การศึกษาและออกแบบเครือข่ายการสื่อสารในระบบขนส่งทางราง

RAILWAY COMMUNICATION NETWORK STUDY AND DESIGN

วรวิช เดชบุญ

WORAWIT DETBOON

วิศุทธิ์ สุขจิตต์นิตยกาล

WISUT SUKCHITNITAYAKAN

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2557

การศึกษาและออกแบบเครือข่ายการสื่อสารในระบบขนส่งทางราง

RAILWAY COMMUNICATION NETWORK STUDY AND DESIGN

วรวิช เดชบุญ
WORAWIT DETBOON
วิศุทธิ์ สุขจิตต์นิตยกาล
WISUT SUKCHITNITAYAKAN

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
สาขาวิชาวิศวกรรมสารสนเทศ
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ.2557

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

RAILWAY COMMUNICATION NETWORK STUDY AND DESIGN

WORAWIT DETBOON
WISUT SUKCHITNITAYAKAN

THIS THESIS IS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
BACHELOR OF ENGINEERING IN INFORMATION ENGINEERING
FACULTY OF ENGINEERING
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
ACADEMIC YEAR 2014

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองปริญญานิพนธ์

หัวข้อปริญญานิพนธ์	การศึกษาและออกแบบเครือข่ายการสื่อสารในระบบขนส่งทางราง
Thesis Title	RAILWAY COMMUNICATION NETWORK STUDY AND DESIGN
ชื่อนักศึกษา	นายวรวิช เดชบุญ นายวิศุทธิ์ สุขจิตต์นิตยกาล
ระดับปริญญา	วิศวกรรมศาสตรบัณฑิต
สาขาวิชา	วิศวกรรมสารสนเทศ
ปริญญานิพนธ์ปีการศึกษา	2557

(.....)

ดร.วันวิสา ชัชวงษ์

อาจารย์ที่ปรึกษาปริญญานิพนธ์

(.....)

ผศ.บุณย์ชนะ ภู่ระหงษ์

อาจารย์ที่ปรึกษาปริญญานิพนธ์ร่วม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อปริญญานิพนธ์ การศึกษาและออกแบบเครือข่ายการสื่อสารในระบบขนส่งทางราง
Thesis Title RAILWAY COMMUNICATION NETWORK STUDY AND DESIGN
ชื่อนักศึกษา นายวรวิช เดชบุญ รหัสนักศึกษา 54011134
นายวิศุทธิ์ สุขจิตต์นิตยกาล รหัสนักศึกษา 54011212
ระดับปริญญา วิศวกรรมศาสตรบัณฑิต
สาขาวิชา วิศวกรรมสารสนเทศ
ปีการศึกษา 2557
อาจารย์ที่ปรึกษาปริญญานิพนธ์ ดร.วันวิสา ชัชวงษ์
อาจารย์ที่ปรึกษาปริญญานิพนธ์ร่วม ผศ.บุณย์ชนะ ภู่ระหงษ์

บทคัดย่อ

งานวิจัยนี้เป็นการศึกษาระบบงานและระบบสื่อสารในระบบขนส่งทางราง เพื่อออกแบบระบบเครือข่ายการสื่อสารผ่านโปรแกรมจำลองที่สามารถรองรับการทำงานของระบบต่างๆดังนี้ ระบบการสื่อสารทางเสียงผ่านไอพี (Voice over IP : VoIP) ระบบสกาดา (Supervisory Control and Data Acquisition : SCADA) ระบบเครือข่ายไร้สารสาธารณะ (Public Wi-Fi) ระบบข้อมูลผู้โดยสาร (Passenger Information : PI) ระบบสำนักงาน (Office IT) ระบบควบคุมความปลอดภัยการเข้าออก (Control Access Security System : CASS) ระบบประชาสัมพันธ์ (Passenger Announcement) ระบบอาณัติสัญญาณรถไฟ (Signaling) ระบบเวลา (Clock) และระบบกล้องวงจรปิด (CCTV) โดยระบบเครือข่ายจำลองที่ออกแบบขึ้นจะสามารถรองรับการสื่อสารของทุกระบบข้างต้นไว้ได้ในระบบเครือข่ายเดียวกัน เพื่อให้การบริหารจัดการเครือข่ายการสื่อสารทั้งหมดให้มีประสิทธิภาพสูงขึ้น และสะดวกในการบำรุงรักษา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Thesis Title	RAILWAY COMMUNICATION NETWORK STUDY AND DESIGN	
Student	Mr.Worawit Detboon	Student ID. 54011134
	Mr.Wisut Sukchitnitayakan	Student ID. 53011212
Degree	Bachelor of Engineering	
Program	Information Engineering	
Academic Year	2557	
Thesis Advisor	Dr. Vanvisa Chutchavong	
Thesis Co-Advisor	Asst.Prof. Boonchana Purahong	

ABSTRACT

This thesis to design a network as to support all service systems and commercial in the railway system. The system that we need support is Voice over IP: VoIP, Supervisory Control and Data Acquisition system: SCADA, Public Wi-Fi, Passenger Information: PI, Office IT, Control Access Security System: CASS, Passenger Announcement: PA, Signaling, Clock and CCTV. Network communication model designed will include all of the system in the one communication network for the management of communication networks to more powerful and ease of maintenance. The designed network is implanted onto a network simulation in order verify the design.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จได้อย่างดี ด้วยความอนุเคราะห์ช่วยเหลือจากอาจารย์ที่ปรึกษา ดร.วันวิสา ชัชวงษ์ และผศ.บุณย์ชนะ ภู่ระหงษ์ที่ช่วยให้คำชี้แนะและแนวคิดในการสร้างผลงานขึ้นมา

ขอบคุณสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติที่มอบทุนวิจัยให้

ขอบคุณมหาวิทยาลัยมหิดลที่จัดค่ายอบรมความรู้ในเรื่องระบบขนส่งทางราง

ขอบคุณวิศวกรพี่เลี้ยงที่คอยให้ความรู้และความช่วยเรื่องการด้านเทคนิคต่างๆ

และขอบคุณผู้มีพระคุณทุกๆ คน ที่อาจจะไม่ได้กล่าวถึง ณ ที่แห่งนี้

สิ่งที่มีประโยชน์ สิ่งที่เกิดคุณค่า อันเกิดจากปริญญานิพนธ์นี้ คณะผู้จัดทำขอมอบให้แก่ผู้มีพระคุณทุกท่าน

