10.5 และ 192.168.10.20 ดังนั้น Type จะมีค่าเท่ากับ 2 x 4 = 8 และหมายเลขไอพีซึ่งเป็น Value จะมีค่าเท่ากับ c0a80a05 (192.168.10.5) และ c0a80a14 (192.168.10.20) โดยสรุปการตั้งค่า TLV ของ DHCP Option 43 จะมีค่าเป็น f108c0a80a05c0a80a14 เป็นต้น

2.4 Wireless LAN Controller (WLC)

ในสถาปัตยกรรม Cisco Unified Wireless Network และ Access Point (APs) เป็นแบบ lightweight นั่นหมายถึง LAPs ไม่สามารถทำงานโดยเป็นอิสระจาก WLC ได้ ซึ่ง Lightweight Access Points (LAPs) จะมีการค้นหาและลงทะเบียนกับ WLCs ก่อนที่ LAPs จะให้บริการกับ Clients

2.4.1 ข้อมูลพื้นฐาน

Cisco WLCs และ LAPs เป็นส่วนหนึ่งของสถาปัตยกรรม Cisco unified wireless network ซึ่งสถาปัตยกรรม Cisco unified wireless network แบบศูนย์กลางใช้การตั้งค่า และควบคุม WLAN บน WLC โดย LAPs ไม่สามารถทำงานโดยเป็นอิสระจาก WLC ได้ เพราะ WLC เป็นตัวจัดการการตั้งค่าและเฟิร์มแวร์บน LAP ดังนั้น LAPs จะถูกใช้งานในรูปแบบ “zero touch” หมายถึง ไม่มีการตั้งค่าแยกกันในแต่ละ LAP

และเพื่อให้ WLC สามารถจัดการ LAP ได้ อุปกรณ์ LAP จะค้นหา และลงทะเบียนกับ WLC หลังจาก LAP ลงทะเบียนกับ WLC เสร็จ จะมีการแลกเปลี่ยนข้อความ Lightweight access point protocol (LWAPP) และ AP จะเริ่มต้นการดาวน์โหลดเฟิร์มแวร์จาก WLC (ถ้าเวอร์ชันของ AP และ WLC ไม่ตรงกัน) ถ้าเฟิร์มแวร์บนบอร์ดของ LAP ไม่ตรงกับ WLC อุปกรณ์ AP จะดาวน์โหลดเฟิร์มแวร์ที่ซิงก์กับ WLC โดยขั้นตอนการดาวน์โหลดนี้จะใช้โปรโตคอล LWAPP หลังจากนั้น WLC จะจัดเตรียม LAP จากการตั้งค่าที่กำหนดให้กับ Wireless LANs จากนั้น LAP จึงจะ

สามารถยอมรับการเชื่อมต่อจากไคลเอนต์ โดย Wireless LAN ที่มีการกำหนดค่าต่างๆ ประกอบด้วย

- สิ่งที่ระบุกลุ่มของการบริการ (SSID)
- พารามิเตอร์ความปลอดภัย
- IEEE 802.11 พารามิเตอร์ เช่น
  - อัตราการส่งข้อมูล
  - ช่องสัญญาณ
  - ระดับกำลังของสัญญาณ

2.4.2 ขั้นตอนการลงทะเบียนของ WLC และ LAP

ลำดับของกิจกรรมที่จะเกิดขึ้นตามลำดับสำหรับการลงทะเบียน LAP กับ WLC :

- LAPs ส่ง DHCP discovery request เพื่อรับหมายเลขไอพี ถ้าไม่จะต้องมีการตั้งค่า เพื่อกำหนดไอพีไว้ก่อนหน้าแล้ว
- LAP ส่ง LWAPP discovery request ไปหา WLCs
- WLC ใดๆที่ได้ LWAPP discovery request จะตอบสนองด้วย LWAPP discovery response message
- จากการตอบสนอง LWAPP discovery ที่ LAP ได้รับจะเลือก WLC เพื่อเชื่อมต่อ
- LAP ส่ง LWAPP เพื่อร้องขอการเชื่อมต่อไปหา WLC และคาดหวังว่าจะได้การตอบรับ LWAPP join response
- WLC ตรวจเช็คและพิสูจน์ LAP และส่ง LWAPP join response ให้กับ LAP
- LAP ตรวจเช็คและพิสูจน์ WLC ที่เสร็จสิ้นกระบวนการค้นหาและเชื่อมต่อ ซึ่งขั้นตอนการร่วมใช้งาน LWAPP ประกอบไปด้วยการยืนยันการเข้าใช้งานที่ถูกต้องและการเข้ารหัสกุญแจที่สำคัญ ที่ถูกใช้เข้ารหัสกระบวนการร่วมเข้าใช้งาน และช่องทางการควบคุมในอนาคตโดยใช้ LWAPP
- LAP ลงทะเบียนกับ Controller (WLC)

ปัญหาแรกของ LAP ที่เจอคือ การกำหนดการส่ง LWAPP discover request (จากขั้นตอนที่ 2) โดยที่ LAP ใช้วิธีการค้นหาเป็นลำดับ และอัลกอริทึมในการค้นหา เพื่อจะตรวจสอบ รายการของ WLCs ที่ LAP สามารถที่จะส่งคำร้องขอการค้นหาไปได้

โดยกระบวนการค้นหามีดังนี้ :

- LAP จะส่ง DHCP request ไปยัง DHCP Server เพื่อที่จะได้รับหมายเลขไอพี ยกเว้นในกรณีที่กำหนดหมายเลขไอพีไว้ก่อนหน้า
- ถ้ารองรับโหมด LWAPP layer 2 บน LAP ซึ่ง LAP จะกระจายข้อความ LWAPP discovery ในเฟรม LWAPP layer 2 โดย WLC ใดๆที่เชื่อมต่อเครือข่าย และถูกตั้งค่าสำหรับโหมด LWAPP layer 2 จะตอบกลับด้วย Layer 2 discovery response ถ้าหาก LAP ไม่รองรับโหมด Layer 2 หรือถ้า WLC หรือ LAP ล้มเหลวในการรับ LWAPP discovery response ไปยัง Layer 2 LWAPP discovery message broadcast อุปกรณ์ LAP จะดำเนินการตามขั้นตอนถัดไป
- ถ้าขั้นตอนแรกล้มเหลวหรือ LAP/WLC ไม่สนับสนุนโหมด Layer 2 อุปกรณ์ LAP จะค้นหาใน Layer 3 LWAPP WLC
- ถ้าขั้นตอนที่ 3 ล้มเหลว LAP จะรีเซตและกลับไปยังขั้นตอนแรกใหม่อีกครั้ง

2.4.3 อัลกอริทึมค้นหา WLC โดยใช้ LWAPP layer 2

สำหรับโปรโตคอลการสื่อสาร LWAPP ที่ใช้ระหว่าง AP กับ WLC สามารถทำได้ โดยใช้เฟรม Ethernet ชั้นที่ 2 แต่วิธีนี้ไม่เป็นที่ยอมรับของ CISCO เพียงแต่เป็นแบบร่างใน RFC เท่านั้น

ดังนั้นโหมด LWAPP layer 2 มีเพียง Cisco 1000 series LAPs ที่รองรับโหมด LWAPP layer 2 และนอกจากนี้โหมด LWAPP layer 2 ไม่ถูกรองรับบนอุปกรณ์ Cisco 2000 Series WLCs เนื่องจากบนอุปกรณ์ WLCs รองรับเฉพาะโหมด LWAPP layer 3

ขั้นตอนแรกที่ LAPs ใช้ในการค้นหา WLC โดยอุปกรณ์ที่รองรับการทำงานโหมด LWAPP layer 2 จะกระจายข้อความ LWAPP discovery request ในเฟรมของ Layer 2 ออกไป ถ้ามี WLC อยู่ในเครือข่ายที่ถูกตั้งค่าสำหรับโหมด LWAPP layer 2

Controller จะตอบกลับด้วย Discovery response และ LAP ก็เข้าสู่เฟสของการร่วมใช้งาน (Join) โดยตัวอย่างของผลลัพธ์ที่แสดงออกมา เช่น

```
Thu Sep 27 00:24:25 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY
REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '2'
Thu Sep 27 00:24:25 2007: 00:0b:85:51:5a:e0 Successful transmission
of
LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 2
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN
REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:48:53:c0 on port '2'
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0:
txNonce  00:0B:85:48:53:C0 rxNonce  00:0B:85:51:5A:E0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 LWAPP Join-Request MTU
path from
AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Successfully added NPU
Entry for
AP 00:0b:85:51:5a:e0 (index 48)Switch IP: 0.0.0.0, Switch Port: 0,
intIfNum 2,
vlanId 0AP IP: 0.0.0.0, AP Port: 0, next hop MAC: 00:0b:85:51:5a:e0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Successfully
transmission of
LWAPP Join-Reply to AP 00:0b:85:51:5a:e0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Register LWAPP event for
AP 00:0b:85:51:5a:e0 slot 0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Register LWAPP event for
AP 00:0b:85:51:5a:e0 slot 1
```

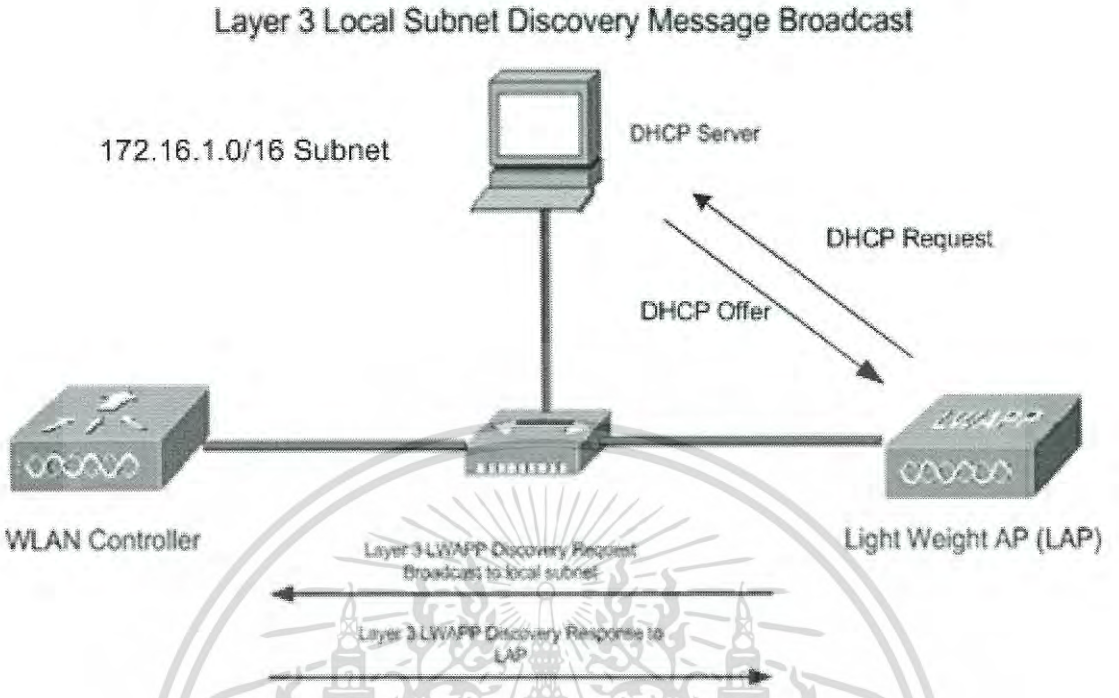
2.4.4 อัลกอริทึมค้นหา WLC โดยใช้ LWAPP layer 3

LAPs ใช้อัลกอริทึมการค้นหาบนเลเยอร์ 3 ถ้าวิธีการค้นหาบนเลเยอร์ 2 ไม่รองรับหรือล้มเหลว

อัลกอริทึมการค้นหาบนเลเยอร์ 3 ถูกใช้ในการสร้างรายการตัวควบคุม (Controller) หลังจากรายการตัวควบคุมถูกสร้าง AP จะเลือก WLC และพยายามเข้าร่วมใช้งาน โดยกระบวนการนี้จะทำซ้ำเรื่อยๆ จนกว่าจะเจอ WLC อย่างน้อยหนึ่ง และร่วมใช้งานได้สำเร็จ

ต่อไปเป็นการอธิบายขั้นตอนของ Layer 3 discovery algorithm ที่พยายามค้นหา WLC หลังจาก LAP ได้รับหมายเลขไอพีจาก DHCP Server แล้ว โดยมีขั้นตอนดังนี้

- LAP กระจายข้อความ Layer 3 LWAPP discovery บนซับเน็ตไอพีในพื้นที่เดียวกัน WLC ใดๆที่ถูกตั้งค่าไว้สำหรับโหมด Layer 3 LWAPP และที่เชื่อมต่ออยู่ในสถานที่เดียวกัน ได้รับข้อความ Layer 3 LWAPP discovery
- แต่ละ WLCs ที่ได้รับข้อความ LWAPP discovery จึงตอบกลับด้วยข้อความ LWAPP discovery response ไปยัง LAP แบบ Unicast



รูปที่ 2.9 ภาพแสดงขั้นตอนการค้นหา WLC

2.4.5 กระบวนการเลือก WLC

หลังจาก LAP เสร็จขั้นตอนการค้นหาจากการใช้อัลกอริทึม Layer 3 LWAPP WLC Discovery แล้ว อุปกรณ์ LAP จะเลือก WLC จากรายการสมัครของ WLC และการส่งที่มี LWAPP WLC เข้าร้องขอร่วมทำงาน

WLC ฝั่งสิ่งที่เป็นข้อมูลสำคัญใน LWAPP discovery response ดังนี้

- The controller sysName
- The controller type
- ความจุ Controller AP and AP load ในขณะนั้น
- The Master Controller flag
- An AP-manager IP address

LAP ใช้ข้อมูลเหล่านี้เพื่อทำการเลือก Controller กับใช้กฎเหล่านี้เพื่อเลือก อุปกรณ์ตัวที่มีลำดับสูงกว่าดังนี้

- ถ้า LAP มีการตั้งค่า controller ลำดับที่ 1, 2 และ/หรือ 3 ไว้แล้ว LAP จะตรวจสอบฟิลด์ Controller sysName (จาก LWAPP discovery responses) ในการพยายามหา WLC ที่มีการตั้งค่าแล้วเป็น controller ลำดับที่ 1 ถ้าหาก LAP หา sysName เจอเหมือนกันสำหรับเลือกเป็นอุปกรณ์ลำดับที่ 1 แล้ว LAP จะส่ง LWAPP join request ไปที่ WLC ถ้า LAP ไม่สามารถหา Controller ลำดับที่ 1 เจอ หรือ LWAPP ไม่สามารถเชื่อมต่อได้ อุปกรณ์ LAP จะพยายามที่จะหา sysName ที่ตรงกับ Controller ลำดับที่ 2 ที่ได้ถูกตั้งค่าไว้ และถ้าไม่พบ WLC ลำดับที่ 2 หรือไม่สามารถเชื่อมต่อได้ LAP จะทำซ้ำกระบวนการนี้เพื่อหา Controller ลำดับที่ 3
- LAP มองหาฟิลด์ Master controller flag ใน LWAPP discovery responses จากการสมัครของ WLCs ถ้าหนึ่งในสิ่งต่อไปนี้เป็นจริง :
    - ไม่มีการตั้งค่า Controller ลำดับที่ 1, 2 และ/หรือ 3 สำหรับ AP
    - Controller เหล่านั้นไม่พบในรายการสมัคร
    - LWAPP เชื่อมต่อเพื่อเข้าร่วมใช้งาน Controller เหล่านั้นล้มเหลว
- ถ้าหาก LAP ไม่สามารถเข้าร่วมกับ WLC ได้สำเร็จบนพื้นฐานของหลักเกณฑ์ ในขั้นตอนที่ 1 และ 2 โดย LAP จะพยายามที่จะเชื่อมต่อเพื่อร่วมใช้งานกับ WLC ที่มีความจุที่มากที่สุด

หลังจาก LAP เลือก WLC แล้ว LAP ส่ง LWAPP เพื่อร้องขอการร่วมทำงานกับ WLC ในการร้องขอของ LWAPP อุปกรณ์ LAP ได้ฝังลงชื่อใบรับรองดิจิตอล X.509 เมื่อใบรับรองนั้นถูกตรวจสอบแล้ว WLC จะตอบกลับ LWAPP ที่ร้องขอการเชื่อมต่อ เพื่อที่จะแสดงให้ LAP ที่เชื่อมต่ออุปกรณ์ควบคุมได้สำเร็จ ซึ่งอุปกรณ์ WLC ฝังใบรับรองดิจิตอล X.509 ของตัวเอง ใน LWAPP join response ที่ LAP จะต้องตรวจสอบ หลังจาก LAP ตรวจสอบใบรับรองของ WLC แล้ว LWAPP ถึงจะเสร็จสิ้นในขั้นตอนของการเชื่อมต่อ

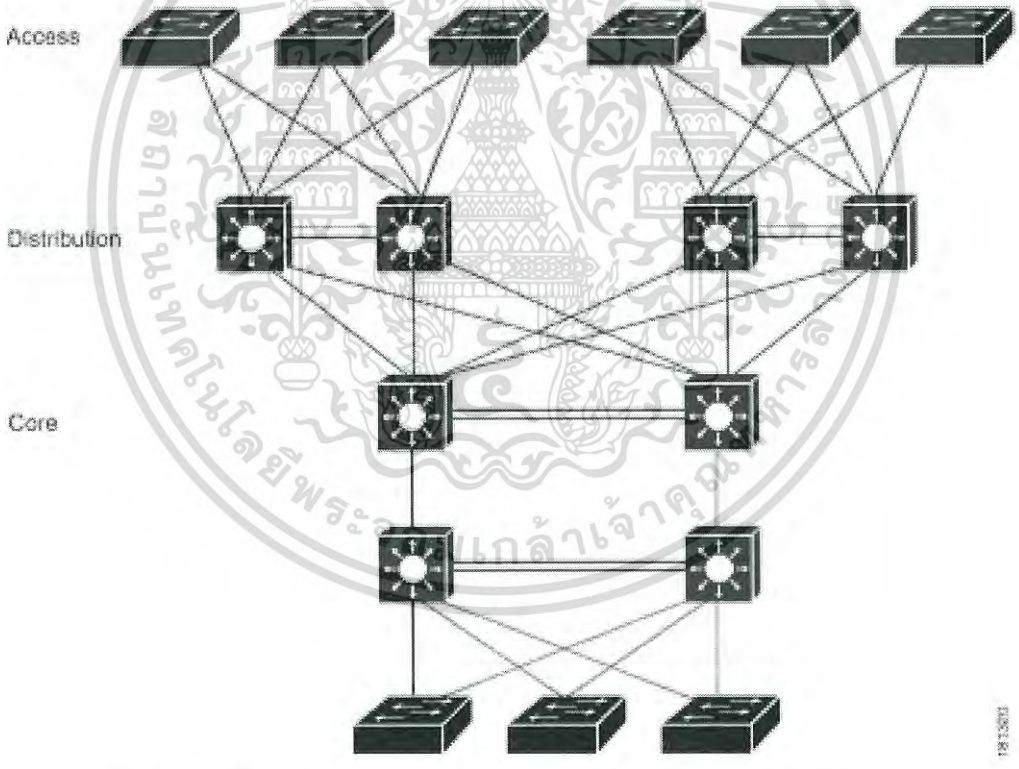
LAP และ WLC ดูแลการแยกชิ้นส่วนและประกอบใหม่สำหรับท่อ LWAPP พวกมันดำเนินการภายใต้สมมติฐาน MTU 1500 ไบต์ ซึ่งไม่สามารถตั้งค่าพารามิเตอร์ที่ AP หรือ WLC ถ้า MTU ใหญ่กว่า 1500 ไบต์ แพ็คเกตจะถูกแยกชิ้นส่วนของแพ็คเกต และส่งแพ็คเกตข้ามไป ซึ่งระบบสามารถจัดการดูแลได้ถึง 4 ชิ้นส่วน ในขณะที่เวอร์ชัน 3.2 หรือเวอร์ชันก่อนหน้าสนับสนุนเพียง 2 ชิ้นส่วน

2.5 Virtual Switching Systems (VSS)

2.5.1 ภาพรวมของ VSS

การดำเนินการทางเครือข่ายที่เพิ่มความน่าเชื่อถือยิ่งขึ้นผ่านการตั้งค่าอุปกรณ์ Switch และการเตรียมพร้อมลิงค์เพื่อเชื่อมต่อแบบคู่ซ้ำซ้อน (Redundant)

จากรูปที่ 2.10 แสดงตัวอย่างการตั้งค่าของเครือข่าย รวมไปถึงการเชื่อมต่อ และส่วนประกอบของเครือข่ายแบบซ้ำซ้อน สามารถเพิ่มความซับซ้อนให้กับการออกแบบ และดำเนินการ ซึ่งการทำสวิทซ์เสมือน (Virtual Switching) ลดความยุ่งยากของเครือข่าย โดยการลดจำนวนของส่วนประกอบของเครือข่าย และซ่อนความซับซ้อน ของการจัดการอุปกรณ์สวิทซ์และลิงค์เชื่อมต่อที่มีความซ้ำซ้อน

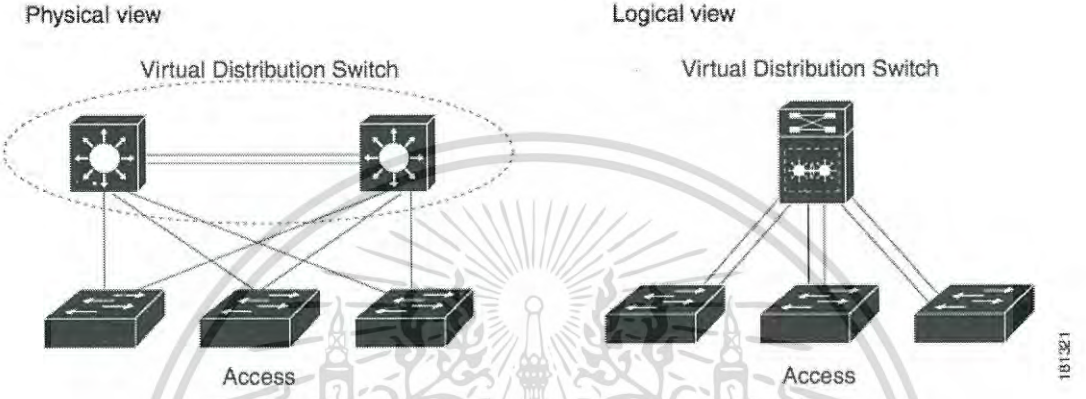


รูปที่ 2.10 แสดงตัวอย่างการตั้งค่าและเชื่อมต่อของเครือข่ายแบบซ้ำซ้อน

VSS ช่วยลดความยุ่งยากในการตั้งค่าเครือข่ายและดำเนินการ โดยการลดทอนจำนวนของการหาเส้นทางข้างเคียงของชั้น 3 และไม่มีลูปบนโครงสร้างชั้น 2 ตาม OSI model

2.5.2 แนวคิดสำคัญสำหรับ VSS

VSS เกิดจากการรวมกันของคู่อุปกรณ์สวิทซ์กลายเป็นองค์ประกอบเครือข่ายเดียว ตัวอย่างเช่น VSS ในชั้นการกระจายของเครือข่ายที่มีการโต้ตอบกับการเข้าถึง และเครือข่ายหลัก ดังรูปที่ 2.11



รูปที่ 2.11 แสดง VSS ในเครือข่ายแบบกระจาย

Access switch เชื่อมต่อถึงสวิทซ์ทั้งสองของ VSS โดยใช้หนึ่ง Port-channel ในเชิงตรรกะ ซึ่ง VSS จัดการความซ้ำซ้อนและโหลดบาเลนซ์ (Load balance) บน Port-channel และยังมีความสามารถเปิดใช้ “Loop-free” บนโครงสร้างเครือข่ายชั้นที่ 2 และ VSS ยังลดความยุ่งยากบนโครงสร้างเครือข่ายชั้นที่ 3 โดยลดองค์ประกอบของ Routing peers ในเครือข่าย

2.5.3 VSS Active and VSS Standby Switch

เมื่อสร้างหรือเริ่มระบบใหม่อีกครั้ง VSS จะมีการเจรจาต่อรองบทบาทของ Peer switches จากนั้น Switch หนึ่งตัวจะกลายมาเป็น Active switch และตัวอื่นๆจะกลายเป็น Standby switch

VSS ที่ทำหน้าที่เป็น Active switch จะควบคุม VSS ทำงานบนชั้นที่ 2 และ 3 ควบคุมโปรโตคอลสำหรับโมดูลบนทั้งสองสวิทซ์ บน VSS Active switch จะให้บริการฟังก์ชั่นดูแลจัดการสำหรับ VSS เช่น การใส่โมดูลเพิ่มหรือนำออกขณะที่เครื่องทำงานอยู่ และอินเตอร์เฟสคอนโซล

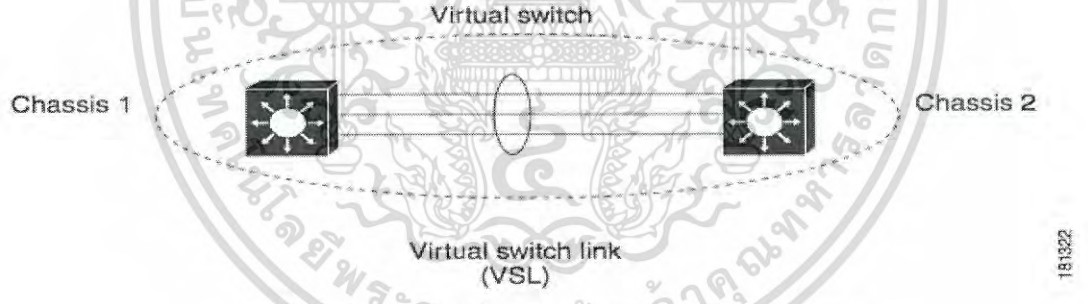
ทั้ง VSS ที่เป็น Active และ Standby switches จะปฏิบัติหน้าที่ส่งต่อแพ็คเกต สำหรับข้อมูลจะเข้าบนอินเตอร์เฟสโฮสเชิงตรรกะ และไม่ว่าอย่างไร VSS standby switch จะส่งส่วนทราฟฟิคในการควบคุมทั้งหมดไปให้ VSS active switch ที่กำลังทำงานอยู่

2.5.4 Virtual Switch Link

สำหรับสองสวิทซ์ของ VSS ที่แสดงเป็นองค์ประกอบเครือข่ายเดียว ซึ่งสวิทซ์ทั้งสองจำเป็นจะต้องแลกเปลี่ยนข้อมูลและทราฟฟิคร่วมกัน

Virtual Switch Link (VSL) เป็นลิงค์เชื่อมต่อพิเศษที่ขนส่งทั้งทราฟฟิคควบคุม และข้อมูลระหว่างอุปกรณ์ทั้งสองของ VSS ดังรูปที่ 2.12

VSL ถูกใช้เป็น EtherChannel มีลิงค์รวมกันได้มากสุด 8 ลิงค์ และให้การควบคุม และจัดการทราฟฟิคที่มีความสำคัญสูงกว่าทราฟฟิคข้อมูลทั่วไป ดังนั้นการสื่อสารที่ใช้ควบคุมและจัดการไม่มีทางที่จะถูกยกเลิก ส่วนทราฟฟิคข้อมูลจะถูกกระจายให้เกิดความสมดุล ผ่านลิงค์ VSL โดย EtherChannel load-balancing algorithm



รูปที่ 2.12 แสดงการเชื่อมต่อ Virtual Switch Link (VSL)

2.5.5 Multichassis EtherChannel (MEC)

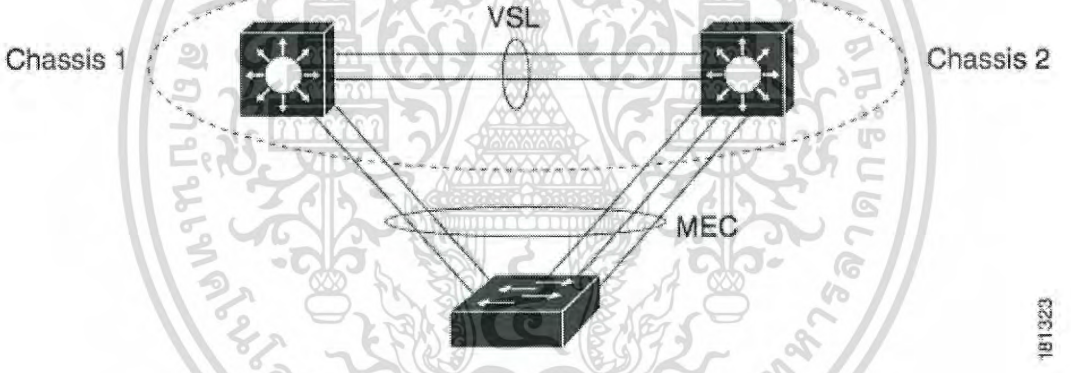
EtherChannel (หรือที่เรียกกันว่า port channel) คือการรวบรวมของสองลิงค์กายภาพหรือมากกว่าที่ประกอบรวมกันเป็นหนึ่งลิงค์เชิงตรรกะ โดยโปรโตคอล Layer 2 ดำเนินการบน EtherChannel เป็นเหมือนกับเป็นหน่วยเดียวเชิงตรรกะ

VSS เปิดการสร้างของ Multichassis EtherChannel (MEC) ซึ่งเป็น EtherChannel ที่มีสมาชิกหลายพอร์ตสามารถกระจายไปทั่วทุกสมาชิกของสวิทซ์ใน VSS ได้ เพราะว่าสวิทซ์ที่

ไม่ใช่ VSS ที่เชื่อมต่อมายัง VSS จะมอง MEC เป็นเหมือน EtherChannel ทั่วๆไป สวิทช์ที่ไม่ใช่ VSS สามารถเชื่อมต่อได้ใน dual homed manner

ในรูปที่ 2.13 แสดงการเชื่อมต่อ dual-homed สำหรับ MEC เข้ากับ VSS โดย VSS ดูเหมือนเป็นสวิทช์เดี่ยวเชิงตรรกะ ทราฟฟิคจะข้ามผ่านและ MEC สามารถที่จะกระจายโหลดภายในผ่านสมาชิก VSS มาตรฐาน นอกจากนี้ Cisco MEC รองรับโปรโตคอลการมัดรวมทั้ง LACP และ PAgP ตลอดจนโหมด ON

VSS รองรับ EtherChannel มากสุด 256 ข้อจำกัดนี้นำไปใช้กับจำนวนทั้งหมดของ EtherChannel ตามปกติ และ MECs เพราะว่า VSL ต้องการ 2 EtherChannel (1 เส้นสำหรับแต่ละสวิทช์ใน VSS)



รูปที่ 2.13 แสดง VSS กับ MEC

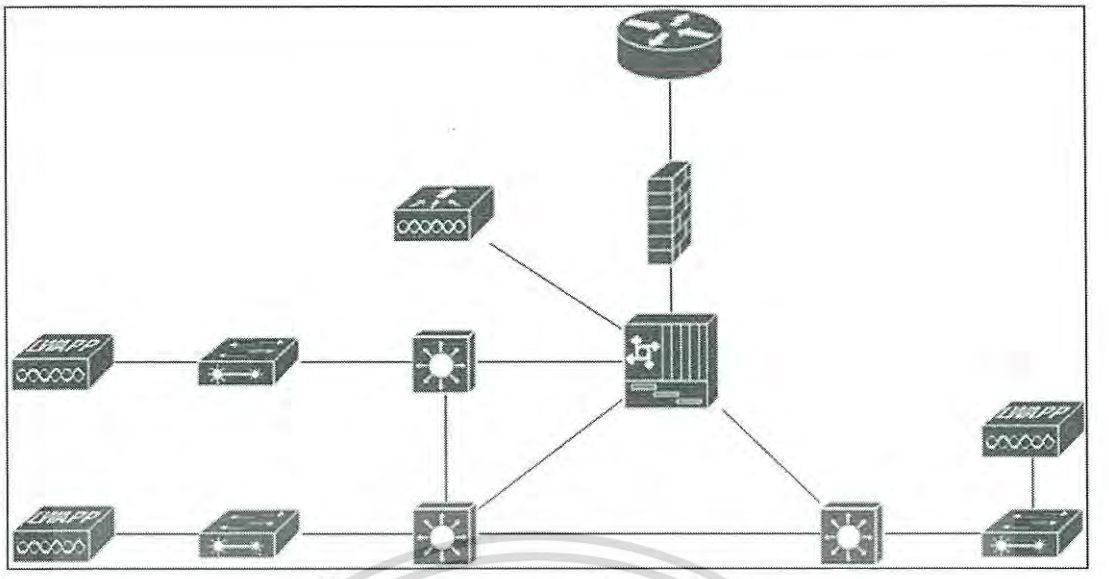
บทที่ 3
วิธีการดำเนินงานในเครือข่ายไร้สายของลูกค้ารายที่หนึ่ง

3.1 วิเคราะห์งานที่ได้รับมอบหมาย

เนื่องจากบริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด ได้รับการว่าจ้างในการดำเนินการปรับปรุงระบบเครือข่ายทั้งหมดของสถาบันการศึกษาแห่งหนึ่ง ซึ่งในส่วนที่ได้รับมอบหมาย จะเป็นในส่วนของระบบเครือข่ายไร้สาย โดยการติดตั้งอุปกรณ์เครือข่ายไร้สาย เพื่อแทนที่ของเดิมที่มีอยู่ รวมทั้งติดตั้ง Wireless LAN Controller (WLC) เพื่อควบคุมและดูแลจัดการ Access Point (AP) ที่ติดตั้งไปเหล่านั้น ซึ่งระบบเครือข่ายไร้สายของเดิมที่มีอยู่นั้น ได้มีการติดตั้ง AP แบบ Standalone ทำให้ยากต่อการดูแลจัดการ ส่งผลให้ Access Point (AP) เดิมที่มีอยู่ ไม่สามารถใช้งานได้เป็นจำนวนมากและเมื่อเกิดปัญหาขัดข้องเจ้าหน้าที่ของทางสถาบันศึกษาจะรับรู้หลังจากที่บุคลากรและนักศึกษาแจ้งเข้ามาเท่านั้น

ดังนั้นการปรับปรุงระบบเครือข่ายไร้สายครั้งนี้จะช่วยให้ระบบทำงานได้อย่างมีประสิทธิภาพมากขึ้น สามารถดูแลจัดการได้ง่าย มีการใช้ VLAN เพื่อแบ่ง broadcast domain ทำให้ไม่มีข้อมูลที่อุปกรณ์ใช้สำหรับสื่อสารกันเองมากจนเกินไปในเครือข่าย อีกทั้งยังมีการแบ่ง data traffic และ management traffic ออกจากกัน