นายวรวิช เดชบุญ

นายวิศุทธิ์ สุขจิตต์นิตยกาล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

ตารางที่ หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การพัฒนาระบบการขนส่งทางรางเป็นการพัฒนาโครงสร้างสาธารณูปโภคขนาดใหญ่ที่เป็นปัจจัยสำคัญในการพัฒนาประเทศด้วยเหตุผลหลายประการ ในมุมมองของผู้ให้บริการสมัยใหม่จำเป็นต้องมีการสร้างสมดุลระหว่างปริมาณการลงทุนในโครงสร้าง และความพึงพอใจในการรับบริการของผู้โดยสารให้มีความสอดคล้องกัน โดยการเลือกที่จะลงทุนและใช้ประโยชน์จากเทคโนโลยีสารสนเทศและการสื่อสารที่ดีนั้น เป็นส่วนสำคัญในระบบขนส่งทางราง

ทั้งนี้ระบบเครือข่ายยุคใหม่มุ่งไปใช้ระบบเครือข่ายแบบ ไอพี/อีเทอร์เน็ต กันมากขึ้น และระบบการขนส่งทางรางก็เป็นหนึ่งในนั้นเช่นกัน ดังนั้นการที่รวบรวมให้ระบบเครือข่ายต่างๆ ที่เคยมีอยู่เป็นจำนวนมากในการขนส่งทางรางให้เหลือเพียงแค่เครือข่ายเดียวจะทำให้เกิดความสะดวกในการบำรุงรักษา และการบริหารจัดการเครือข่ายให้เกิดประสิทธิภาพสูงสุด ซึ่งประโยชน์ที่ได้รับนั้นไม่เพียงเกิดกับผู้ให้บริการเท่านั้น แต่ผู้ใช้บริการก็จะได้รับการบริการที่มีประสิทธิภาพสูงยิ่งขึ้นด้วยเช่นกัน

1.2 จุดประสงค์

ในการทำโครงงานนี้มีจุดประสงค์ในการทำงานโดยสามารถระบุได้ดังนี้

1.2.1 เพื่อศึกษาการทำงานของเครือข่ายการสื่อสารของระบบขนส่งทางราง

1.2.2 เพื่อออกแบบระบบเครือข่ายการสื่อสารของระบบขนส่งทางราง

1.2.3 เพื่อศึกษาวิธีการตั้งค่าอุปกรณ์เครือข่ายการสื่อสารต่างๆ

1.2.4 จำลองเครือข่ายการสื่อสารของระบบขนส่งทางราง และการตั้งค่าอุปกรณ์ต่างๆ ในการใช้งานจริง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.3 ขอบเขตของโครงงาน

1.3.1 สามารถจำลองเครือข่ายการสื่อสาร ที่มี 4 สถานีย่อย และ 1 สถานีใหญ่ได้

1.3.2 สามารถรับ-ส่งข้อมูลต่างๆได้ และกำหนดไม่ให้ส่วนที่ไม่เกี่ยวข้องกันในการทำงานไม่สามารถติดต่อกันได้

1.3.3 สามารถตั้งค่าอุปกรณ์ได้ทั้งหมด โดยอ้างอิงจากโปรแกรม Cisco Packet Tracer

1.3.4 สามารถกำหนดกำหนดการไหลของข้อมูลในระบบ โดยเหมาะสมกับความต้องการของแต่ละระบบย่อย

1.4 ผลที่คาดว่าจะได้รับ

1.4.1 ระบบเครือข่ายจำลองของระบบขนส่งทางรางที่สามารถรับ-ส่งข้อมูลได้จริง

1.4.2 ระบบเครือข่ายจำลองของระบบขนส่งทางรางที่สามารถกำหนดการไหลของข้อมูลได้อย่างเหมาะสม

1.4.3 มีความรู้ความเข้าใจในการตั้งค่าอุปกรณ์ต่างๆ ที่ใช้ในระบบเครือข่าย

1.4.4 มีความรู้ความเข้าใจในระบบเครือข่ายของระบบขนส่งทางรางมากขึ้น

1.5 อุปกรณ์ที่ต้องใช้

ซอฟต์แวร์

- Cisco Packet Tracer

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2
ทฤษฎีพื้นฐานที่ใช้

2.1 ทฤษฎีเกี่ยวกับไอพีแอดเดรส (IP Address)

ไอพีแอดเดรสย่อมาจาก Internet Protocol address หรือชื่ออื่นเช่น ที่อยู่ไอพี, หมายเลขไอพี, เลขไอพี คือฉลากหมายเลขที่กำหนดให้แก่อุปกรณ์แต่ละชนิด (เช่นคอมพิวเตอร์ เครื่องพิมพ์) ที่มีส่วนร่วมอยู่ในเครือข่ายคอมพิวเตอร์หนึ่งๆ ที่ใช้อินเทอร์เน็ตโปรโตคอลในการสื่อสาร อินเทอร์เน็ตโปรโตคอลได้กำหนดเลขที่อยู่ไอพีให้เป็นตัวเลข 32 บิตค่าหนึ่ง ซึ่งเป็นที่รู้จักในชื่อเลขที่อยู่ไอพีรุ่น 4 (IPv4) และระบบนี้ยังคงมีการใช้งานอยู่ในปัจจุบัน เลขที่อยู่ไอพีเป็นเลขฐานสอง แต่ก็มักจะแสดงผลและเก็บบันทึกในไฟล์ข้อความด้วยตัวเลขที่มนุษย์ทั่วไปสามารถอ่านได้ ตัวอย่างเช่น 172.16.254.1

องค์การกำหนดหมายเลขอินเทอร์เน็ต (IANA) เป็นผู้ดำเนินการจัดสรรเลขที่อยู่ไอพีทั่วโลก และมอบอำนาจให้หน่วยงานทะเบียนอินเทอร์เน็ตประจำภูมิภาค (RIR) ทั้ง 5 เขต ทำหน้าที่จัดสรรกลุ่มเลขที่อยู่ไอพีสำหรับหน่วยงานทะเบียนอินเทอร์เน็ตส่วนท้องถิ่น (ผู้ให้บริการอินเทอร์เน็ต) และหน่วยงานอื่น ๆ

2.1.1 เลขที่อยู่ไอพีรุ่น 4

เลขที่อยู่ไอพีรุ่น 4 ประกอบด้วยเลข 32 บิต ซึ่งสามารถรองรับที่อยู่ที่ไม่ซ้ำกันมากสุดเท่าที่จะเป็นไปได้ 4,294,967,296 (2^{32}) หมายเลข แต่เลขที่อยู่ไอพีรุ่น 4 ก็ได้สงวนบางหมายเลขไว้สำหรับจุดประสงค์พิเศษอย่างเช่น เครือข่ายส่วนตัว (ประมาณ 18 ล้านหมายเลข) และเลขที่อยู่มัลติแคสต์ (ประมาณ 270 ล้านหมายเลข)

เลขที่อยู่ไอพีรุ่น 4 เขียนแทนด้วยตัวเลขฐานสิบ ซึ่งประกอบด้วยเลขฐานสิบ 4 จำนวน แต่ละจำนวนมีค่าได้ตั้งแต่ 0 ถึง 255 และคั่นด้วยจุด ตัวอย่างเช่น 172.16.254.1 เป็นต้น แต่ละส่วนของหมายเลขแทนกลุ่มของเลข 8 บิต ในงานเขียนเชิงเทคนิคบางงาน เลขที่อยู่ไอพีรุ่น 4 ก็อาจเขียนแทนด้วยเลขฐานสิบหก เลขฐานแปดหรือเลขฐานสองก็ได้

2.1.2 การแบ่งเครือข่ายย่อยของรุ่น 4

ในช่วงแรกๆ ของการพัฒนาอินเทอร์เน็ตโปรโตคอล ผู้ดูแลระบบเครือข่ายแปลเลขที่อยู่ไอพีเป็นสองส่วนคือ ส่วนหมายเลขเครือข่าย และส่วนหมายเลขแม่ข่าย ออกเตตอันดับสูงสุด (กลุ่ม 8 บิตที่มีนัยสำคัญมากสุด) ของเลขที่อยู่ไอพีถูกตั้งให้เป็น หมายเลขเครือข่าย (network number) และจำนวนบิตที่เหลือเรียกเป็น เขตข้อมูลส่วนเหลือ (rest field) หรือ ตัวระบุแม่ข่าย (host identifier) และได้นำมาใช้กำหนดหมายเลขภายในเครือข่ายหนึ่งๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

วิธีการในช่วงแรกนี้ได้รับการพิสูจน์ในเวลาต่อมาว่าไม่พอเพียง เนื่องจากเครือข่ายเพิ่มเติมที่พัฒนาขึ้นโดยอิสระจากเครือข่ายที่มีอยู่ มีหมายเลขเครือข่ายกำหนดไว้อยู่แล้ว คุณลักษณะการกำหนดที่อยู่อินเทอร์เน็ตจึงได้แก้ไขปรับปรุงใน ค.ศ. 1981 โดยแนะนำสถาปัตยกรรมเครือข่ายแบบคลาส (classful network) เพิ่มเข้าไป

เครือข่ายแบบคลาสได้ออกแบบให้สามารถกำหนดเครือข่ายเอกเทศได้จำนวนมากขึ้นกว่าเดิม และสามารถออกแบบเครือข่ายย่อย (subnet) โดยละเอียดได้ 3 บิตแรกของออกเตตที่มีนัยสำคัญมากสุดของเลขที่อยู่ไอพี ถูกนิยามว่าเป็น คลาส (class) ของหมายเลขนั้น คลาส 3 คลาส (A, B, และ C) ได้นิยามขึ้นเพื่อการกำหนดเลขที่อยู่ยูนิแคสต์ (unicast) อย่างสากล ตัวระบุเครือข่ายจะมีพื้นฐานอยู่บนส่วนขอบเขตของออกเตตจากทั้งเลขที่อยู่ โดยขึ้นอยู่กับคลาสที่อยู่ แต่ละคลาสจะใช้ออกเตตเพิ่มขึ้นเป็นตัวระบุเครือข่าย ดังนั้นจำนวนแม่ข่ายที่เป็นไปได้จะลดลงในคลาสอันดับที่สูงขึ้น (B กับ C) ตารางต่อไปนี้แสดงถึงภาพรวมของระบบซึ่งปัจจุบันเลิกใช้แล้ว

ตารางที่ 2.1 สถาปัตยกรรมเครือข่ายแบบคลาส

คลาส	บิตขึ้นต้น	ขนาดบิตหมายเลขเครือข่าย	ขนาดบิตเขตข้อมูลส่วนเหลือ	จำนวนเครือข่าย	จำนวนเลขที่อยู่ต่อเครือข่าย	เลขที่อยู่เริ่มต้น	เลขที่อยู่สิ้นสุด
A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255

2.1.3 เลขที่อยู่ส่วนตัวของรุ่น 4

การออกแบบเครือข่ายในช่วงแรก ในตอนที่ความสามารถในการเชื่อมต่อจากปลายถึงปลาย (end-to-end connectivity) ของทั้งโลกสามารถแลเห็นได้เพื่อการสื่อสารกับแม่ข่ายอินเทอร์เน็ต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ทุกแม่ข่าย ได้ตั้งเจตนารมณ์ไว้ว่าเลขที่อยู่ไอพีจะถูกกำหนดให้คอมพิวเตอร์หรืออุปกรณ์แต่ละเครื่องโดยไม่ซ้ำกันทั้งโลก อย่างไรก็ตามไม่จำเป็นเสมอไปเมื่อเครือข่ายส่วนตัวได้พัฒนาขึ้น

คอมพิวเตอร์ที่ไม่ได้เชื่อมต่อกับอินเทอร์เน็ตก็ไม่จำเป็นต้องมีเลขที่อยู่ไอพีที่ไม่ซ้ำกับใครในโลกเช่น เครื่องจักรอุตสาหกรรมที่สื่อสารระหว่างกันผ่านทีซีพี/ไอพีเป็นต้น ช่วงเลขที่อยู่ไอพีรุ่น 4 จำนวน 3 ช่วงจึงถูกสงวนไว้ในอาร์เอฟซี 1918 สำหรับใช้กับเครือข่ายส่วนตัว เลขที่อยู่เหล่านี้จะไม่ถูกนำไปใช้จัดเส้นทางบนอินเทอร์เน็ต และการใช้งานเลขที่อยู่เหล่านี้ก็ไม่ต้องรายงานต่อหน่วยงานทะเบียนฯ แต่อย่างใด

ในทุกวันนี้ เครือข่ายส่วนตัวสามารถเชื่อมต่อกับอินเทอร์เน็ตผ่านทางการแปลที่อยู่เครือข่าย (network address translation: NAT) เมื่อต้องการใช้

ตารางที่ 2.2 ช่วงเลขที่อยู่ไอพีรุ่น 4 ที่สงวนไว้สำหรับเครือข่ายส่วนตัวโดย IANA

	เริ่มต้น	สิ้นสุด	จำนวนเลขที่อยู่
บล็อก 24 บิต (ขึ้นต้น 8 บิต, 1 × A)	10.0.0.0	10.255.255.255	16,777,216
บล็อก 20 บิต (ขึ้นต้น 12 บิต, 16 × B)	172.16.0.0	172.31.255.255	1,048,576
บล็อก 16 บิต (ขึ้นต้น 16 บิต, 256 × C)	192.168.0.0	192.168.255.255	65,536