เพราะฉะนั้นรูปแบบการเชื่อมต่อของเครือข่ายเพื่อให้ได้เครือข่ายไร้สายที่มีประสิทธิภาพภายใต้งบประมาณและเวลาจึงมีลักษณะดังรูป



รูปที่ 3.1 แผนผังจำลองการเชื่อมต่อที่ดำเนินการ

จากรูปที่ 3.1 แผนผังจำลองการเชื่อมต่อที่ได้ดำเนินการในการปฏิบัติงาน โดยแผนผังนี้ได้ถูกปรับมาจากแผนผังการดำเนินการจริง เนื่องมาจากเงื่อนไขที่ตกลงระหว่าง บริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด กับผู้ว่าจ้าง จึงไม่สามารถที่จะเปิดเผยข้อมูล ในบางส่วนได้

ซึ่งแผนผังที่ใช้ในการปฏิบัติงานได้รับการออกแบบมาจากการร่วมกันของวิศวกรจากทางบริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด และผู้ว่าจ้าง โดยวิศวกรให้คำแนะนำกับทางผู้ว่าจ้าง พร้อมพิจารณาร่วมกับปัจจัย และข้อจำกัดต่างๆ ที่ได้มาจากผู้ว่าจ้าง

ในการปฏิบัติงานได้มีการกำหนดจำนวนอุปกรณ์ LAP ในแต่ละอาคาร จึงได้ดำเนินการจัดสรร และติดตั้งอุปกรณ์ในแต่ละอาคาร โดยมีการใช้ LAP เชื่อมต่อกับสาย UTP และใช้ Power injector เพื่อจ่ายไฟฟ้าให้กับอุปกรณ์ผ่านสาย UTP ซึ่งเชื่อมต่ออยู่กับ Access Switch ของแต่ละชั้นของอาคาร และ Access Switch แต่ละชั้นจะถูกเชื่อมต่อเข้ากับ Distributed Switch ที่อยู่ตามจุดต่างๆ สุดท้าย Distributed Switch จะเชื่อมต่อเข้ากับ Core Switch ซึ่งเป็นอุปกรณ์ส่งผ่านข้อมูลหลักของลูกค้า โดยมี WLC เชื่อมต่อเข้ากับ Core Switch ใน Data Center ของลูกค้า

จาก Core Switch มีการเชื่อมต่อเข้ากับ Firewall ซึ่งมีการตั้งค่ากฎ เพื่อคัดกรองข้อมูลที่ไหลผ่านเครือข่ายระหว่างภายใน และภายนอกองค์กร โดยการเชื่อมต่ออินเทอร์เน็ต ภายนอกองค์กร จะมีการหาเส้นทางเพื่อส่งแพ็คเกต ผ่านอุปกรณ์ Router

นอกจากนี้ข้อมูลการหาเส้นทางภายในองค์กร ได้มีการใช้อุปกรณ์ Layer 3 เพื่อแลกเปลี่ยนข้อมูลเหล่านี้ ในที่นี้ ได้แก่ Core switch และ Distributed switch โดยใช้โปรโตคอล OSPF ในการแลกเปลี่ยนข้อมูลการหาเส้นทาง พร้อมทั้งตั้งค่ารากของ VLAN ไว้ที่ Core switch เพื่อง่ายต่อการจัดการ

โดยการกำหนด VLAN ของ LAP ในแต่ละชั้นจะถูกกำหนดให้แตกต่างกัน ในแต่ละชั้น เพื่อแบ่ง Broadcast domain ออกจากกัน ทำให้ไม่มี Broadcast frame ในเครือข่ายมากจนเกินไป

3.1.1 อุปกรณ์ที่ใช้ในการติดตั้ง

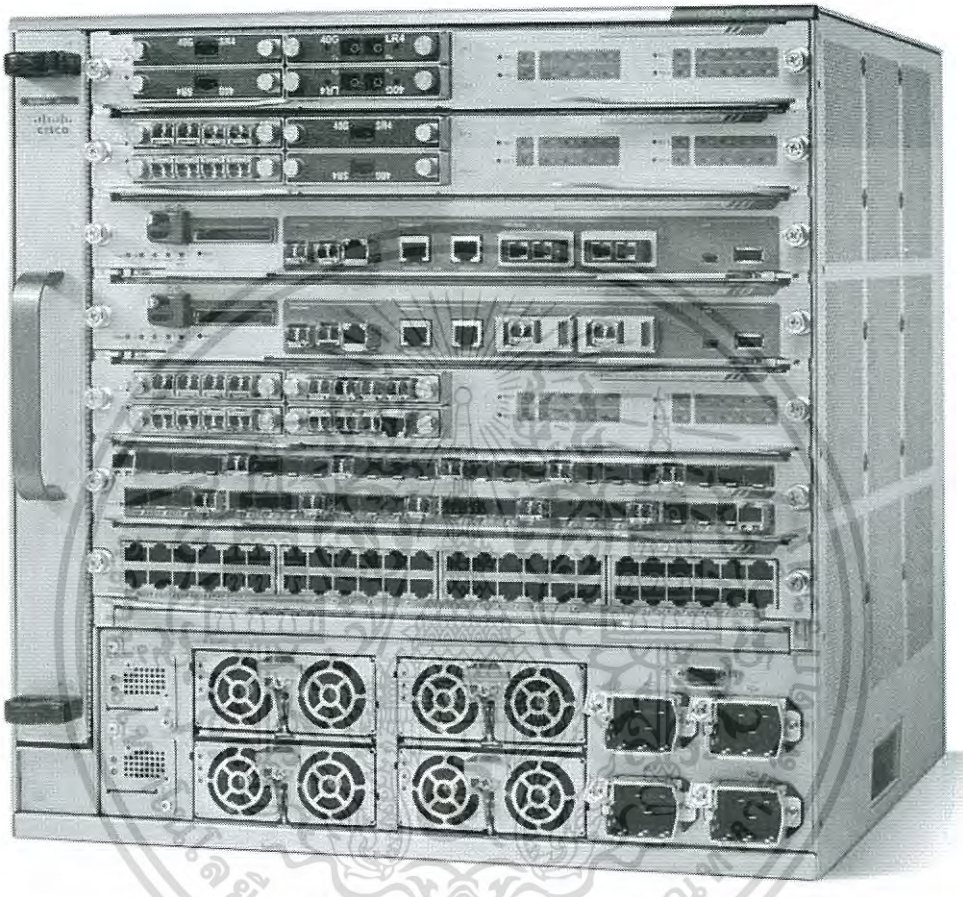
a) Cisco ASR1001-X Router

เพื่อใช้ในการคำนวณหาเส้นทางเครือข่าย

รูปที่ 3.2 Cisco ASR1001-X Router

b) Cisco 6807-XL Switch

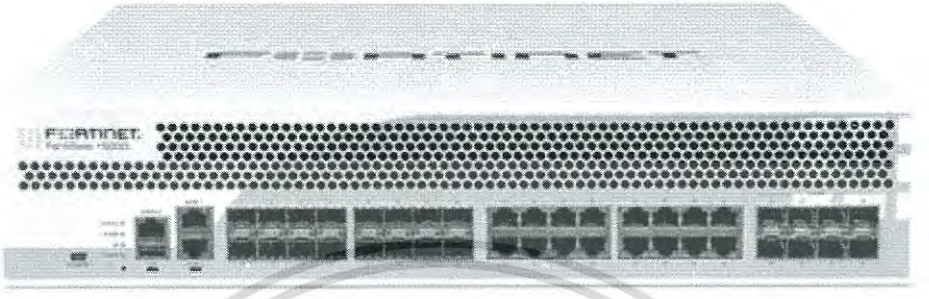
ใช้เพื่อเป็นอุปกรณ์เชื่อมต่อกับเครือข่ายหลัก



รูปที่ 3.3 Cisco 6807-XL Switch

c) Fortigate FG-1500D Firewall

ใช้เพื่อเป็นอุปกรณ์ป้องกันและรักษาความปลอดภัยระบบเครือข่าย



รูปที่ 3.4 Fortigate FG-1500D Firewall

d) Fortigate Log Analyzer FAZ02000B-E02S

ใช้เพื่อเป็นอุปกรณ์เก็บข้อมูลจราจรคอมพิวเตอร์ทางอินเทอร์เน็ต

รูปที่ 3.5 Fortigate Log Analyzer FAZ02000B-E02S

e) Cisco Wireless Controller 5508

ใช้เป็นอุปกรณ์ควบคุมระบบเครือข่ายไร้สาย

รูปที่ 3.6 Cisco Wireless Controller 5508

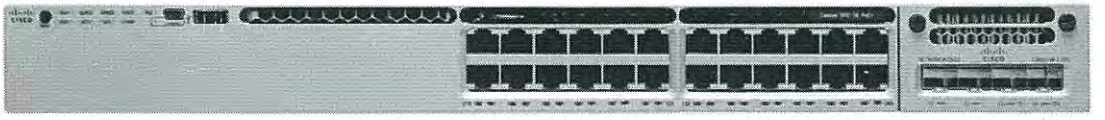
f) Cisco Wireless Access Point 2702I

ใช้เป็นอุปกรณ์กระจายสัญญาณไร้สาย

รูปที่ 3.7 Cisco Wireless Access Point 2702I

g) Cisco 3850 SFP Switch

อุปกรณ์เชื่อมต่อระบบเครื่องข่ายรองแบบที่ 1



รูปที่ 3.8 Cisco 3850 SFP Switch

h) Cisco 3850 Switch

อุปกรณ์เชื่อมต่อระบบเครื่องข่ายรองแบบที่ 2

รูปที่ 3.9 Cisco 3850 Switch

i) Cisco 2960 Switch

อุปกรณ์เชื่อมต่อระบบเครื่องข่ายปลายทาง

รูปที่ 3.10 Cisco 2960 Switch

3.2 การปฏิบัติงาน

3.2.1 การวางตำแหน่งในการติดตั้ง Cisco wireless access point

ตำแหน่งที่ใช้ในการติดตั้งอุปกรณ์ Access Point ออกแบบโดยการที่วิศวกรร่วมกับลูกค้าเพื่อให้ได้ตำแหน่งในการวางที่ดีภายใต้เงื่อนไขต่างๆ

3.2.2 การติดตั้งอุปกรณ์ Cisco wireless access point

เนื่องจากอุปกรณ์ Access Point เดิมที่มีอยู่ไม่สามารถใช้งานได้หลายตำแหน่ง ทำให้การติดตั้ง Access Point ตัวใหม่สามารถดำเนินการได้ทันที

โดยก่อนการติดตั้ง อุปกรณ์ Access point (AP) ได้ทำการ Staging เพื่อตั้งค่าบางส่วน คือ IP address, IP netmask, Default Gateway และ Primary Controller ซึ่งในการ Staging หรือเตรียมอุปกรณ์ก่อนการติดตั้งจะต้องมีการดำเนินการดังนี้

- เชื่อมต่อ Access Point เข้ากับ PoE switch และให้สามารถสื่อสารกับ Wireless LAN Controller ได้
- ตั้งค่าเบื้องต้น ได้แก่ IP address, IP netmask, Default Gateway และ Primary Controller หลังจากการตั้งค่าเบื้องต้นเสร็จ ตัวอุปกรณ์จะ Discover เพื่อค้นหา Controller ตามที่ได้ตั้งค่า Primary Controller ไว้ หลังจากที่เชื่อมต่อกับ Controller ได้แล้ว ตัวอุปกรณ์จะ Reboot ตัวเอง
- หลังจากที่อุปกรณ์ Reboot ตัวเองเสร็จ จะต้องตั้งค่า Primary Controller อีกครั้ง เนื่องจากเป็นข้อผิดพลาดของอุปกรณ์ Access Point รุ่นนี้
- ตรวจสอบและยืนยันว่าอุปกรณ์ Access Point สามารถเชื่อมต่อกับ Controller ได้ โดยดูจากหน้าเว็บจัดการที่อยู่ใน Wireless LAN Controller (WLC)

3.2.3 การตั้งค่าอุปกรณ์

ในการตั้งค่าอุปกรณ์ Access point แต่ละตัวจะมีลักษณะคล้ายคลึงกัน โดยอุปกรณ์แต่ละตัวจะแตกต่างกันเฉพาะหมายเลข IP address เท่านั้น

สำหรับตัวอย่างการตั้งค่า **Access point** มีดังนี้

```
capwap ap ip address 10.0.0.55 255.255.255.0
capwap ap ip default-gateway 10.0.0.254
capwap ap controller ip address 10.0.100.10
```

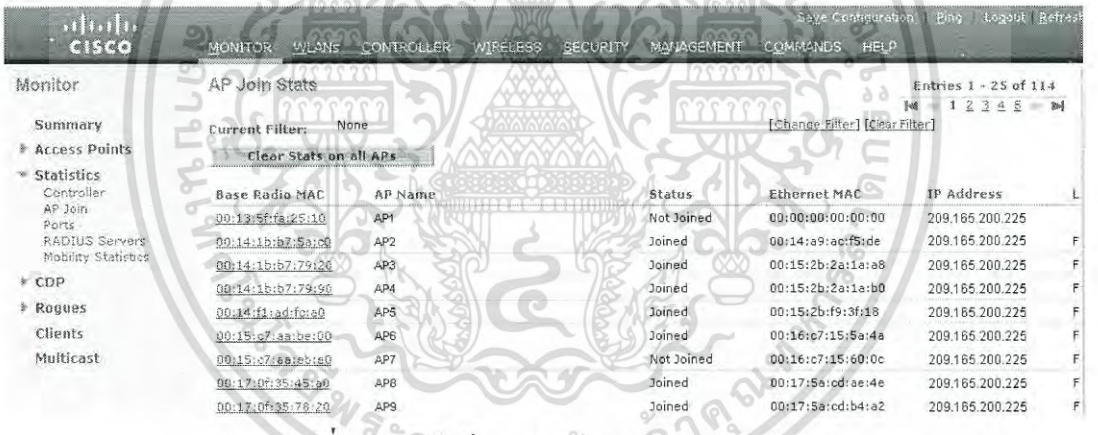
ในขั้นแรกเป็นการตั้งค่า IP address, IP netmask และ Default Gateway ให้กับตัวอุปกรณ์ Access Point ต่อมาคือกำหนด IP address ของ Wireless LAN Controller (WLC) โดยใส่ IP address ของ Controller ลงไป โดยใช้คำสั่ง capwap ย่อมาจาก Control and Provisioning of Wireless Access Points เป็นคำสั่งที่ใช้ควบคุมจัดการ Access Point โดยมี Controller เป็นตัวจัดการดูแล

สุดท้ายเป็นการตั้งค่าในหมวดของการทำ High Availability (HA) ให้กับ Access point และสำหรับสถาบันแห่งนี้มี Controller เพียงตัวเดียว ดังนั้นจึงมีแค่ Primary-base ในการตั้งค่า

```
capwap ap primary-base WLC-Name 10.0.100.10
```

ทั้งนี้ IP address ของ Controller ไม่จำเป็นต้องอยู่ในเครือข่ายวงเดียวกันกับ Access point แต่ Access point จะต้องสามารถติดต่อได้ โดยใช้คำสั่งดังนี้

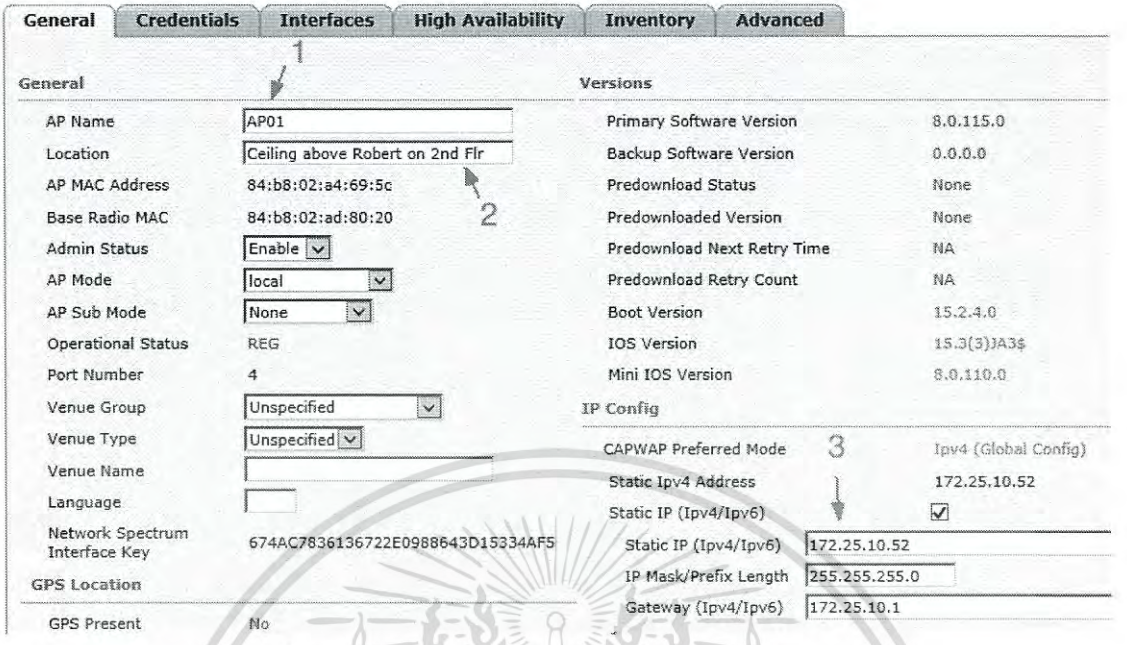
สำหรับการตั้งค่า **Wireless LAN Controller**