ผู้ใช้สามารถใช้บล็อกที่สงวนไว้ดังกล่าวอันใดก็ได้ โดยทั่วไปแล้ว ผู้ดูแลเครือข่ายจะแบ่งบล็อกเป็นเครือข่ายย่อย ตัวอย่างเช่น เราเตอร์ตามบ้านหลาย ๆ เครื่องใช้ช่วงเลขที่อยู่เป็น 192.168.0.0 ถึง 192.168.0.255 (เครือข่ายย่อย 192.168.0.0/24) โดยอัตโนมัติ

2.1.4 เครือข่ายย่อยของไอพี

เครือข่ายไอพีอาจแบ่งเป็นเครือข่ายย่อยได้ทั้งไอพีรุ่น 4 เลขที่อยู่ไอพีหมายเลขหนึ่งจะถูกจำแนกเป็นสองส่วนเพื่อจุดประสงค์นี้ได้แก่ เลขขึ้นต้นเครือข่าย(network prefix) และ ตัวระบุแม่ข่ายสำหรับรุ่น 4 โดยเขียนเครื่องหมายทับตามด้วยตัวเลขฐานสิบต่อท้ายเลขที่อยู่ไอพี ซึ่งบางทีก็เรียกว่า เลขขึ้นต้นของการจัดเส้นทาง (routing prefix) ยกตัวอย่าง กำหนดให้เลขที่อยู่ไอพีเป็น 192.0.2.1 และเลขที่เครือข่ายย่อยเป็น 255.255.255.0 หรือ 192.0.2.1/24 เพราะ 24 บิตแรกของเลขที่อยู่ไอพีแสดงถึงหมายเลขเครือข่ายและเครือข่ายย่อย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2 ทฤษฎีเกี่ยวกับ DHCP (Dynamic Host Configuration Protocol)

DHCP คือ โปรโตคอล client/server พื้นฐานที่ช่วยลดการจัดการไอพีแอดเดรส ของโฮสต์คอมพิวเตอร์และการตั้งค่าโครงสร้างอื่นๆให้ง่ายขึ้น

2.2.1 DHCP Messages

DHCP client และ DHCP server ทำการติดต่อสื่อสารโดยการแลกเปลี่ยนข้อความ DHCP ข้อความ DHCP ประกอบด้วย 8 ประเภท ซึ่งทั้งหมดจะส่งโดย User Datagram Protocol (UDP) ในกระบวนการตั้งค่าไอพีแอดเดรสของ DHCP client จะใช้การกระจายข้อความ DHCP ส่งไปยังไอพีแอดเดรส 255.255.255.255 DHCP client กับไอพีแอดเดรสและผู้ที่ได้รับจะใช้ unicast ข้อความ DHCP ตอบกลับมา DHCP client ตั้งอยู่บน UDP พอร์ทที่ 68 DHCP server และ DHCP relay agent อยู่ในพอร์ทที่ 67

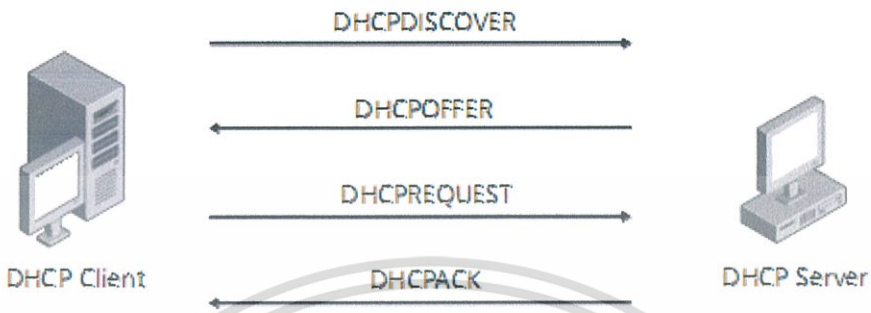
ประเภทข้อความ DHCP ทั้ง 8 มีดังต่อไปนี้:

- DHCPDISCOVER ส่งโดย DHCP client ไปยังตำแหน่งของ DHCP server
- DHCPOFFER ส่งโดย DHCP server ไปยัง DHCP client ในการตอบรับข้อความ DHCPDISCOVERประกอบด้วยการหาไอพีแอดเดรสและการกำหนดค่าอื่นๆ
- DHCPREQUEST ส่งโดย DHCP client ไปยัง DHCP server เพื่อขอไอพีแอดเดรสและการกำหนดค่าอื่นๆ จาก DHCP server การปฏิเสธข้อเสนอจาก server อื่น หรือการยอมรับความถูกต้องของแอดเดรสที่มีอยู่แล้ว (ตัวอย่างเช่น หลังจากรีสตาร์ทหรือการขยาย DHCP ที่มีอยู่)
- DHCPACK ส่งโดย DHCP server ไปยัง DHCP client เพื่อตอบสนอง DHCPREQUEST เพื่อยอมรับไอพีแอดเดรสและให้ลูกข่ายกำหนดค่าพารามิเตอร์เหล่านั้นที่ลูกข่ายร้องขอและ server ได้กำหนดค่าให้
- DHCPNAK ส่งโดย DHCP server ไปยัง DHCP client แต่ลูกข่ายไม่ยอมรับ DHCPREQUEST ในที่นี้อาจเกิดขึ้นหากที่อยู่ที่ต้องการไม่ถูกต้องเพราะลูกข่ายได้ย้ายไปยังเครือข่ายย่อยใหม่หรือ DHCP client หมดอายุและไม่สามารถสร้างใหม่ได้
- DHCPDECLINE ส่งโดย DHCP client ไปยัง DHCP server แล้ว server จะแจ้งว่าไอพีแอดเดรสใช้ไม่ได้เนื่องจากถูกใช้โดยคอมพิวเตอร์เครื่องอื่น
- DHCPRELEASE ส่งโดย DHCP client ไปยัง DHCP server การยกเลิกไอพีแอดเดรสและการการยกเลิกบริการที่มีอยู่
- DHCPINFORM ส่งโดย DHCP client ไปยัง DHCP server เพื่อร้องขอการตั้งค่าเพิ่มเติมแล้วลูกข่ายมีการกำหนดไอพีแอดเดรสไว้อยู่แล้ว ข้อความประเภทนี้จะใช้สำหรับตรวจสอบผู้บุกรุก DHCP server ใน Windows server 2008

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2.2 DHCP Message Exchanges

การแลกเปลี่ยนข้อความ DHCP สำหรับการรับและการกำหนด DHCP-leased ไอพีแอดเดรส และสำหรับตรวจสอบผู้บุกรุกใน DHCP servers จะมีขั้นตอนดังรูปที่ 2.2



รูปที่ 2.1 การแลกเปลี่ยนข้อความ DHCP ในระหว่างเริ่มต้นให้บริการ
(อ้างอิงโดย http://cpe.rmutt.ac.th/comnet/pr/2552-2/Sec2-Tuesday/Ch14/Docs/Chapter%2014%20Dynamic%20Host%20Configuration%20Protocol%20(DHCP))

เมื่อ DHCP client และ DHCP server ถูกคั่นโดย DHCP relay agent แล้ว DHCP relay agent ได้รับการกระจายสัญญาณข้อความ DHCPDISCOVER และ DHCPREQUEST โดยการเพิ่มของฟิลด์ Hops และบันทึกไอพีแอดเดรสที่ระบุอินเตอร์เฟซที่ติดต่อกับ DHCP relay agent ที่ได้รับข้อความในฟิลด์ Gateway ไอพีแอดเดรสและหลังจากนั้นส่งต่อไปยังการตั้งค่า DHCP server แล้ว DHCP server ตอบรับข้อความ DHCPOFFER และ DHCPACK ไปยังแอดเดรสของ DHCP relay agent หลังจากยูนิแคช DHCP relay agent แล้ว

2.2.3 การสร้าง Lease ใหม่

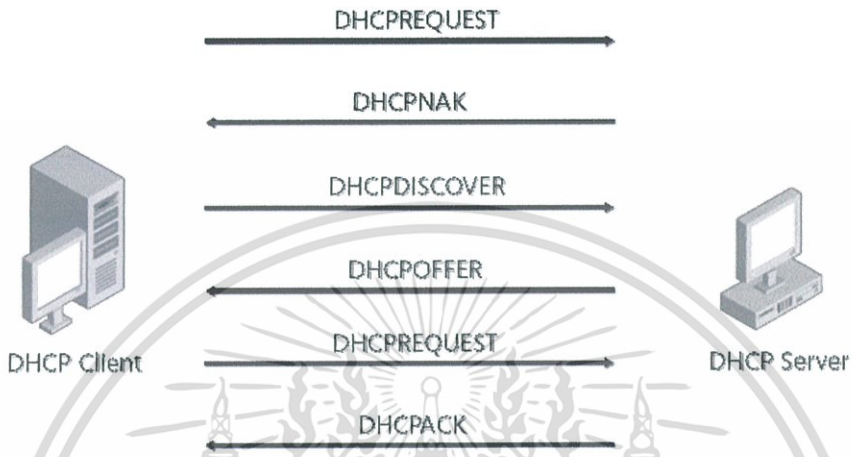
เพราะว่าลักษณะการกำหนดค่าหมายเลขไอพีแอดเดรสนั้นมีเวลาที่จำกัด เครื่องลูกข่ายจึงต้องสร้างการเช่าใหม่ การสร้างการเช่าใหม่เมื่อ DHCP client นั้นมีข้อความ DHCP สองตัวอยู่ด้วยกันคือ DHCPREQUEST และ DHCPACK ซึ่งถ้าการสร้างการเช่าใหม่ในระหว่างที่ DHCP client นั้นอยู่บนเครือข่ายย่อยอย่างต่อเนื่อง DHCP server และ DHCP client จะใช้การส่งข้อความ DHCPREQUEST และ DHCPACK แบบ unicast แต่ถ้าการสร้างการเช่าใหม่นั้นเกิดเมื่อ DHCP client เริ่มใหม่บนเครือข่ายย่อยเดียวกันและไอพีแอดเดรสนั้นมีให้สำหรับการสร้างใหม่ DHCPREQUEST และ DHCPACK จะสื่อสารกันโดยการส่งข้อความ DHCPREQUEST และ DHCPACK แบบ broadcast

2.2.4 การเปลี่ยนเครือข่ายย่อย

ถ้า DHCP client ร้องขอการเช่าผ่านข้อความ DHCPREQUEST ที่ DHCP server นั้นไม่สามารถทำได้ DHCP server จะส่งข้อความ DHCPNAK ไปยัง DHCP client ซึ่งข้อความนี้จะแจ้งทางฝั่ง client ว่าการเช่าไอพีแอดเดรสที่ร้องขอนั้นจะไม่ถูกสร้างใหม่ ฝั่ง client จะได้รับการเช่า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ใหม่โดยการแลกเปลี่ยนข้อความ DHCP จากเดิมจากการเริ่มต้นขึ้นดังอธิบายไปก่อนหน้านี้ซึ่งตัวอย่างที่ดีคือเมื่อ DHCP client นั้นปิดเครื่องโดยไม่คืนไอพีแอดเดรสและเปิดเครื่องบนเครือข่ายย่อยอื่นหรือเมื่อ Wireless แบบ IEEE802.11 เคลื่อนที่ข้ามพื้นที่บริการของ Access Point นั่นคือ DHCP client ได้เชื่อมต่อบนเครือข่ายย่อยอื่นแล้ว ดังรูปที่ 2.3



รูปที่ 2.2 ข้อความ DHCP ที่แลกเปลี่ยนกันเมื่อ DHCP client ย้ายไปยังเครือข่ายย่อยอื่น (อ้างอิงโดย http://cpe.rmutt.ac.th/comnet/pr/2552-2/Sec2-Tuesday/Ch14/Docs/Chapter%2014%20Dynamic%20Host%20Configuration%20Protocol%20(DHCP))