รูปที่ 3.11 หน้าเว็บแสดงรายการ AP บน WLC

จากรูปที่ 3.11 เป็นตัวอย่างที่แสดงรายชื่อและข้อมูลโดยสรุปของ Access point ที่เข้ามาเชื่อมต่อแต่ละตัว ซึ่งปกติการที่ Access point เชื่อมต่อกับ Controller ครั้งแรก ชื่อของ Access point จะเป็นหมายเลข MAC address เป็นค่าเริ่มต้น

ดังนั้นเราจึงต้องเปลี่ยนให้ชื่อ Access point (AP) นั้น ให้สื่อความหมายเพื่อง่ายต่อการจัดการ โดยการเปลี่ยนชื่อ AP สามารถทำได้โดยคลิกที่ชื่อ AP จากนั้นเปลี่ยนชื่อที่ช่องชื่อ AP Name ในหมวดของ General ตามรูปที่ 3.12 หมายเลขที่ 1 แล้วกด Apply ด้านบนขวา



รูปที่ 3.12 ภาพแสดงการตั้งค่าของ Access Point บน WLC

และเพื่อให้การจัดการง่ายขึ้นควรใส่สถานที่ติดตั้งของ Access point (AP) ในช่องชื่อ Location นอกจากนี้ยังสามารถแก้ไข เปลี่ยนแปลง IP address ของ AP ได้โดยแก้ไขตรงหมายเลข 3 ตามรูปที่ 3.12

นอกจากนี้เราสามารถตั้งค่าเพิ่ม IP address ของ WLC ได้จากหน้าเว็บทันที ถ้าหากในอนาคตมีการพัฒนาประสิทธิภาพและความทนทานมากขึ้น โดยได้ตั้งค่าที่ High availability tab โดยลักษณะของการตั้งค่าจะเป็นดังนี้

รูปที่ 3.13 ตัวอย่างการตั้งค่าเพิ่ม WLC เพื่อการทำ HA

ในการตั้งค่าสามารถเพิ่ม WLC เพื่อทำ High availability (HA) ได้มากสุด 3 เครื่อง ได้แก่ Primary controller, Secondary controller และ Tertiary controller ตามลำดับ โดยการใช้จะต้องกรอกชื่อของ Controller และ Management IP Address (IP ของ Controller)

ส่วนการใช้งาน Access point (AP) จะเลือกเชื่อมต่อกับ Controller ตัวแรกก่อนเสมอ ถ้าหากไม่สามารถเชื่อมต่อกับ Controller ตัวแรกได้ AP จึงจะพยายามเชื่อมต่อกับ Controller ตัวที่ 2 และ 3 ตามลำดับ

3.2.4 Site survey

เป็นการสำรวจสถานที่หลังทำการติดตั้ง Access point (AP) เสร็จเรียบร้อย เพื่อทำการสำรวจความครอบคลุมของสัญญาณไร้สายที่ได้ติดตั้งแล้ว และ นำมาใช้สำหรับทำเป็นเอกสารสรุปการทำงานให้กับลูกค้า รวมถึงใช้ประเมินประสิทธิภาพของสัญญาณตามสัญญาณที่ได้ตกลงกันไว้

3.2.4.1 การเตรียมความพร้อม

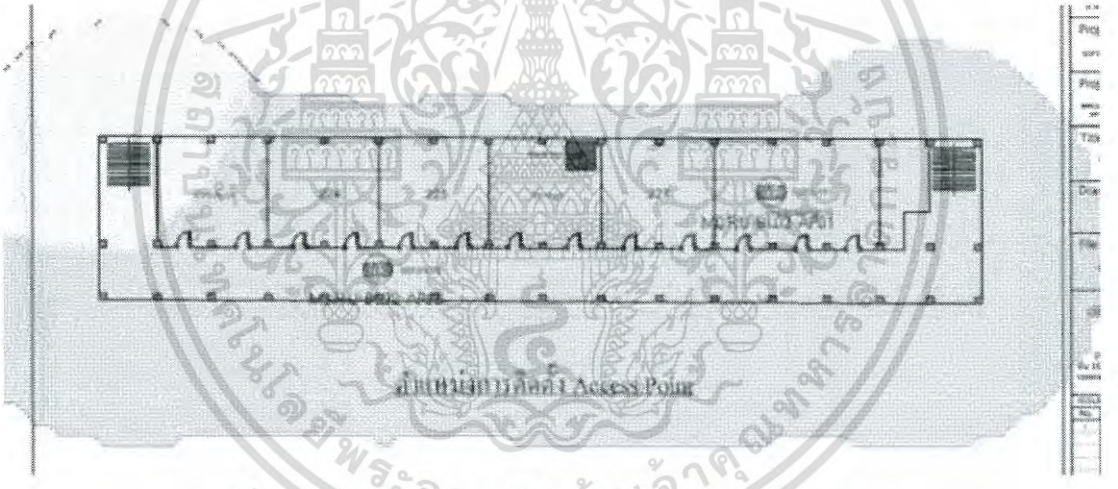
ในการเตรียมสำรวจสถานที่จะต้องมี Floor plan ของแต่ละชั้นในแต่ละอาคารที่ทำการติดตั้งและโปรแกรมชื่อว่า AIRMAGNET ผลิตโดยบริษัท FLUKE NETWORK ซึ่งการใช้อุปกรณ์จะใช้ผ่าน USB Port ของคอมพิวเตอร์ เพื่อเป็นตัวรับสัญญาณที่ต้องการจะตรวจสอบ

3.2.4.2 การเดินสำรวจ

ก่อนการเดินสำรวจจะต้องกำหนดอัตราส่วนของแผนภาพ (Floor plan) ก่อน โดยการใช้ Tool ในโปรแกรมลากจากจุดหนึ่งไปยังอีกจุดหนึ่งแล้วใส่ขนาดที่มีหน่วยเป็นเมตร ในที่นี้ได้ใช้ความกว้างของบานประตูในการกำหนดอัตราส่วนนี้ เพื่อให้โปรแกรมนำไปคำนวณ

หลังจากที่ได้ตั้งค่าเบื้องต้นแล้ว จะต้องเลือก SSID ของ Access point ที่เราต้องการดักจับสัญญาณ จากนั้นเราจึงเดินตามจุดต่างๆในแต่ละชั้น โดยจุดหลักๆคือ ตำแหน่งที่ได้รับสัญญาณไร้สายได้ดีที่สุด ในที่นี้ได้วัดใต้อุปกรณ์ Access point หนึ่งจุด จากนั้นจึงวัดที่มุมห้อง 4 จุด และสุดท้ายเป็นตามทางเดินหน้าห้องเรียนทุกๆ 3-5 เมตร เมตรละหนึ่งจุด

หลังจะมาร์คจุดได้ครบทั้งชั้นตัวโปรแกรม AIRMAGNET จะทำการคำนวณระยะการครอบคลุมของสัญญาณไร้สายของอุปกรณ์ที่เราเลือกไว้ออกมาเป็นไฟล์ ตัวอย่างเช่น



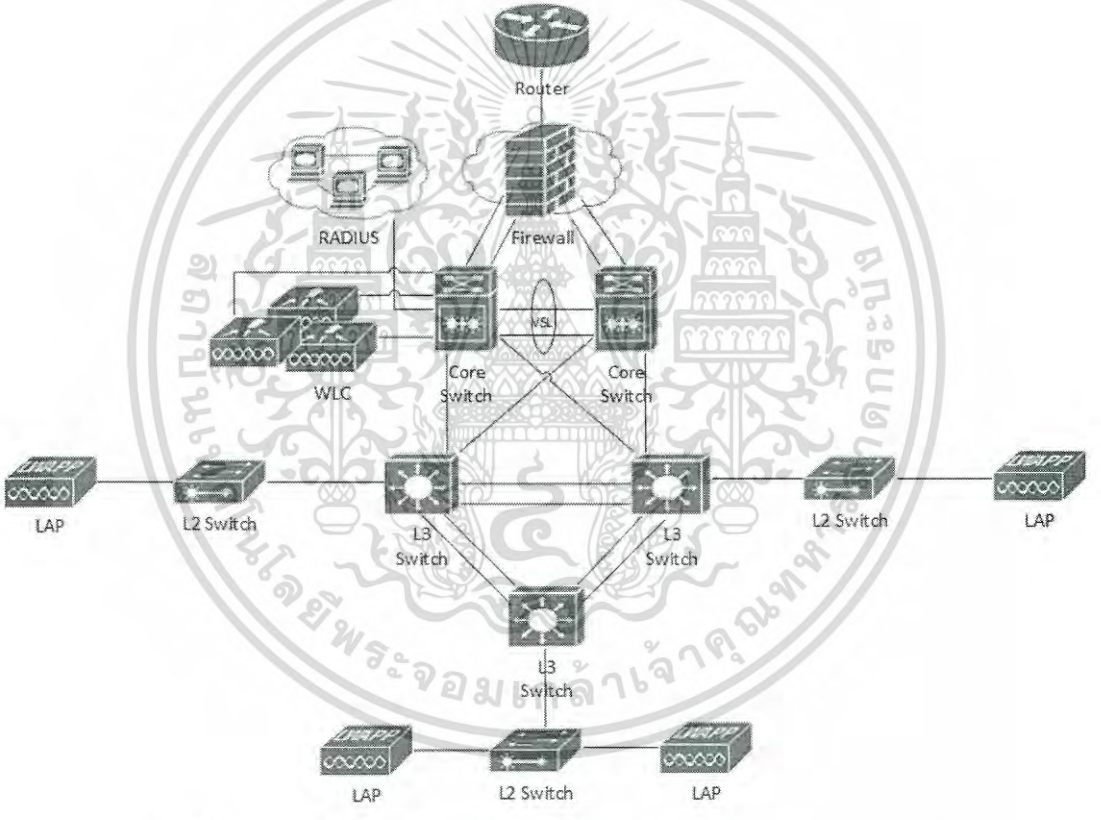
รูปที่ 3.14 ตัวอย่างแสดงผลลัพธ์ของโปรแกรม AIRMAGNET

จากผลการสำรวจที่ได้จากโปรแกรม AIRMAGNET สามารถนำไปวิเคราะห์ อัตราการครอบคลุมของสัญญาณ Wireless LAN เพื่อทำการพิจารณาเพิ่มอุปกรณ์ Lightweight access point (LAP) หรือโยกย้ายอุปกรณ์ เพื่อให้ได้สัญญาณการครอบคลุมที่ดีขึ้น โดยทั้งนี้ขึ้นอยู่กับข้อจำกัดและเงื่อนไขต่างๆของผู้ว่าจ้าง

3.3 สรุปผล

การวางระบบเครือข่ายไร้สายโดยใช้ Cisco Lightweight Access Point (Cisco LAP) รุ่น 2702I จำนวน 90 ตัว ร่วมกับ Wireless LAN Controller (WLC) รุ่น 5508 จำนวน 1 ตัว ใช้ติดตั้งทั้งหมด 33 อาคาร เสร็จสิ้นพร้อมทำรายงานความครอบคลุมของสัญญาณไร้สาย ส่งมอบให้กับผู้ว่าจ้าง

3.4 การประยุกต์หลักการออกแบบ



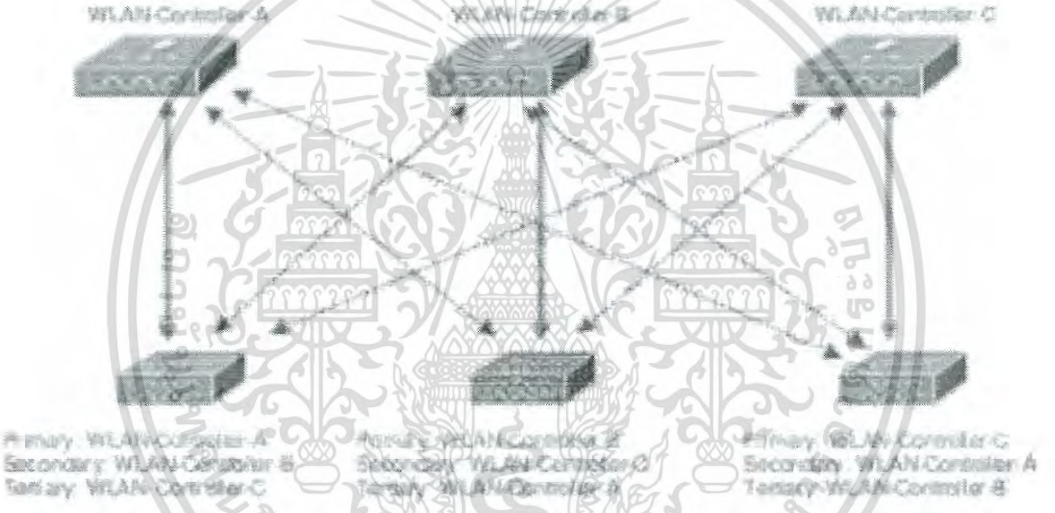
รูปที่ 3.15 แผนผังการเชื่อมต่ออุปกรณ์โดยประยุกต์หลักการออกแบบ

จากการออกแบบที่ได้เสนอให้กับลูกค้าเป็นการออกแบบที่ดีที่สุดภายใต้ข้อจำกัดต่างๆ ที่ลูกค้าและสถานที่มี อาทิเช่น ข้อจำกัดด้านงบประมาณ, สภาพแวดล้อม และ วัสดุพื้นผิวที่ติดตั้ง

ดังนั้นในการประยุกต์การออกแบบนี้จะออกแบบโดยตัดองค์กอบที่เป็นอุปสรรค์ออก เพื่อให้ได้ระบบที่ดียิ่งขึ้น โดยในที่นี้จะเพิ่มศักยภาพหลายๆด้าน เช่น Availability, Resilience และ Reliability

จากแผนผังการออกแบบประยุกต์ ได้มีการเพิ่มอุปกรณ์เพื่อความ Redundancy ของระบบ เช่น WLC, RADUIS cluster, Firewall cluster, Core switch อีกทั้งมีการใช้ VSS เพื่อเพิ่มประสิทธิภาพของเครือข่าย และใช้ L2 Switch PoE เพื่อจ่ายไฟให้กับตัวอุปกรณ์ Access point เพื่อง่ายต่อการจัดการดูแลระบบ

3.3.1 วิธีที่ดีที่สุดในการเชื่อมต่อ Access point กับ Controller



รูปที่ 3.16 แสดงตัวอย่างการเชื่อมต่อแบบ Best practice

จาก Best practice ที่ซิสโก้แนะนำ สามารถนำไปประยุกต์ เพื่อดำเนินการปรับปรุงโครงสร้างการเชื่อมต่อของสถาบันการศึกษาได้ โดยจะมีการเพิ่มอุปกรณ์ WLCs และตั้งค่าอุปกรณ์ LAPs ให้แต่ละตัวมี Primary WLAN Controller ที่แตกต่างกัน เพื่อให้อุปกรณ์ LAPs ลงทะเบียนกับ WLC ที่ต่างกัน ซึ่งเป็นการกระจายโหลดการทำงานของอุปกรณ์ LAPs ออกจากกัน โดยมีการเปรียบเทียบการใช้วิธีการดังกล่าวดังนี้

ข้อดี

1. ง่ายต่อการดูแลและจัดการอุปกรณ์
2. มีความยืดหยุ่นและมีประสิทธิภาพในการออกแบบให้เกิด Redundancy

3. สามารถทำการ Failback ได้หากเกิดข้อผิดพลาด (Failover)

ข้อเสีย

1. ต้องเตรียมพร้อมในการวางแผนและตั้งค่ามากขึ้น

ทั้งนี้วิธีที่ซิสโก้แนะนำจะต้องใช้งบประมาณ และการดำเนินการเปลี่ยนการตั้งค่าในอุปกรณ์ LAPs แต่ละอุปกรณ์ซึ่งกระจายอยู่ในหลายอาคาร ทำให้การปฏิบัติงานจริง ดำเนินการได้ค่อนข้างได้ค่อนข้างยาก

อีกแนวทางหนึ่ง คือการใช้ High Availability (HA) โดยใช้อุปกรณ์ WLC จำนวน 2 เครื่อง และเชื่อมต่อกันผ่านพอร์ต Redundancy Port (RP) โดยใช้สาย UTP

ในการใช้งาน เมื่อเชื่อมต่อ และตั้งค่าพอร์ต RP อุปกรณ์ WLC ทั้ง 2 เครื่องจะรีบูตตัวเอง และเมื่อเริ่มต้นทำงานอุปกรณ์จะเลือกหน้าที่ของเครื่อง โดยจะต่อรองว่าเครื่องใดจะมีหน้าที่เป็น Active และอีกเครื่องจะมีหน้าที่เป็น Standby-Hot ในการเชื่อมต่อพอร์ต RP จะมีการส่งข้อความ Keep-alive ผ่าน UDP เพื่อตรวจสอบการทำงานของอุปกรณ์ โดยจะส่งข้อความ Keep-alive ทุกๆ 100 มิลลิวินาที จากเครื่องที่มีหน้าที่เป็น Standby-Hot ส่งข้อความ Keep-alive ไปหาเครื่องที่ทำหน้าที่เป็น Active ถ้าข้อความ Keep-alive ที่ส่งล้มเหลว พอร์ต RP จะถูกใช้เพื่อแจ้งอุปกรณ์ที่ ทำหน้าที่เป็น Standby-hot จากนั้นจะมีการสลับหน้าที่ให้อุปกรณ์ที่เป็น Standby-Hot ขึ้นมาทำหน้าที่เป็น Active แทน