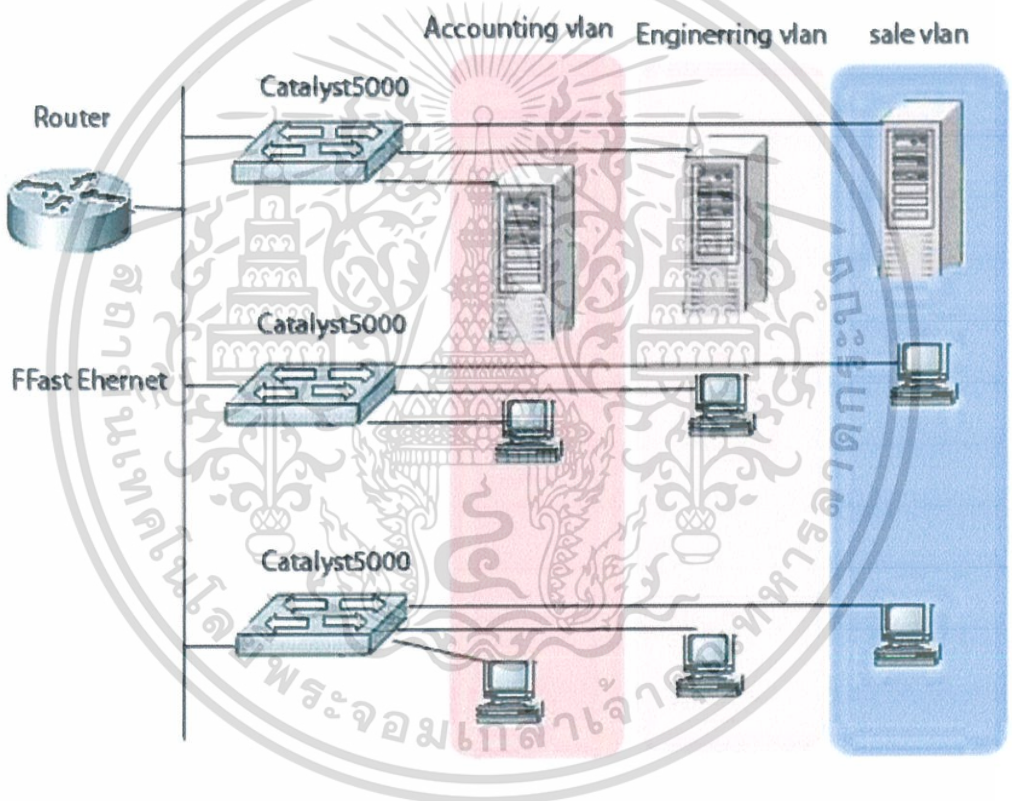
เมื่อเครื่องลูกข่ายของ Windows-Based DHCP นั้นได้เช่าหมายเลขแอดเดรสเริ่มต้นแล้ว เครื่องลูกข่ายจะส่งข้อความ DHCPREQUEST แบบ broadcast เพื่อสร้างการเช่าหมายเลขใหม่ซึ่งมั่นใจได้ว่าการร้องของการเช่าของ DHCP ใหม่นั้นได้ส่งไปยัง DHCP server ที่เป็นผู้จ่าย DHCP address ให้เครื่องลูกข่ายนั้นเปิดอยู่ ซึ่งอาจแตกต่างกับเครื่อง server ที่จ่ายการเช่าชื่อต้น เมื่อ DHCP server นั้นได้รับข้อความ broadcast แล้วจะทำการตรวจสอบโดยการจับคู่กับขอบเขตที่กำหนดไว้บนเครื่อง server และเครือข่ายย่อยที่ได้รับ DHCPREQUEST แต่ถ้าไม่สามารถยอมรับการร้องขอของ client ได้ DHCP server จะส่ง DHCPNAK และ DHCP client จะได้รับการเช่าหมายเลขใหม่

ถ้าเครื่องลูกข่ายของ Windows-Based DHCP นั้นไม่สามารถระบุตำแหน่งของ DHCP server เพื่อทำการสร้างการเช่าใหม่ได้ จะทำการ broadcast เฟรมของ ARP Request เพื่อหา Default-gateway ที่ได้รับมาก่อนหน้านี้และถ้าไอพีแอดเดรสของ Default-gateway นั้นถูกแก้ไขแล้ว DHCP client จะคิดว่าถูกตั้งอยู่บนเครือข่ายย่อยเดียวกันกับการเช่าก่อนหน้านี้และจะใช้การเช่านี้ต่อไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3 ทฤษฎีเกี่ยวกับ VLAN (Virtual Local Area Network)

แลนเสมือนเหมือนการสร้างตรรกะให้สวิสต์ตัวหนึ่งสามารถแบ่งออกมาเป็นหลายๆ VLAN ได้เหมือนมีสวิตช์ (Switch) หลายตัวหรือมีฮับ (hub) หลายตัว แต่จริงๆมีแค่ตัวเดียวแล้วแบ่งซอยออกมา โดยมากแบ่งตามพื้นที่ใช้งานเช่น แบ่งตามแผนก แบ่งตามหน่วยงาน แบ่งตามลักษณะการใช้งาน การทำแลนเสมือนนั้นไม่ขึ้นอยู่กับการต่อทางกายภาพของอุปกรณ์ โดยค่าดีฟอล์ท (Default) ทุกๆ พอร์ทของสวิตช์นั้น จะถูกจัดให้อยู่ใน VLAN 1 หรือที่เรียกกันว่า “Management VLAN” ซึ่งในการสร้าง แก้ไข และลบ VLAN นั้น เราจะไม่สามารถลบ VLAN 1 นี้ได้และหมายเลข VLAN สามารถสร้างได้ตั้งแต่หมายเลข 1 – 1005



รูปที่ 2.3 ลักษณะของ VLAN

(อ้างอิงโดย http://th.wikipedia.org/wiki/แลนเสมือน)

2.3.1 ชนิดของ VLAN

2.3.1.1 สแตติก (Static)

สแตติก VLAN หรือ อีกชื่อหนึ่งคือ Port-Based Membership นั้น จะเป็นการพิจารณาความเป็นสมาชิกของ VLAN หนึ่งๆ โดยดูจากพอร์ท ซึ่งพอร์ทของสวิตช์ที่เชื่อมต่ออยู่กับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

client นั้น ถึงแม้ว่าจะเป็นพอร์ทของสวิตช์เดียวกัน แต่หากพอร์ททั้งสองนั้นอยู่คนละ VLAN กัน ก็ไม่สามารถที่จะติดต่อกันได้ หากไม่มีอุปกรณ์ในlayer 3 มาช่วยในการหาเส้นทาง ซึ่งการเซตพอร์ทแต่ละพอร์ทให้เป็นสมาชิกของ VLAN ใดๆ นั้น จะถูกกระทำแบบมือ (Manual) จาก System Administrator

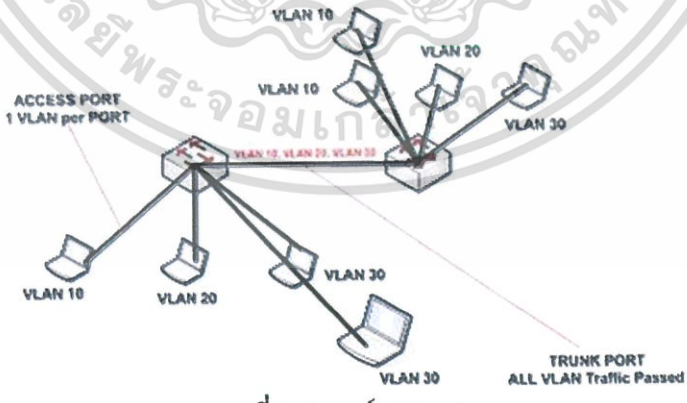
2.3.1.2 ไดนามิค (Dynamic)

ไดนามิค VLAN เป็นการกำหนด VLAN ให้กับเครื่อง client โดยพิจารณาจากหมายเลข MAC Address ของ client ซึ่งเมื่อ client ทำการเชื่อมต่อไปยังสวิตช์ตัวใดๆ สวิตช์ที่รัน Dynamic VLAN นี้ก็จะไปหาหมายเลข VLAN ที่ MAP กับ MAC Address นี้จากฐานข้อมูลส่วนกลางมาให้ ซึ่ง System Administrator สามารถที่จะเซตหมายเลข MAC Address ในการจับคู่กับ VLAN ได้ที่ VLAN Management Policy server (VMPS)

2.3.2 พอร์ท Trunk

เป็นพอร์ททำหน้าที่เชื่อมต่อสวิตช์ตัวอื่น ๆ ที่ต้องการให้เป็นสมาชิกของ VLAN ต่างๆ กันให้มาอยู่ด้วยกันและทำหน้าที่ส่งผ่านข้อมูลเส้นทางต่างๆ ของหลายๆ VLAN ให้กระจายไปยังสวิตช์ตัวอื่นๆ ที่มีพอร์ทที่ถูกกำหนดให้เป็น VLAN เดียวกันกับสวิตช์ตัวต้นทางได้ หรือที่เรียกกันโดยทั่วไปว่าพอร์ท Uplink ซึ่งตัวอย่างในการเซตพอร์ทให้เป็นพอร์ท Trunk นี้ ก็คือ

- พอร์ทที่ทำหน้าที่คอนเนคไปยังสวิตช์ตัวอื่นๆ เช่น พอร์ท Uplink
- พอร์ทที่ทำหน้าที่เชื่อมไปยังเราเตอร์ตัวที่ทำหน้าหาเส้นทางระหว่าง VLAN



รูปที่ 2.4 พอร์ท Trunk

(อ้างอิงโดย http://th.wikipedia.org/wiki/แลนเสมือน)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3.3 ข้อดีและข้อเสียของการทำ VLAN

2.3.3.1 ข้อดีของการทำ VLAN

- เพิ่มประสิทธิภาพของเครือข่าย จำกัดการแพร่กระจายของ broadcast

- ง่ายต่อการใช้งาน ผู้ใช้งานสามารถที่จะเคลื่อนย้ายไปยัง VLAN ของเครือข่ายย่อยอื่นๆ ได้โดยเพียงแค่การเปลี่ยนคอนฟิกของสวิตช์และไอพีแอดเดรสของ client เพียงนิดเดียว ไม่จำเป็นต้องมีการย้ายสวิตช์ หรือสายเคเบิลใดๆ

- เพิ่มเครื่องง่าย สามารถรองรับการขยายตัวของระบบเนตเวิร์คที่จะเพิ่มขึ้นในอนาคตได้ง่าย เนื่องจากมีการวางแผนเกี่ยวกับการทำเครือข่ายย่อย และการดีไซน์ระบบที่ไม่ยึดติดกับทางกายภาพอีกต่อไป

- เพิ่มเรื่องของความปลอดภัย สามารถสร้างกลไกด้านความปลอดภัยได้ง่ายขึ้น เช่น การสร้าง Access Control Lists บนอุปกรณ์layer 3 และ ลดความเสี่ยงเกี่ยวกับการดักจับข้อมูล (Sniffing)

2.3.3.2 ข้อเสียของการทำ VLAN

- ถ้าเป็นการแบ่ง VLAN แบบ Port-based นั้นจะมีข้อเสียเมื่อมีการเปลี่ยนพอร์ทนั้นอาจจะต้องทำการคอนฟิก VLAN ใหม่

- ถ้าเป็นการแบ่ง VLAN แบบ MAC-based นั้นจะต้องให้ค่าเริ่มต้นของ VLAN membership ก่อน และปัญหาที่เกิดขึ้นคือในระบบเครือข่ายที่ใหญ่มาก จำนวนเครื่องนับพันเครื่อง นอกจากนี้ถ้ามีการใช้เครื่อง Notebook ด้วย ซึ่งก็จะมีค่า MAC และเมื่อทำการเปลี่ยนพอร์ทที่ต่อก็ต้องทำการคอนฟิก VLAN ใหม่

2.3.4 การติดต่อสื่อสารระหว่าง VLAN

VLAN ก็คือ LAN วงหนึ่งที่ LAN 2 วงจะติดต่อสื่อสารกันตรงๆไม่ได้ต้องผ่านอุปกรณ์ layer3 และเราเตอร์ก็เป็นอุปกรณ์หนึ่งใน layer3 ทำหน้าที่หาเส้นทางเครือข่ายย่อยจาก VLAN วงหนึ่งไปอีก เครือข่ายย่อย VLAN

2.3.5 มาตรฐานของ VLAN

มาตรฐาน IEEE 802.1Q นั้นเป็นมาตรฐานในการนำข้อมูลของ VLAN membership ใส่เข้าไปใน Ethernet Frame หรือที่เรียกว่า การ Tagging และโปรโตคอล 802.1Q นี้ถูกพัฒนาเพื่อแก้ปัญหาเรื่องการบริหารจัดการด้านเครือข่ายที่เพิ่มขึ้น เช่น การกระจายเครือข่ายใหญ่ๆ ให้เป็นส่วนย่อยๆ (Segment) ทำให้ไม่สูญเสียแบนวิธให้กับการ broadcast และ multicast มากเกินไป และยังเป็นการรักษาความปลอดภัยระหว่างส่วนย่อยต่างๆ ภายในเครือข่ายให้สูงขึ้นอีกด้วย การต่อ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เติมเฟรม (tagging Frame) ด้วยมาตรฐาน 802.1Q นั้นจะทำในระดับ Data-Link layer และการทำ VLAN Tagging นั้นจะเป็นการเปลี่ยนรูปแบบของ Ethernet Frame มาตรฐาน 802.3 ให้เป็นรูปแบบใหม่ที่เป็นมาตรฐาน 802.3 ac

2.4 ทฤษฎีเกี่ยวกับ VTP (Virtual Trunking Protocol)

ในการที่เราจะสร้าง VLAN หนึ่งๆ ขึ้นมาใช้งานนั้น เราจำเป็นที่จะต้องสร้าง VLAN ที่ตัวสวิตช์หนึ่งๆ (รวมถึงตั้งชื่อให้ VLAN ในบางกรณี) ซึ่งหากว่า ในโครงสร้างระบบ (Infrastructures) ของเรานั้นมีสวิตช์หลายๆ ตัวอยู่ในระบบนั้น การที่จะสร้าง VLAN ทุกๆ VLAN ขึ้นมานั้น คงเป็นเรื่องที่เสียเวลามากเลยทีเดียว ดังนั้นทาง CISCO จึงมีเทคนิคที่จะทำให้เราสามารถออกแบบ และสร้างหมายเลข VLAN ที่จุดๆ เดียว และมีการกระจาย (Propagation) ไปยังสวิตช์ตัวอื่นๆ ภายในเนตเวิร์คของเราได้ โดยที่โปรโตคอล VTP นี้ จะมีหลักการในการทำงานดังต่อไปนี้