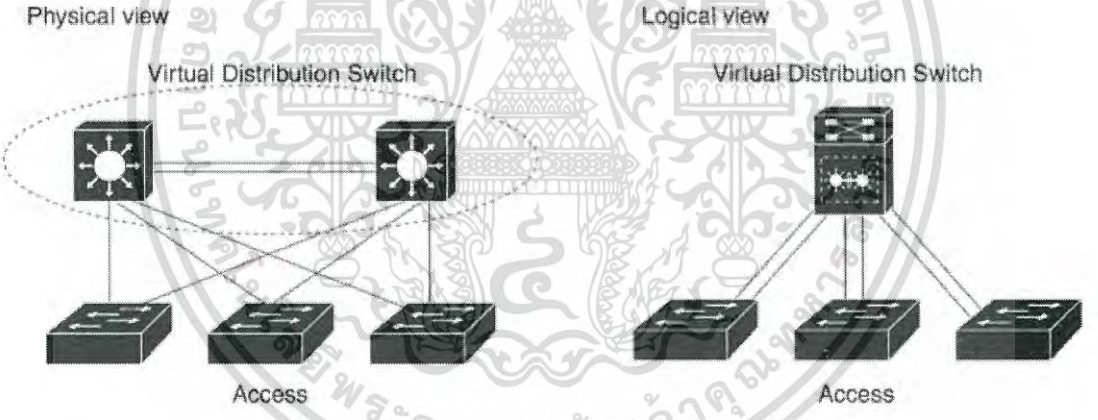
ในขณะที่เกิด Stateful switchover of access points (AP SSO) อุปกรณ์ LAPs ทั้งหมดเซสชันที่เป็น Stateful จะถูกสับเปลี่ยน และ Client ทั้งหมดจะถูกตัดการเชื่อมต่อ และเชื่อมต่อใหม่อีกครั้ง เข้ากับ WLC เครื่องใหม่ที่ทำหน้าที่เป็น Active ยกเว้น Clients ในพื้นที่ที่ถูกสับเปลี่ยนแล้วในโหมด FlexConnect

บทที่ 4
วิธีการดำเนินงานในเครือข่ายหลักของลูกค้ารายที่สอง

4.1 วิเคราะห์งานที่ได้รับมอบหมาย

ลูกค้ารายที่สองได้ทำการว่าจ้างบริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด ให้ติดตั้งอุปกรณ์ที่ใช้เชื่อมกับเครือข่ายหลัก (Core switch) โดยการติดตั้งจะเป็นโรงงาน 3 แห่งของทางลูกค้า เนื่องจากอุปกรณ์ที่มีอยู่เดิมมีสภาพเก่าและหมดอายุการใช้งาน อีกทั้งอุปกรณ์แยกกันทำงาน (Standalone) ทำให้มีประสิทธิภาพที่ต่ำ

ดังนั้นจึงจำเป็นต้องเปลี่ยนอุปกรณ์ใหม่ เพื่อปรับปรุงประสิทธิภาพของเครือข่าย ซึ่งแนวคิดและการเชื่อมต่อที่ใช้งานจริงจะเป็นดังรูป

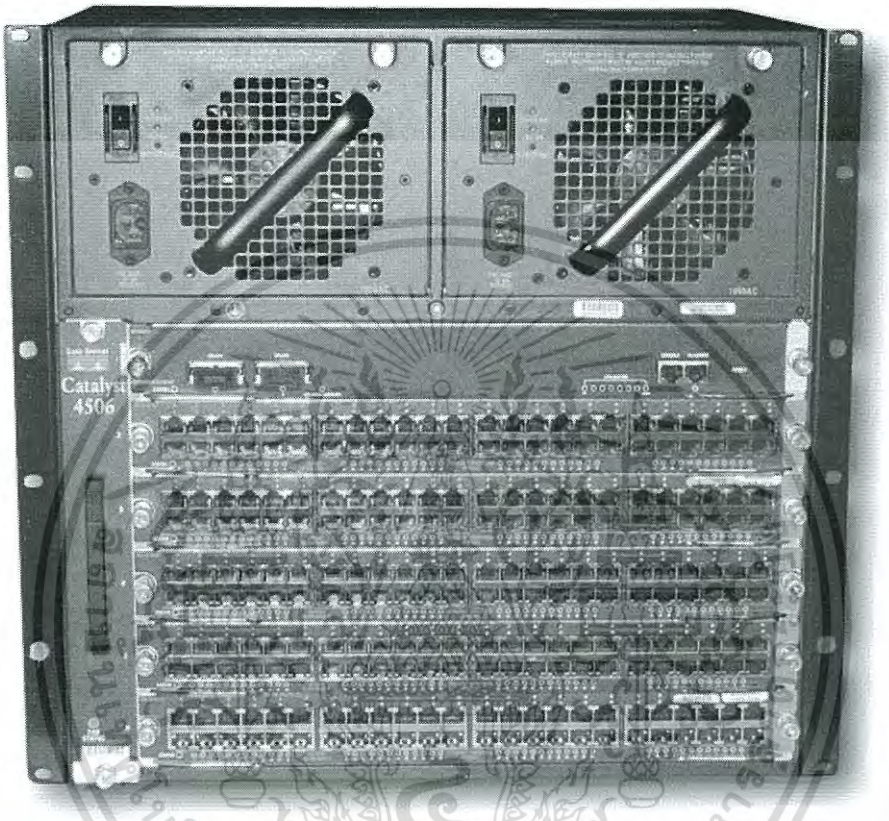


รูปที่ 4.1 แสดงแนวคิด VSS ที่ใช้งาน

4.1.1 อุปกรณ์ที่ใช้ในการติดตั้ง

a) Cisco Catalyst WS-C4506-E

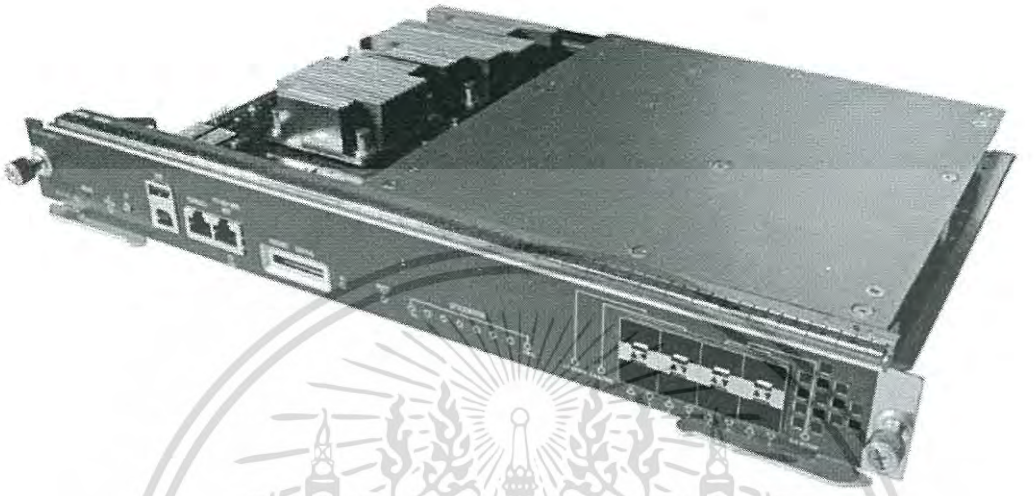
ใช้เป็นอุปกรณ์เชื่อมต่อกับเครือข่ายหลัก



รูปที่ 4.2 Cisco Catalyst WS-C4506-E

b) Cisco WS-X45-SUP8-E

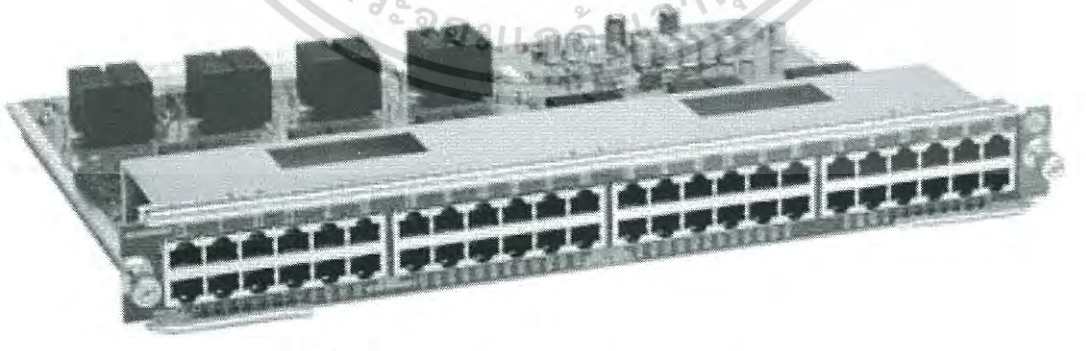
เป็น Supervisor card ใช้ควบคุมการทำงานของตัวอุปกรณ์



รูปที่ 4.3 Cisco WS-X45-SUP8-E Supervisor card

c) Cisco WS-X4748-RJ45-E

เป็น Line card เพื่อเพิ่มฟังก์ชั่นการทำงานให้กับอุปกรณ์



รูปที่ 4.4 Cisco WS-X4748-RJ45-E Line card

d) Cisco WS-X4712-SFP-E

เป็น Line card เพื่อเพิ่มฟังก์ชั่นการทำงานให้กับอุปกรณ์

รูปที่ 4.5 Cisco WS-X4712-SFP-E Line card

4.2 การปฏิบัติงาน

4.2.1 การเตรียมพร้อมอุปกรณ์

ก่อนการนำอุปกรณ์ไปติดตั้งจะต้องมีการทดสอบและเตรียมความพร้อมของอุปกรณ์ (Staging) เพื่อตรวจสอบสภาพและคุณภาพของสินค้า

โดยวิธีการในการตรวจสอบเริ่มจากเปิดอุปกรณ์ให้ทำงาน เพื่อดูว่าระบบเริ่มทำงานถูกต้องหรือไม่ จากนั้นทดสอบการใช้งาน โดยการจำลองการตั้งค่าจากงานที่ได้รับ ซึ่งงานที่ได้รับจะใช้เทคโนโลยี Virtual Switch System (VSS) โดยมีข้อจำกัดว่าทั้ง 2 เครื่องจะต้องมีการ์ด Supervisor ที่มีเวอร์ชันตรงกัน และเวอร์ชันของการ์ด Supervisor engine 7-E, 7+E ขึ้นไป ส่วนเครื่องที่นำมาใช้งาน ทั้งสองเครื่องเป็นการ์ด Supervisor เวอร์ชัน 8 รวมถึงเวอร์ชัน IOS ต้องตรงกัน

ในที่นี้จะเป็นการตั้งค่า Virtual Switch Link (VSL) และ Dual-Active with fast-hello message หลังจากที่ทดสอบการตั้งค่าอุปกรณ์เสร็จแล้ว จะต้องเปิดเครื่องให้ทำงานไว้ระยะหนึ่ง เพื่อให้มั่นใจว่าอุปกรณ์จะไม่เสียหายเมื่อนำไปใช้งานในสภาพแวดล้อมจริง

4.2.2 การติดตั้งอุปกรณ์

หลังจากที่เราได้ทดสอบและเตรียมความพร้อมของอุปกรณ์เรียบร้อยแล้ว เราจึงนำอุปกรณ์ไปติดตั้งให้กับลูกค้า โดยจะต้องโอนย้ายการการเชื่อมต่อ รวมไปถึงการตั้งค่า ไม่ว่าจะเป็นเส้นทางการส่งข้อมูล, การควบคุมสิทธิ์ต่างๆในการส่งข้อมูลผ่านอุปกรณ์ และการตั้งค่าสำหรับใช้ในการดูแลตรวจสอบอุปกรณ์ เป็นต้น

โดยการโอนย้ายระบบเครือข่ายและอุปกรณ์จะมีการหยุดทำงานของเครือข่ายเก่า (downtime) เพื่อเปลี่ยนจากอุปกรณ์เก่าไปเป็นอุปกรณ์ใหม่ เนื่องจากจะต้องโยกย้ายถึงระดับกายภาพ จึงทำให้เกิดช่วงเวลาที่เครือข่ายไม่สามารถใช้งานได้ ในระยะเวลาหนึ่ง

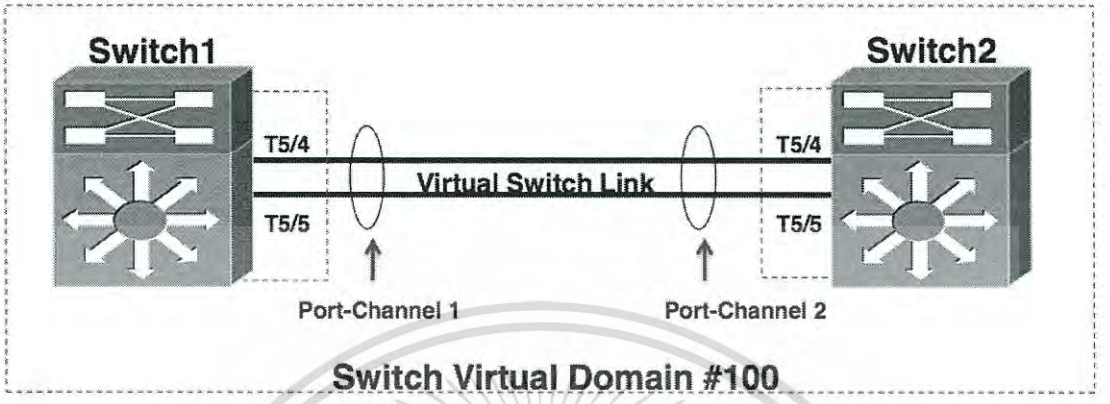
4.2.3 การตั้งค่าอุปกรณ์

สำหรับการตั้งค่าอุปกรณ์ โดยมี Cisco Catalyst WS-C4506-E จำนวน 2 เครื่อง ซึ่งปกติแล้วอุปกรณ์ทั้งสองตัวจะอยู่ในโหมดที่เรียกว่า Standalone เราจึงต้องทำให้อุปกรณ์ทั้งสองแปลงเป็นโหมดเสมือน (virtual) เพื่อให้ทั้งสองอุปกรณ์ร่วม VSS เดียวกัน โดยมีกระบวนการดังรูป

รูปที่ 4.6 แสดงกระบวนการแปลงโหมดจาก Standalone เป็น Virtual

ในการอธิบายจะสมมติการเชื่อมต่อโดยใช้สาย Twin ax จำนวน 2 เส้น เชื่อมต่อจากอุปกรณ์ตัวที่หนึ่ง พอร์ต T5/4 และ T5/5 ไปยังอุปกรณ์ตัวที่สอง พอร์ต T5/4 และ T5/5 โดยในฝั่งของอุปกรณ์ตัวที่หนึ่งทำการรวมพอร์ต T5/4 และ T5/5 เป็น Port-Channel หมายเลข 1 และอุปกรณ์ตัวที่สองทำการรวม พอร์ต T5/4 และ T5/5 เป็น Port-Channel หมายเลข 2 และในการทำ

VSS จะต้องตั้งค่าให้กับอุปกรณ์ทั้งสองอยู่ใน Virtual Domain หมายเลขเดียวกัน ในที่นี้จะสมมติให้เป็น Virtual Domain หมายเลข 100 ดังรูปต่อไปนี้



รูปที่ 4.7 แสดงแบบจำลองการเชื่อมต่อ

จากรูปที่ 4.7 การตั้งค่าอุปกรณ์ที่ 1 เพื่อเตรียมอุปกรณ์ให้ทำงานเป็น VSS มีดังนี้

```
Router(config)#hostname VSS
VSS(config)#switch virtual domain 100

Domain ID 100 config will take effect only after the
exec command 'switch convert mode virtual' is issued

VSS(config-vs-domain)#switch 1 priority 100
VSS(config-vs-domain)#exit

VSS(config)#interface port-channel 1
VSS(config-if)#no switchport
VSS(config-if)#switch virtual link 1

VSS(config-if)#interface range tenG 5/4 - 5
VSS(config-if-range)#channel-group 1 mode on

VSS(config-if-range)#int port-channel 1
VSS(config-if)#no shutdown
VSS(config-if)#end
```

จากรูปที่ 4.7 การตั้งค่าอุปกรณ์ที่ 2 เพื่อเตรียมอุปกรณ์ให้ทำงานเป็น VSS มีดังนี้

```
Router(config)#hostname VSS
VSS(config)#switch virtual domain 100

Domain ID 100 config will take effect only after the
exec command 'switch convert mode virtual' is issued

VSS(config-vs-domain)#switch 2 priority 90
VSS(config-vs-domain)#exit

VSS(config)#interface port-channel 2
VSS(config-if)#no switchport
VSS(config-if)#switch virtual link 2

VSS(config-if)#interface range tenG 5/4 - 5
VSS(config-if-range)#channel-group 2 mode on

VSS(config-if-range)#int port-channel 2
VSS(config-if)#no shutdown
VSS(config-if)#end
```

4.2.3.1 อธิบายการตั้งค่า VSL โดยใช้เทคโนโลยี VSS

- ตั้งค่า Virtual Domain ให้มีหมายเลข (ID) ที่ตรงกัน
- ตั้งค่าหมายเลขของอุปกรณ์ รวมถึงกำหนดความสำคัญของอุปกรณ์ ถ้าหากเลขความสำคัญมากสุด อุปกรณ์เครื่องนั้นจะเป็นเครื่องหลักในการทำงาน
- จากนั้นตั้งค่า Virtual link โดยขั้นตอนนี้จะเป็นการสร้าง Virtual Switch Link (VSL)
- ตั้งค่าให้พอร์ต tenG 5/4 ถึง tenG 5/5 ให้เป็น Port-channel เดียวกัน และใช้โหมด ON
- เปิดใช้งานพอร์ตด้วยคำสั่ง no shutdown

หลังจากที่ได้ตั้งค่าเบื้องต้นแล้ว จึงใช้คำสั่งดังต่อไปนี้เพื่อแปลงโหมดของอุปกรณ์จาก Standalone ไปเป็น Virtual (VSS) โดยใช้คำสั่ง “switch convert mode virtual”

จะมีข้อความแจ้งว่าถ้าหากเปลี่ยนโหมดแล้วชื่ออินเตอร์เฟซจะถูกเปลี่ยนโดยจะมีรูปแบบเป็น “หมายเลขอุปกรณ์/หมายเลขช่องการ์ด/หมายเลขพอร์ต” และมีข้อความถามว่าจะเซฟการตั้งค่าที่ได้ตั้งค่าไปก่อนหน้านี้และรีบูตเครื่องหรือไม่ ให้เราตอบ “yes” จากนั้นเครื่องจะรีบูต

```
vss#switch convert mode virtual

This command will convert all interface names to
naming convention "interface-type switch-
number/slot/port", save the running config to startup-
config and reload the switch.

Do you want to proceed? [yes/no]: yes
Converting interface names
Building configuration...
[OK]

Saving converted configuration to bootflash:
...
Destination filename [startup-
config.converted_vs-20071031-150039]?
```

ขณะที่เครื่องกำลังบูต สามารถสังเกตข้อความที่แสดงบน Console ได้ เพื่อยืนยันว่าทั้ง 2 เครื่องทำ VSS กันเรียบร้อยแล้ว โดยจะมีข้อความดังนี้

ข้อความที่แสดงจากอุปกรณ์ตัวที่ 1 ขณะบูตเป็นดังนี้

```
<...snip...>
System detected Virtual Switch configuration...

Interface TenGigabitEthernet 1/5/4 is member of
PortChannel 1

Interface TenGigabitEthernet 1/5/5 is member of
PortChannel 1

<...snip...>
00:00:26: %PFREDUN-6-ACTIVE: Initializing as ACTIVE
processor for this switch
Initializing as Virtual Switch ACTIVE processor

<...snip...>
00:01:19: %VSLP-5-RRP_ROLE_RESOLVED: Role resolved as
ACTIVE by VSLP

00:01:19: %VSL-5-VSL_CNTRL_LINK:  New VSL
Control Link  5/4
```

ข้อความที่แสดงจากอุปกรณ์ตัวที่ 2 ขณะบูตเป็นดังนี้

```
<...snip...>
System detected Virtual Switch configuration...

Interface TenGigabitEthernet 2/5/4 is member of
PortChannel 2

Interface TenGigabitEthernet 2/5/5 is member of
PortChannel 2

<...snip...>
00:00:26: %PFREDUN-6-ACTIVE: Initializing as ACTIVE
processor for this switch
Initializing as Virtual Switch STANDBY processor

<...snip...>
00:01:02: %VSLP-5-RRP_ROLE_RESOLVED: Role resolved as
STANDBY by VSLP

00:01:02: %VSL-5-VSL_CNTRL_LINK:  New VSL
Control Link  5/4
```

จากข้อความที่แสดงข้างต้นของอุปกรณ์ทั้งสอง เห็นได้ว่าอุปกรณ์ตัวแรกเริ่มต้นการทำงานของตัวเองเป็น Active และอุปกรณ์ตัวที่สองเริ่มต้นการทำงานของตัวเองเป็น Standby

นอกจากนี้ยังสามารถยืนยันและตรวจสอบการทำ VSS ได้ โดยสามารถใช้คำสั่งเพื่อดูการเชื่อมต่อของอุปกรณ์ทั้งสอง ดังนี้

```
vss#show switch virtual

Switch mode : Virtual Switch
Virtual switch domain number : 100
Local switch number : 1
Local switch operational role: Virtual Switch Active
Peer switch number : 2
Peer switch operational role : Virtual Switch Standby
vss#
```

นอกจากนี้สามารถสังเกตได้จากการต่อ Console กับอุปกรณ์เครื่องที่ 2 แล้วเมื่อพิมพ์คำสั่งใดๆ จะมีข้อความแจ้งว่า Standby console ถูกปิด ตัวอย่างดังนี้

```
vss-sdby>enable
Standby console disabled
vss-sdby>
```

โดยปกติแล้วการทำ Virtual Switch Link (VSL) โดยใช้เทคโนโลยี Virtual Switch System (VSS) เป็นการทำให้อุปกรณ์ 2 เครื่อง กลายเป็นเครื่องเดียวกัน ในมุมมองเชิงตรรกะ

ดังนั้นเมื่อเกิดการล้มเหลวของอุปกรณ์ใดอุปกรณ์หนึ่งจะทำให้ไม่สามารถใช้งานได้ ตัวอย่างเช่น อุปกรณ์ตัวที่ 1 ไม่สามารถใช้งานได้จะเกิดการสูญหายของข้อมูล เพราะว่าอุปกรณ์ตัวที่ 2 ยังมีสถานะของ Control plane เป็น Standby หมายความว่า เมื่อเกิดข้อผิดพลาดอุปกรณ์ไม่มีการทำกระบวนการกู้คืน (recovery)

เพราะฉะนั้นเราจะต้องตั้งค่าให้อุปกรณ์สามารถกู้คืนได้ ถ้าหากเกิดข้อผิดพลาด โดยจะสามารถทำได้ในรุ่นที่รองรับเท่านั้น เช่น Catalyst 6800, 6500 และฟีเจอร์ที่รองรับบน Catalyst 4500-E, 4500-X โดยจะเรียกเทคนิคนี้ว่า Dual-Active

4.2.3.2 การตั้งค่า Dual-Active

โดยหลักการของ Dual-Active จะเป็นการทำงานในลักษณะตรวจจับ และกู้คืนอุปกรณ์ ในที่นี้เราจะใช้วิธีการตรวจจับที่เรียกว่า Fast Hello ด้วยการทำ Dual-Active นี้จะทำให้เกิด High Availability (HA) ขึ้นในระบบ

ซึ่งมีข้อควรระวังขณะที่อยู่ในโหมด Dual-Active Recovery ห้ามเปลี่ยนการตั้งค่าใดๆ ถ้าหากเปลี่ยนการตั้งค่าบนอุปกรณ์ในโหมดนี้แล้ว ระบบจะไม่กู้คืนให้ VSL กลับมาใช้งานได้อีกครั้ง เนื่องมาจากการตั้งค่าของทั้ง 2 อุปกรณ์ไม่ตรงกัน

เนื่องจากปกติ Dual-Active จะใช้ SSO เพื่อทำให้การตั้งค่าของทั้งสองอุปกรณ์ตรงกัน ถ้าหากมีการตั้งค่าขณะที่ SSO ไม่ทำงานหรือคือกำลังอยู่ในโหมด Recovery จะทำให้ VSL ไม่สามารถกลับมาใช้งานได้

ทางออกเดียวคือต้องใช้คำสั่ง “write memory” แล้วรีบูตอุปกรณ์ที่อยู่ในโหมด Recovery โดยใช้คำสั่ง “reload shelf”

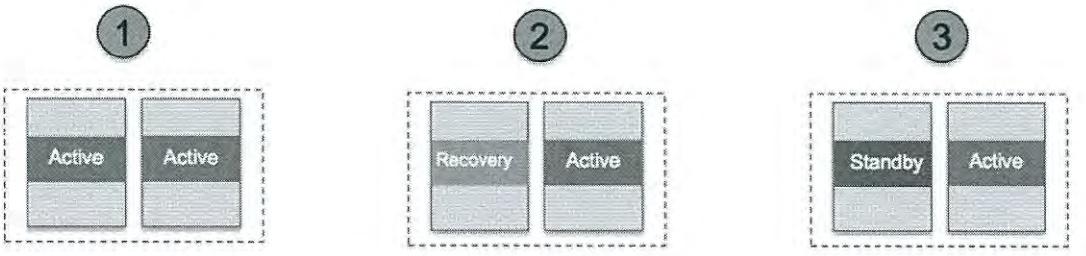
การตั้งค่า Dual-Active ให้กับอุปกรณ์มีดังนี้

```
switch virtual domain 100
dual-active recovery ip address {ip_address} {netmark}
dual-active detection fast-hello

interface GigabitEthernet1/2/3
 description "to VSS-SW2 gi2/2/3"
 no switchport
 no ip address
 dual-active fast-hello
!

interface GigabitEthernet2/2/3
 description "to VSS-SW1 gi1/2/3"
 no switchport
 no ip address
 dual-active fast-hello
!
```

และสามารถตรวจสอบความถูกต้องในการทำ Dual-Active ได้โดย

```
vss#show switch virtual dual-active fast-hello

Fast-hello dual-active detection enabled: Yes

Fast-hello dual-active interfaces:

Port      Local State  Peer Port  Remote State

-----------------------------------------------------

Gi1/2/3    Link up      Gi2/2/3    Link up
```

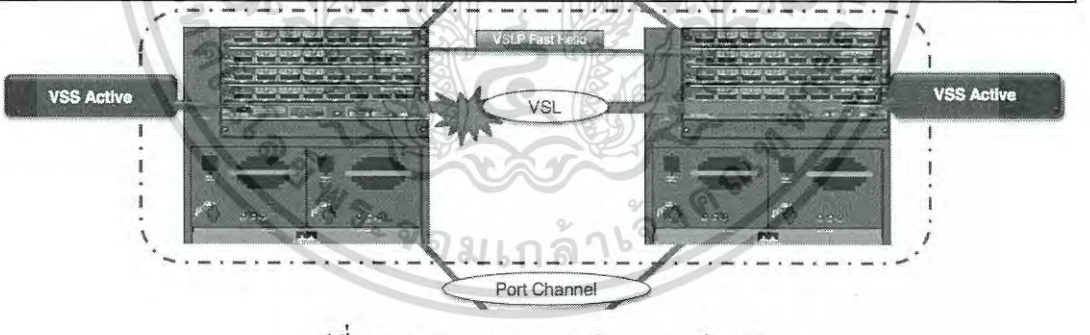
ซึ่งวิธีนี้จะมีลิงค์ระหว่างอุปกรณ์ทั้งสองเครื่อง เพื่อตรวจจับสัญญาณชีพจร (Heartbeat) ระหว่างเครื่อง โดยมีเฟสของกระบวนการตรวจจับและกู้คืนดังนี้



รูปที่ 4.8 ภาพรวมของการกู้คืนระบบ

a) เมื่อ Virtual Switch Link (VSL) เกิดความเสียหายหรือไม่สามารถเชื่อมต่อได้ อุปกรณ์จะแจ้งเตือนการตรวจจับและปิดทุกพอร์ตยกเว้นพอร์ตที่ถูกละเว้น

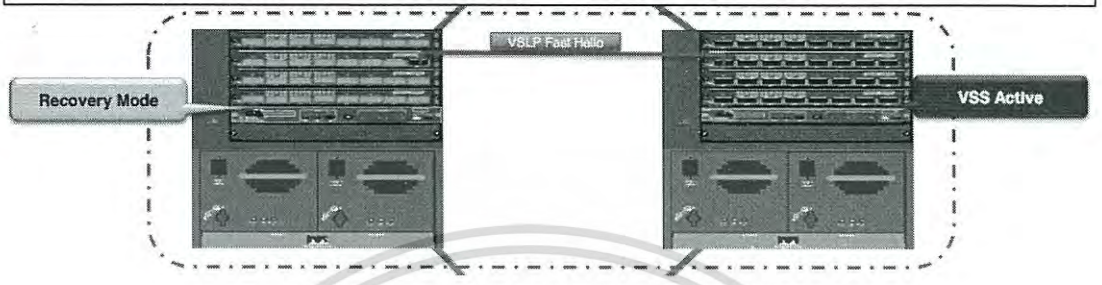
```
%DUAL_ACTIVE-SW1_SP-1-DETECTION: Dual-active condition
detected: all non- VSL and non-excluded interfaces
have been shut down
```



รูปที่ 4.9 ภาพแสดง VSL เกิดความเสียหาย

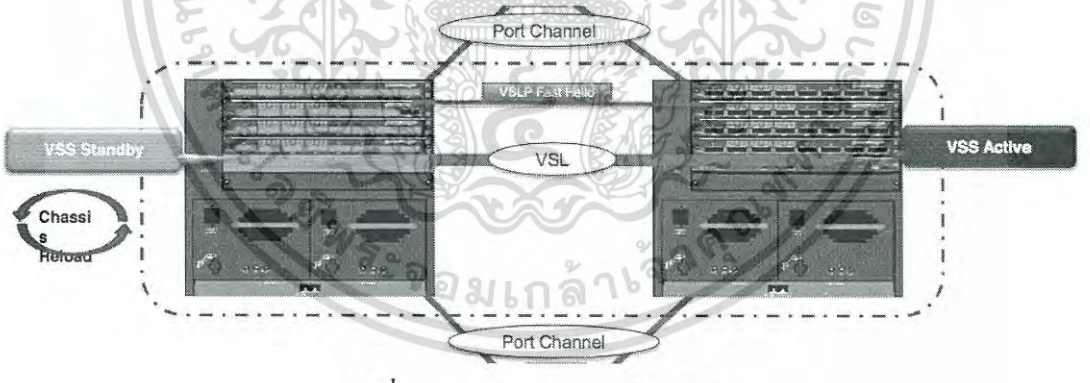
b) เฟสต่อมาหลังจากที่อุปกรณ์ทำการสั่งปิดพอร์ตทุกพอร์ตแล้ว มันจะพยายามที่จะกู้คืน VSL

```
%DUAL_ACTIVE-SW1_SP-1-DETECTION: Dual-active condition
detected: all non- VSL and non-excluded interfaces have
been shut down
```



รูปที่ 4.10 ภาพแสดงกระบวนการกู้คืน

c) เฟสสุดท้ายคือการกู้คืน เมื่อการรีบูตเสร็จสิ้นจะเห็นได้ว่า อุปกรณ์ที่เคยเป็น Standby จะเปลี่ยนเป็น Active และอุปกรณ์ที่กู้คืนสำเร็จจะกลายเป็น Standby



รูปที่ 4.11 ภาพแสดงการกู้คืนสำเร็จ

4.3 สรุปผล

อุปกรณ์ Cisco Catalyst WS-C4506-E ทั้งสองเครื่องที่นำมาใช้แทนเครื่องเดิม พร้อมเชื่อมต่อกันด้วย Virtual Switch Link (VSL) จากเทคโนโลยี Virtual Switch System (VSS) กันได้สำเร็จ

นอกจากนี้ยังมีคุณสมบัติ High Availability (HA) โดยการใช้ Dual-Active ด้วย Fast Hello message เพื่อทำให้สามารถเข้าถึงได้ตลอดเวลาแม้มีอุปกรณ์ใดอุปกรณ์หนึ่งเกิดข้อผิดพลาดหรือเสียหายขึ้น อีกทั้งยังสามารถใช้งานเครือข่ายได้อย่างมีประสิทธิภาพมากขึ้น เนื่องจากข้อมูลที่วิ่งจะกระจายผ่านอุปกรณ์ทั้งสองเครื่อง

บทที่ 5
ข้อเสนอแนะเกี่ยวกับสหกิจศึกษา

สำหรับการปฏิบัติงานสหกิจศึกษาที่บริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด ซึ่งเป็นบริษัท System Integrated (SI) กล่าวคือเป็นบริษัทที่รับผิดชอบการสร้าง ดูแล และแก้ไขระบบต่างๆ จากคุณสมบัติข้อนี้ทำให้นักศึกษาที่ได้ร่วมปฏิบัติงาน มีประสบการณ์มากกว่าบริษัททั่วๆไป อีกทั้งได้สัมผัสอุปกรณ์ การทำงานจริง ที่ไม่มีภายในการเรียนการสอนปกติของคณะเทคโนโลยีสารสนเทศ อีกทั้งยังมีงานที่หลากหลาย ซึ่งเป็นการเปิดโอกาสให้กับนักศึกษาที่ได้ศึกษาโครงสร้าง รูปแบบการทำงาน การทำงานของระบบ

จากข้างต้นที่กล่าวไป การปฏิบัติงานกับบริษัทที่เป็น System Integrated ขอเสนอในการให้เวลากับนักศึกษาที่ปฏิบัติงาน เนื่องจากทางบริษัทมีงานจำนวนมาก และใช้เวลาในการทำงานมากกว่าบริษัทรูปแบบอื่น เพื่อให้นักศึกษาโฟกัสกับการเรียนรู้งาน ควรแยกเวลาในการทำเอกสารกับช่วงเวลาในการปฏิบัติงานออกจากกัน

รวมไปถึงการปฏิบัติงานที่ได้รับมอบหมายให้ปฏิบัติแต่ละงานในช่วงเวลาที่สั้นๆ ทำให้ยากต่อการศึกษา และทำความเข้าใจในงานนั้นๆ

บรรณานุกรม

[1] David Hucaby. **CCNA Wireless 640-722 Official Cert Guide.** Reading : Cisco Press

[2] Mark Ciampa, Ph.D. **CWNA Guide to Wireless LANs, Third Edition.** Reading : Course Technology

[3] Roland Salinas. **"Cisco Catalyst Virtual Switch System."** [Online].Available : https://www.ciscolive.com/online/connect. 2015.

[4] Cisco. **"Configuring Virtual Switching Systems."** [Online].Available : http://www.cisco.com/c/en/us/products/switches/catalyst-4500-series-switches/index.html. 2015.

[5] Cisco. **"Design, Deployment and Management of Unified WLAN."** [Online].Available : http://www.slideshare.net/CiscoCanada/cisco-plusdesigndeploymentandmgmntgirardandlloyd. 2012.

[6] Cisco. **"Understanding and Configuring VLANs."** [Online].Available : http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html. 2015.

[7] Cisco. **"Configuring DHCP."** [Online].Available : http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfdhcp.html. 2015

[8] Cisco. **"DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example."** [Online].Available : http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html. 2015.

[9] Cisco. **"Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC)."** [Online].Available : http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70333-lap-registration.html. 2015

[10] Cisco. **"Cisco Wireless LAN Controller Configuration Guide, Release 7.4."** [Online].Available : http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED.html. 2015

ภาคผนวก

ภาคผนวก ก
ข้อมูลเกี่ยวกับสถานประกอบการ

แนะนำสถานประกอบการ

ชื่อและที่ตั้ง

บริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด (Dimension Data (Thailand) Co., Ltd)
ชั้น 16 คอลัมน์ทาวเวอร์ 199 ถนนรัชดาภิเษก
เขตคลองเตย กรุงเทพ 10110
โทรศัพท์ 0-2625-0999

ลักษณะการประกอบการ ผลิตภัณฑ์และบริการ

รายละเอียดบริษัท

บริษัทฯอันดับหนึ่งทางด้าน ICT Service and Solution Provider ที่มีเครือข่ายครอบคลุมในประเทศไทยและต่างประเทศ ยอดขายมากกว่า 1.7 แสนล้านบาททั่วโลก อยู่ในเครือ NTT Group ซึ่งใหญ่เป็นอันดับที่ 32 ของโลก ดำเนินงานด้านการวางระบบการสื่อสารข้อมูลคอมพิวเตอร์, งานออกแบบและสร้างข่ายสาย Fibre optic, LAN, ให้คำปรึกษา ออกแบบ ติดตั้ง ย้าย ระบบห้อง Data centre, ให้คำปรึกษา ออกแบบ ติดตั้ง และทดสอบระบบรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์, งานออกแบบติดตั้งระบบโทรศัพท์ไอพี, งานระบบสื่อสารทางไกลแบบเสมือนจริง, งานสำรองระบบข้อมูลคอมพิวเตอร์, ให้คำปรึกษา ออกแบบ ติดตั้งและดูแลระบบคอมพิวเตอร์แม่ข่าย และระบบปฏิบัติการ Microsoft, Exchange Server, VM ware, งานบริการทางด้าน outsource งานระบบ Cloud computing และงานอื่นๆที่เกี่ยวข้องกับระบบ IT ของหน่วยงานภาครัฐ ธนาคาร โรงงานอุตสาหกรรม สถาบันการศึกษา โรงพยาบาล ท่าอากาศยาน บริษัทขนส่ง ธุรกิจน้ำมัน ผู้ผลิตรถยนต์ ผู้ให้บริการโทรศัพท์ และบริษัทเอกชนต่างๆในประเทศไทยและทั่วโลก ดำเนินงานในประเทศไทยมาแล้วกว่า 30 ปี มีอัตราการขยายตัวอย่างรวดเร็ว

วิสัยทัศน์

ไดเมนชั่น ดาต้า เชื่อมั่นในพลังของเทคโนโลยีที่จะเปลี่ยนองค์กรของคุณ ให้ได้สิ่งที่ทำงานได้ดีขึ้น และยกระดับธุรกิจของคุณขึ้นไปในอีกระดับ เราเป็นบริการไอซีทีและผู้ให้บริการโซลูชั่นที่ใช้ความเชี่ยวชาญด้านเทคโนโลยี เพื่อเร่งความทะเยอทะยานทางธุรกิจของลูกค้าของเรา

พันธกิจ

"Accelerate Your Ambition"

เร่งความใฝ่ฝันของคุณโดยการส่งมอบโซลูชั่นบริการไอซีทีที่เปิดใช้ ดำเนินการ และเปลี่ยนธุรกิจ

ความทะเยอทะยานของธุรกิจที่เราช่วยให้คุณบรรลุจุดมุ่งหมายทางธุรกิจ เช่น

- ลดค่าใช้จ่ายของคุณ
- ยั่งยืนมากขึ้น
- การปรับปรุงประสิทธิภาพของคุณ
- เพิ่มศักยภาพในการแข่งขันของคุณ
- ลดความเสี่ยงของคุณ
- ขยายรายได้ของคุณ
- ปรับปรุงประสบการณ์ของลูกค้าของคุณ

ธุรกิจของบริษัท

การบริการหรือสินค้าของบริษัท ได้แก่

- Systems integration services

  เรานำเสนอวงจรชีวิตของการบริการสำหรับเทคโนโลยีรวมไปถึง
  - ให้คำปรึกษาและบริการประเมิน
  - บริการระดับมืออาชีพ
  - บริการสนับสนุน (support)
  - บริการด้านการจัดการ
- IT outsourcing

  การเจริญเติบโตของธุรกิจไอทีเอาท์ซอร์สใช้บริการทั้งหมดของเรา และรวมไปถึง
  - อาคารเครือข่ายและการสื่อสาร
  - อาคารศูนย์ข้อมูล
  - อาคารศูนย์การติดต่อ
- IT-as-a-service

  ความสามารถของคลาวด์ที่มีประสิทธิภาพของเรารวมถึง
  - โซลูชั่นคลาวด์สาธารณะจากแพลตฟอร์มคลาวด์ที่มีการจัดการของเราเอง อยู่ในแปดประเทศทั่วโลก

- โซลูชั่นคลาวด์ส่วนตัว
- โซลูชั่นคลาวด์ไฮบริด

ตำแหน่งที่ได้รับมอบหมายให้รับผิดชอบ

ตำแหน่ง : วิศวกรเครือข่าย (Network Engineer)

ลักษณะงาน : ปฏิบัติงานตามที่ได้รับมอบหมายในแต่ละวัน โดยช่วยเหลือวิศวกรในการปฏิบัติงาน เช่น เตรียมพร้อมและตั้งค่าอุปกรณ์ สำรวจสถานที่ ติดตั้งอุปกรณ์ ตรวจสอบและแก้ไข

พนักงานที่ปรึกษา

ชื่อ : คุณอารียา จารุภูมิ

ตำแหน่ง : MS Resource Manager

ระยะเวลาปฏิบัติงาน

วันแรกของการปฏิบัติงาน : วันที่ 3 สิงหาคม 2558

วันสุดท้ายของการปฏิบัติงาน : วันที่ 30 พฤศจิกายน 2558

ช่วงเวลาปฏิบัติงาน : จันทร์ - ศุกร์ เวลา 8:00 น. – 17:00 น.

รวมระยะเวลา : 16 สัปดาห์

ภาคผนวก ข

ข้อมูลการปฏิบัติงานในช่วงสหกิจศึกษา

ข้อมูลการปฏิบัติงานในช่วงเวลาสหกิจศึกษา

วันที่ 3 สิงหาคม 2558

ทำความเข้าใจเกี่ยวกับภาพรวมของบริษัท, การทำงาน ระเบียบต่างๆ และลักษณะในการทำงาน

ทำการตรวจสอบสินค้าและเก็บรหัสอุปกรณ์เป็นขั้นแรกของการเตรียมสินค้าที่ Warehouse ของบริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด

วันที่ 4 สิงหาคม 2558

เข้าไซต์งาน Bank of Thailand เพื่อติดตั้งอุปกรณ์ Core Switch และ Core Router (Nexus 7k Series)

วันที่ 5 สิงหาคม 2558

เข้าไซต์งาน Bumrungrad ตรวจสอบและเก็บข้อมูลเกี่ยวกับอุปกรณ์เน็ตเวิร์ค เพื่อใช้กับระบบมอนิเตอร์ (Cisco Prime)

วันที่ 6 สิงหาคม 2558

เข้าไซต์งาน Bank of Thailand เพื่อติดตั้งอุปกรณ์ Core Switch และ Core Router (Nexus 7k Series)

วันที่ 7 สิงหาคม 2558

ทำการตรวจสอบสินค้าและเก็บรหัสอุปกรณ์ และเตรียมพร้อมอุปกรณ์ (Staging) ที่ Warehouse ของบริษัท

วันที่ 10 สิงหาคม 2558

เข้าไซต์งาน Bank of Thailand เพื่อ Staging อุปกรณ์ รวมไปถึงเก็บรายละเอียดของงานติดตั้ง

วันที่ 11 สิงหาคม 2558

ตรวจสอบ เตรียมความพร้อม และทดสอบการใช้งานของอุปกรณ์ (Staging) ที่ Warehouse ของบริษัท

วันที่ 13 สิงหาคม 2558

เข้าไซต์งานกรมการปกครอง (DOPA) เพื่อติดตั้งอุปกรณ์ Switch และปรับเปลี่ยนการตั้งค่าของอุปกรณ์

วันที่ 14 สิงหาคม 2558

เข้าไซต์งานโกดังของแมคโคร เพื่อติดตั้งอุปกรณ์ Switch และ Access point

วันที่ 17 - 18 สิงหาคม 2558

ตรวจสอบ เตรียมความพร้อมของอุปกรณ์ (Staging) ที่ Warehouse ของบริษัท

วันที่ 19 - 20 สิงหาคม 2558

ปฏิบัติงานช่วยเหลือกับทีมงาน Client Service Customer (Support) ในการทำแลปทดสอบอุปกรณ์ต่างๆที่บริษัท

วันที่ 24 - 25 สิงหาคม 2558

ตรวจสอบอุปกรณ์สำรองที่บริษัท

วันที่ 26 สิงหาคม 2558

เข้าไซต์งานที่โรงพยาบาลศิริราช ติดตั้งเซิร์ฟเวอร์และอุปกรณ์ Switch

วันที่ 27 สิงหาคม 2558

เข้าไซต์งานที่โรงพยาบาลศิริราช เพื่อเก็บรายละเอียดของงาน เช่น Cable wiring เป็นต้น

วันที่ 28 สิงหาคม 2558

เข้าไซต์งานที่ Bank of Thailand เพื่อตรวจสอบสาย UTP ที่ไม่ได้ใช้ และจัดระเบียบสาย UTP (Cable wiring)

วันที่ 31 สิงหาคม 2558

เข้าไซต์งานที่ Airports of Thailand (AOT) เพื่อตั้งค่าให้กับอุปกรณ์ Access Switch

วันที่ 1 กันยายน 2558

เข้าไซต์งานที่ Airports of Thailand (AOT) เพื่อตั้งค่าให้กับอุปกรณ์ Access Switch และติดตั้งอุปกรณ์ Access Switch ในตู้วางอุปกรณ์แต่ละชั้น

วันที่ 2, 4, 7 กันยายน 2558

เข้าไซต์งานที่ Airports of Thailand (AOT) เพื่อติดตั้งอุปกรณ์ Access Switch ในตู้วางอุปกรณ์แต่ละชั้น

วันที่ 8 – 9 กันยายน 2558

เข้าไซต์งานที่มหาวิทยาลัยมหิดล เพื่อเตรียมความพร้อม (Staging) อุปกรณ์ Access Point ที่ใช้ในการติดตั้งที่ไซต์โรงพยาบาลศิริราช

วันที่ 10 – 11, 14 – 19, 21 กันยายน 2558

เข้าไซต์งานที่ Airports of Thailand (AOT) ในสุวรรณภูมิ เพื่อติดตั้งอุปกรณ์ IP Phone รวมถึงตรวจสอบการทำงานของอุปกรณ์

วันที่ 22 กันยายน 2558

ช่วยเหลือวิศวกรในการจัดทำเอกสาร และเข้าไซต์งานที่ Bank of Thailand เพื่อจัดระเบียบสาย (Cable wiring)

วันที่ 23 – 24 กันยายน 2558

เข้าไซต์งานที่โรงพยาบาลศิริราช ปิยมหาราชการุณย์ (SiPH) เพื่อติดตั้ง เปลี่ยน และตั้งค่าอุปกรณ์ Access Point

วันที่ 25 กันยายน 2558

เตรียมความพร้อม (Staging) อุปกรณ์ Access Point และ Cisco Switch Nexus 2000 Series ที่ Warehouse ของบริษัท

วันที่ 28 กันยายน 2558

ช่วยเหลือวิศวกรเก็บข้อมูลของสินค้า

วันที่ 29 กันยายน 2558

เข้าไซต์งานที่มหาวิทยาลัยหอการค้าไทย (UTCC) เตรียมการเชื่อมต่อระหว่างอุปกรณ์ Core Switch โดยจัดสาย Fiber, Twin ax และ UTC ในการเชื่อมต่อต่างๆ

วันที่ 30 กันยายน 2558

เข้าไซต์งานที่คณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล เพื่อติดตั้งอุปกรณ์ Router ASR เพื่อเชื่อมต่อระหว่างไซต์ภายในมหาวิทยาลัยมหิดลทั้ง 3 สถานที่

วันที่ 2 ตุลาคม 2558

เข้าไซต์งานที่มหาวิทยาลัยหอการค้าไทย (UTCC) เตรียมการเชื่อมต่อระหว่างอุปกรณ์ Core Switch โดยจัดสาย Fiber, Twin ax และ UTC ในการเชื่อมต่อต่างๆ

วันที่ 5 ตุลาคม 2558

เข้าไซต์งานที่มหาวิทยาลัยหอการค้าไทย (UTCC) เพื่อตรวจสอบ และเปลี่ยนชื่ออุปกรณ์ Lightweight Access Point บน Wireless LAN Controller (WLC) รวมถึงเพิ่มคำอธิบายอินเตอร์เฟสบนอุปกรณ์ Switch

วันที่ 6 - 7 ตุลาคม 2558

จัดระเบียบ และจัดการเอกสารที่ Warehouse ของบริษัท

วันที่ 8 ตุลาคม 2558

เข้าไซต์งานที่มหาวิทยาลัยหอการค้าไทย (UTCC) เพื่อตั้งค่าอุปกรณ์ Distributed Switch และ Access Switch

เข้าไซต์งานที่มหาวิทยาลัยมหิดล (MU) เพื่อติดตั้ง Wireless LAN Controller 8500 (WLC) on Cisco UCS-E server modules, Cisco ASR Router และ Cisco Nexus Switch

วันที่ 9, 12 – 13, 15 – 16 ตุลาคม 2558

เข้าไซต์งานที่ TRUE ตึก Thai Summit เพื่อตรวจจับ (monitor) อุปกรณ์ F5 หลังจากการโยกย้ายระบบ เพื่อตรวจสอบความเสถียรของระบบเครือข่าย พร้อมจัดทำรายงานสรุปผล

วันที่ 19 – 21 ตุลาคม 2558

เข้าไซต์งานที่ธนาคารทหารไทย จำกัด (TMB) ตึก AIA เพื่อสนับสนุนผู้ใช้งาน (Agent) ในการใช้งานโปรแกรม Cisco Finesse ซึ่งเป็น Next-Generation Collaborative Customer Care ของบริษัทธนาคารทหารไทย ร่วมกับ CUCM โดยตัวโปรแกรมมีการเชื่อมต่อกับ 3rd Software อีกด้วย อาทิเช่น LCM จากบริษัท Acqueon และ NICE จากบริษัท NICE Systems

วันที่ 22, 26 - 27 ตุลาคม 2558

ตรวจสอบ เตรียมความพร้อมของอุปกรณ์ (Staging) ที่ Warehouse ของบริษัท

วันที่ 28 ตุลาคม 2558

ตรวจสอบ เตรียมความพร้อมของอุปกรณ์ Access Point ที่ Warehouse ของบริษัท และเข้าร่วมอบรมการใช้งาน Cisco Finesse และระบบที่เกี่ยวข้อง เพื่อใช้สนับสนุน Agent ของ TMB ที่สำนักงานใหญ่ของบริษัท ธนาคารทหารไทย จำกัด

วันที่ 29 - 30 ตุลาคม 2558

เข้าไซต์งานที่โรงพยาบาลศิริราช เพื่อติดตั้งอุปกรณ์ Access Point

วันที่ 2 – 6, 9 พฤศจิกายน 2558

เข้าไซต์งานที่ธนาคารทหารไทย จำกัด (TMB) ตึก AIA เพื่อสนับสนุนผู้ใช้งาน (Agent) ในการใช้งานโปรแกรม Cisco Finesse ซึ่งเป็นส่วนหนึ่งของระบบ Cisco Unified Contact Center Enterprise (CCE)

วันที่ 10 - 12 พฤศจิกายน 2558

ตรวจสอบ เตรียมความพร้อมของอุปกรณ์ (Staging) ที่ Warehouse ของบริษัท

วันที่ 13 พฤศจิกายน 2558

เข้าไซต์งานที่ Bualuang Securities เพื่อตรวจจับ (monitor) หลังจากเปลี่ยนอุปกรณ์เครือข่าย ตรวจสอบ และตั้งค่าอุปกรณ์ Cisco Switch 4500 series ที่ Warehouse ของบริษัท

วันที่ 16 พฤศจิกายน 2558

เข้าไซต์งานที่โรงพยาบาลศิริราช เพื่อเปลี่ยนอุปกรณ์ Access Point และ Power Injector

วันที่ 18 พฤศจิกายน 2558

เข้าไซต์งานที่สำนักงานกสิกร ที่แจ้งวัฒนะ เพื่อสำรวจไซต์ในการติดตั้งอุปกรณ์ Core Switch และ Access Switch

วันที่ 19 – 20, 23 – 24 พฤศจิกายน 2558

เข้าไซต์งานที่ TRUE ตึก Thai Summit เพื่อตรวจจับ (monitor) อุปกรณ์ F5 หลังจากการโยกย้ายระบบ เพื่อตรวจสอบความเสถียรของระบบเครือข่าย หลังจากย้ายการไหลของข้อมูลผ่านอุปกรณ์ F5 ประมาณ 30 เปอร์เซ็นต์

วันที่ 25 พฤศจิกายน 2558

เข้าไซต์งานที่ Bualuang Securities เพื่อตรวจจับ (monitor) หลังจากเปลี่ยนอุปกรณ์เครือข่าย

เข้าไซต์งานที่โรงพยาบาลศิริราช เพื่อติดตั้งอุปกรณ์ Cisco Switch C4500 และ Switch C3850

วันที่ 26 – 27 พฤศจิกายน 2558

เข้าไซต์งานที่ TRUE ตึก Thai Summit เพื่อตรวจจับ (monitor) อุปกรณ์ F5 หลังจากการโยกย้ายระบบ เพื่อตรวจสอบความเสถียรของระบบเครือข่าย หลังจากย้ายการไหลของข้อมูลทั้งหมดผ่านอุปกรณ์ F5

วันที่ 30 พฤศจิกายน 2558

เข้าไซต์งานที่ธนาคารทหารไทย จำกัด (TMB) ตึก AIA เพื่อสนับสนุนผู้ใช้งาน (Agent) ในการใช้งานโปรแกรม Cisco Finesse ซึ่งเป็นส่วนหนึ่งของระบบ Cisco Unified Contact Center Enterprise (CCE)

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายธีรวัจน์ นำศรีเจริญสุข
วัน เดือน ปีเกิด	24 ตุลาคม 2536
สถานที่เกิด	กรุงเทพมหานคร
ที่อยู่	46 ถ.สุวินทวงศ์ ต.หน้าเมือง อ.เมือง จ.ฉะเชิงเทรา 24000
โทรศัพท์	08-0560-1102
ประวัติการศึกษา	พ.ศ. 2558 วิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

การพัฒนาระบบเครือข่ายไร้สายและการเพิ่มความพร้อมในการให้บริการในเครือข่ายหลัก

ธีรวัจน์ นำศรีเจริญสุข[1]

[1]คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

Emails: tengteerawat@gmal.com[1]

บทคัดย่อ

บริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด เป็นบริษัทให้บริการเกี่ยวกับระบบต่างๆ รวมถึงดำเนินการให้บรรลุตามความต้องการของลูกค้า อาทิเช่น ออกแบบ ติดตั้ง และแก้ไขปัญหาระบบเครือข่าย โดยในรายงานฉบับนี้จะกล่าวถึงระบบที่ทางบริษัทได้รับการว่าจ้างให้ดำเนินการพัฒนาระบบเครือข่ายให้กับลูกค้า 2 ราย เพื่อให้สามารถรองรับเทคโนโลยีใหม่ และเพิ่มประสิทธิภาพในการใช้งาน ความเสถียรและประสิทธิภาพของระบบให้มากขึ้น ทั้งนี้เพื่อให้สามารถดำเนินการปรับปรุงและพัฒนาระบบให้บรรลุตามความต้องการที่ได้รับมอบหมาย จึงได้ศึกษาความรู้ในทางทฤษฎีและปฏิบัติเกี่ยวกับเทคโนโลยีดังต่อไปนี้ Lightweight Access Point (LAP), Wireless Lightweight Controller (WLC), Virtual Local Area Network (VLAN), Dynamic Host Configuration Protocol (DHCP) และ Virtual Switching System (VSS)

คำสำคัญ – Lightweight Access Point (LAP); Wireless Lightweight Controller (WLC); Virtual Local Area Network (VLAN); Dynamic Host Configuration Protocol (DHCP); Virtual Switching System (VSS)

1. บทนำ

คณะเทคโนโลยีสารสนเทศได้ร่วมกับทางบริษัทจัดทำโครงการสหกิจศึกษา เพื่อศึกษาเทคโนโลยีระบบเครือข่ายและกระบวนการดำเนินงานในการทำงาน โดยมีระบบเครือข่ายหลัก (Core network) และเครือข่ายไร้สายเกี่ยวกับเทคโนโลยีทางด้านเครือข่ายต่างๆ อาทิเช่น Virtual Switching System (VSS), Lightweight access point (LAP) และ Wireless lightweight controller (WLC) โดยนำไปใช้พัฒนาและปรับปรุงระบบเครือข่ายขององค์กร ให้ใช้งานได้ตามความต้องการของลูกค้า ส่งผลให้มีประสิทธิภาพ ความพร้อมใช้งาน ความน่าเชื่อถือของและได้ประโยชน์จากระบบเครือข่ายสูงสุด

2. ขั้นตอนการพัฒนาโครงการ

ดำเนินการศึกษาระบบเครือข่ายและเทคโนโลยีที่ทางบริษัทใช้งาน ซึ่งนำไปใช้ประกอบการวิเคราะห์ ออกแบบ และติดตั้งระบบเครือข่ายตามที่ออกแบบไว้ ในการดำเนินงานขั้นสุดท้ายจึงมีการทดสอบระบบที่ได้ติดตั้งไปก่อนหน้านี้ ถ้าหากเกิดปัญหาจึงจะดำเนินการวิเคราะห์หาสาเหตุของปัญหาและดำเนินการแก้ไข นอกจากนี้ยังมีการเสนอแนะแนวทางการเพิ่มประสิทธิภาพให้กับระบบเครือข่ายโดยหวังว่าจะเกิดประโยชน์ไม่มากก็น้อยกับทางบริษัท และทำการสรุปผลการดำเนินงานที่ได้ดำเนินงานมาทั้งหมด

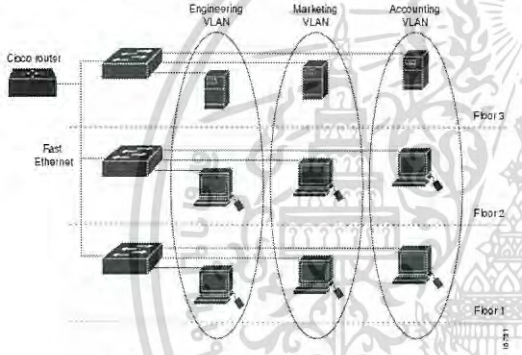
3. ทฤษฎีและเทคโนโลยีที่เกี่ยวข้อง

5.1. IEEE 802.11 Standards

IEEE 802.11 เป็นมาตรฐานที่กำหนดกลไกต่างๆที่อุปกรณ์สามารถนำไปใช้สื่อสารแบบไร้สายกับอุปกรณ์อื่นๆ โดยที่ข้อกำหนดสำคัญต่างๆ เช่น การสัญญาณวิทยุ, การมอดูเลต, การเข้ารหัส, ควบคุมขนาดและความถี่ของช่องสัญญาณ และอัตราการรับส่งข้อมูล โดยทฤษฎีที่เกี่ยวข้องในการดำเนินงานคือมาตรฐาน IEEE 802.11a/b/g/n โดยอธิบายวิธีการทำงาน เทคนิคที่ใช้ในแต่ละเทคโนโลยี

5.2. Virtual Local Network Area (VLAN)

เป็นการนำเทคโนโลยีเสมือน (Virtualization) มาใช้กับระบบเครือข่าย (LAN) ทำให้มีหลายเครือข่ายบนเครือข่ายหลักที่ใช้ร่วมกัน โดยเทคโนโลยีนี้ทำงานบนชั้นที่ 2 ของ OSI model ซึ่งแต่ก่อนอุปกรณ์ทุกตัวจะเชื่อมต่อกันบนเครือข่ายเดียวกันทั้งหมด ส่งผลให้เกิด overhead จำนวนมากบนเครือข่ายจากการส่ง Broadcast สื่อสารกันจากตัวอุปกรณ์ ดังนั้นเพื่อลด overhead จึงนำ VLAN มาช่วยในการลดจำนวนของข้อมูล Broadcast บนเครือข่าย โดยการแบ่งอุปกรณ์ต่างๆบนเครือข่ายหลักออกเป็นเครือข่ายย่อย ทำให้ขนาดของเครือข่ายลดลง และส่งผลให้ Broadcast domain เล็กลงเช่นกัน เพราะข้อมูล Broadcast จะไม่ถูกส่งข้าม VLAN หรืออุปกรณ์ที่ทำงานบนชั้นที่ 3 โดยการสื่อสารข้าม VLAN ของแต่ละกลุ่มอุปกรณ์สามารถทำได้โดยใช้อุปกรณ์ชั้นที่ 3 อาทิเช่น Router เพื่อให้ข้อมูลที่อยู่ต่าง VLAN กันสามารถสื่อการกันได้



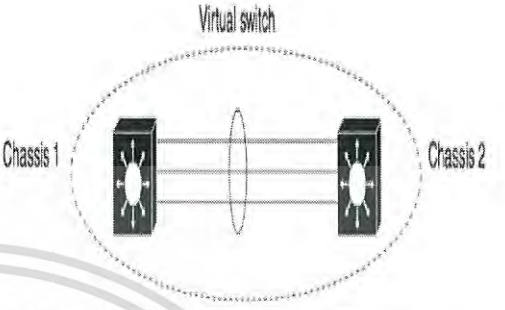
รูปที่ .1แสดงตัวอย่างการใช้งาน VLANs

5.3. Dynamic Host Configuration Protocol (DHCP)

DHCP เป็นโปรโตคอลให้บริการการกำหนดค่าที่ใช้ในระบบเครือข่ายให้กับอุปกรณ์ (Host) เช่น หมายเลข IP address, Subnet mask, Default gateway เป็นต้น โดยประกอบไปด้วย 2 องค์ประกอบ คือ โปรโตคอลสำหรับจัดสรรค่าของตัวแปรต่างๆจากเซิร์ฟเวอร์ส่งให้กับอุปกรณ์ และกลไกการจองที่อยู่บนเครือข่ายให้กับอุปกรณ์ โดย DHCP ถูกสร้างขึ้นบนรูปแบบการสื่อสารแบบ Client/Server โดยที่เซิร์ฟเวอร์ DHCP กำหนดและจัดสรรที่อยู่บนเครือข่าย และส่งการตั้งค่าต่างๆให้กับอุปกรณ์แบบพลวัต (Dynamic)

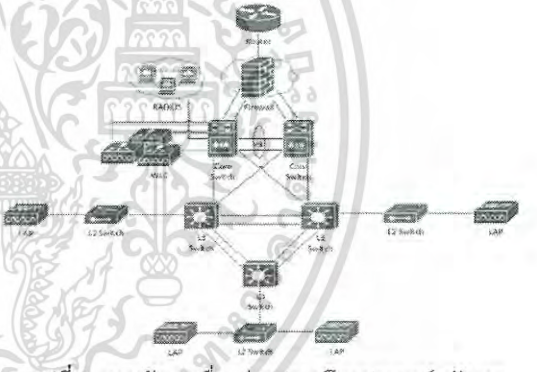
5.4. Virtual Switching Systems (VSS)

เป็นเทคโนโลยีหนึ่งของบริษัท Cisco โดยเป็นการดำเนินการทางเครือข่ายที่ทำให้มีความน่าเชื่อถือเพิ่มยิ่งขึ้น ผ่านการตั้งค่าอุปกรณ์ Switch และการเตรียมพร้อมลิงค์เพื่อเชื่อมต่อแบบคู่ซ้ำซ้อน (Redundant) โดยหลักการ VSS เป็นการรวมกันของคู่อุปกรณ์สวิทช์กลายเป็นองค์ประกอบเครือข่ายเดียว เรียกว่า การทำสวิทช์เสมือน (Virtual switching)



รูปที่ 2 .แสดงการเชื่อมต่อ Virtual Switch Link (VSL)

4. การประยุกต์หลักการออกแบบ



รูปที่ 3 .แผนผังการเชื่อมต่ออุปกรณ์โดยประยุกต์หลักการออกแบบ

ในส่วนนี้เป็นการนำความรู้ ประสบการณ์รวมไปถึงสิ่งที่ได้ศึกษามาจากการดำเนินงาน นำมาประยุกต์ใช้ในการออกแบบเพื่อเสริมให้ระบบเครือข่ายมีความเสถียร และมีประสิทธิภาพมากยิ่งขึ้น

การประยุกต์การออกแบบนี้เพื่อให้ได้ระบบที่ดียิ่งขึ้น โดยในที่นี้จะเพิ่มศักยภาพหลายๆด้าน อาทิเช่น Availability, Resilience และ Reliability อีกทั้งยังได้มีการเพิ่มอุปกรณ์เพื่อความ Redundancy ของระบบในแต่ละส่วน เช่น WLC, RADUIS cluster, Firewall cluster, Core switch อีกทั้งมีการใช้ VSS เพื่อเพิ่มประสิทธิภาพของเครือข่าย และใช้ L2 Switch PoE เพื่อจ่ายไฟให้กับตัวอุปกรณ์ Access point เพื่อง่ายต่อการจัดการดูแลระบบ

5. สรุปผลการดำเนินงาน

การดำเนินการออกแบบและติดตั้ง เพื่อปรับปรุงประสิทธิภาพของเครือข่ายเสร็จสิ้น โดยในส่วนของเครือข่ายไร้สายได้ติดตั้งและตั้งค่าให้ครอบคลุมกับพื้นที่การใช้งานและใช้งานให้ได้ประสิทธิภาพที่ดีที่สุด ส่วนการพัฒนาเครือข่ายหลักดำเนินการติดตั้งและตั้งค่าให้มีการใช้งานอุปกรณ์ทั้งสองเครื่องด้วยเทคโนโลยี Virtual Switching System (VSS) และตั้งค่าเพิ่มเติมในส่วนของ High Availability (HA) โดยการใช้ Dual-Active ด้วย Fast Hello message เพื่อทำให้สามารถเข้าถึงได้ตลอดเวลาแม้มีอุปกรณ์ใดอุปกรณ์หนึ่งเกิดข้อผิดพลาดหรือเสียหายขึ้น

6. กิตติกรรมประกาศ

การที่ข้าพเจ้าได้มาปฏิบัติงานสหกิจศึกษา ณ บริษัท ไดเมนชั่น ดาต้า จำกัด (ประเทศไทย) ในระหว่างวันที่ 3 สิงหาคม 2558 ส่งผลให้ข้าพเจ้าได้รับความรู้ ความเข้าใจ ทางด้านระบบเครือข่ายและความปลอดภัย นอกเหนือจากการเรียนรู้ภายในห้องเรียน รวมทั้งประสบการณ์ต่างๆ ที่ได้จากการทำงาน ซึ่งมีคุณค่าต่อการเรียนและการทำงานในภายภาคหน้า อีกทั้งข้าพเจ้ายังได้มีโอกาสนำความรู้จากการเรียนมาประยุกต์ใช้ในการปฏิบัติงานจริง ข้าพเจ้าใคร่ขอขอบพระคุณทุกท่าน ที่ได้ให้ความกรุณาชี้แนะ ให้คำแนะนำ คำปรึกษา ความช่วยเหลือในเรื่องต่างๆตลอดจนให้การดูแลและให้ความเข้าใจเกี่ยวกับชีวิตในการทำงานจริง

นอกจากนี้ ข้าพเจ้าจักขอบคุณ ที่ได้แนะนำโครงการสหกิจศึกษา ซึ่งเปิดโอกาสให้นักศึกษาได้รับประสบการณ์ที่ดีในอีกด้านหนึ่ง ขอขอบคุณเจ้าหน้าที่ คุณอารียา จารุภูมิ ที่ช่วยประสานงานในการปฏิบัติงานตามขั้นตอนสหกิจและขอขอบคุณ ผศ.ดร. ปานวิทย์ ธุวะนุติ ที่อำนวยความสะดวกในการจัดทำโครงงานเล่มนี้ ขอขอบคุณอาจารย์ที่ปรึกษา ดร. ลภัส ประดิษฐ์ทัศนีย์ ที่คอยช่วยเหลือและรับฟังปัญหาต่าง ๆ จนโครงงานเล่มนี้สำเร็จลุล่วงไปได้ด้วยดี

เอกสารอ้างอิง

[1] David Hucaby. CCNA Wireless 640-722 Official Cert Guide. Reading : Cisco Press

[2] Mark Ciampa, Ph.D. CWNA Guide to Wireless LANs, Third Edition. Reading : Course Technology

[3] Roland Salinas. “Cisco Catalyst Virtual Switch System.” [Online].Available : https://www.ciscolive.com/online/connect. 2015.

[4] Cisco. “Configuring Virtual Switching Systems.” [Online].Available : http://www.cisco.com/c/en/us/products/switches/catalyst-4500-series-switches/index.html. 2015. [5] Cisco. “Design, Deployment and Management of Unified WLAN.” [Online].Available : http://www.slideshare.net/CiscoCanada/cisco-plusdesigndeploymentandmgmntgirardandlloyd. 2012.

[6] Cisco. “Understanding and Configuring VLANs.” [Online].Available : http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html. 2015.

[7] Cisco. “Configuring DHCP.” [Online].Available : http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfdhcp.html. 2015

[8] Cisco. “DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example.” [Online].Available : http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html. 2015.

[9] Cisco. “Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).” [Online].Available : http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70333-lap-registration.html. 2015

[10] Cisco. "Cisco Wireless LAN Controller Configuration Guide, Release 7.4." [Online].Available : http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED.html. 2015