2.4.1 VTP Operation

เมื่อเริ่มแรกต้องโปรโมทสวิตช์ตัวหนึ่งๆ ขึ้นมา โดยต้องมีการสร้าง VLAN ขึ้นที่สวิตช์ตัวนี้ สวิตช์ตัวนี้จะมีหน้าที่เป็น VTP server ให้กับสวิตช์ทุกๆตัวในเนตเวิร์ค เมื่อนำสวิตช์ตัวอื่นๆ มาต่อกับด้วย (สวิตช์ตัวแรก จะต้องถูกเซตให้เป็น VTP server mode และ สวิตช์ตัวต่อๆ มา จะต้องถูกเซตเป็น VTP client mode และมีการเซต โดเมนเนมภายในสวิตช์ให้เหมือนกัน (อย่างน้อยที่สุดในครั้งแรกที่นำสวิตช์ตัวอื่นๆมาต่อกับ VTP server สวิตช์ตัวอื่นๆ จำเป็นที่จะต้องอยู่ในสถานะ client mode จนกระทั่งได้เรียนรู้ VLAN Number เรียบร้อยแล้ว) เมื่อเชื่อมต่อในลักษณะนี้แล้ว VTP server จะเป็นตัวแพร่กระจายหมายเลข VLAN ให้แก่สวิตช์ที่อยู่ใน client mode ที่เหลือ

2.4.2 VTP Domain

เป็นการรวมกลุ่มของสวิตช์ทั้งหมดที่มีการบริหารจัดการ VLAN เหมือนกัน มาอยู่ด้วยกัน และจะมีฐานข้อมูลของ VLAN เป็นชุดเดียวกัน และ สวิตช์จะไม่ share ฐานข้อมูลภายในโดเมนของตน ให้แก่โดเมนอื่นๆ

2.4.3 VTP Modes

2.4.3.1 VTP server mode

สวิตช์ที่ทำหน้าที่เป็น VTP server mode จะมีอิสระอย่างเต็มที่ในการเพิ่มหรือลบ VLAN ได้ ซึ่งใน 1 โดเมน จำเป็นที่จะต้องมีอย่างน้อย 1 VTP server หรืออาจมากกว่าก็ได้

2.4.3.2 VTP client mode

สวิตช์ที่ทำหน้าที่เป็น VTP client mode จะสามารถทำได้เพียงแค่รับหมายเลข VLAN มาจาก VTP server เท่านั้น ไม่สามารถที่จะแก้ไขหรือลบ VLAN ได้

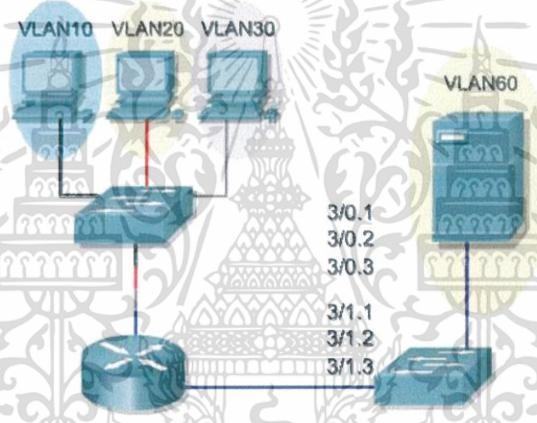
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.4.3.3 VTP transparent mode

สวิตช์ที่ทำหน้าที่เป็น VTP transparent mode จะไม่เกี่ยวข้องในการอัพเดตหรือรับรู้เกี่ยวกับสวิตช์ตัวอื่นๆ ภายในโดเมน แต่จะทำการฟอร์เวิร์ดเฟรมที่วิ่งผ่านไปยังปลายทางได้ผ่านทางพอร์ท Trunk จุดประสงค์ของ VTP transparent Mode นี้ มักใช้ในการ Save Configurations ของสวิตช์ (VTP server, VTP client ไม่สามารถทำได้)

2.4.4 การหาเส้นทางระหว่าง VLAN (Inter-VLAN Routing)

ในการหาเส้นทางระหว่าง VLAN จำเป็นที่จะต้องมีอุปกรณ์ใน layer3 เช่น เราเตอร์หรือสวิตช์ layer 3 เข้ามาช่วยในการหารเส้นทางที่อยู่ต่าง VLAN หรือต่างเครือข่ายย่อยกันออกไป ซึ่งเทคนิคในการนำเอาเราเตอร์มาใช้นั้น เราเรียกว่า "Routes on a stick" และ เทคนิคในการนำเอาสวิตช์ layer 3 มาใช้ในการหาเส้นทางนั้น เราเรียกว่า "Switch Virtual Interface (SVI)"



รูปที่ 2.5 เทคนิคการใช้เราเตอร์ในการหาเส้นทางระหว่าง VLAN
(อ้างอิงโดย http://www.msit.mut.ac.th/newweb/phpfile/show.php?Qid=1055)

รูปแบบในการเชื่อมต่อแบบ Routes on a stick นี้ เราเตอร์จะใช้เพียง Fast Ethernet อย่างน้อย 1 พอร์ทในการต่อเข้ากับสวิตช์และมีการเซต Sub-Interface ที่รองรับ VLAN นั้นๆ เพื่อทำหน้าที่หาเส้นทางระหว่าง VLAN และ จะต้องเซตพอร์ทของสวิตช์พอร์ทนั้นเป็นแบบพอร์ท Trunk ด้วย และพอร์ทของเราเตอร์ จะต้องมีการเซต Encapsulation ในแบบที่สวิตช์ตัวนั้นๆ ยอมรับ เช่น ในการใช้เราเตอร์ในการหาเส้นทางของ สวิตช์ซิสโก้ Catalyst 2950 Series นั้น พอร์ทของเราเตอร์ที่ทำ Routes on a stick นั้น จะต้องเซต Encapsulation เป็นแบบ IEEE 802.1Q จึงจะสามารถใช้งานได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.5 ทฤษฎีเกี่ยวกับ ACLs (Access Control Lists)

แอคเซส คอนโทรลลิสท์ (ACLs) นั้นถือเป็นเทคนิคการป้องกันพื้นฐานของเราเตอร์ในอินเทอร์เน็ต โดยจำแนกของอุปกรณ์การรักษาความปลอดภัยในระบบ LAN-WAN ได้ดังต่อไปนี้

2.5.1 Packet Filtering

เราเตอร์ที่ทำการหาเส้นทางและส่งต่ออย่างมีเงื่อนไข โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ (header) ของแพคเกตที่ผ่านเข้ามาเทียบกับกฎ (rules) ที่กำหนดไว้และตัดสินว่าควรจะทิ้ง (drop) แพคเกตนั้นไปหรือว่าจะยอม (accept) ให้แพคเกตนั้นผ่านไปได้ โดยเราเตอร์ จะพิจารณาจากไอพีแอดเดรสต้นทางและปลายทางรวมถึงพอร์ท

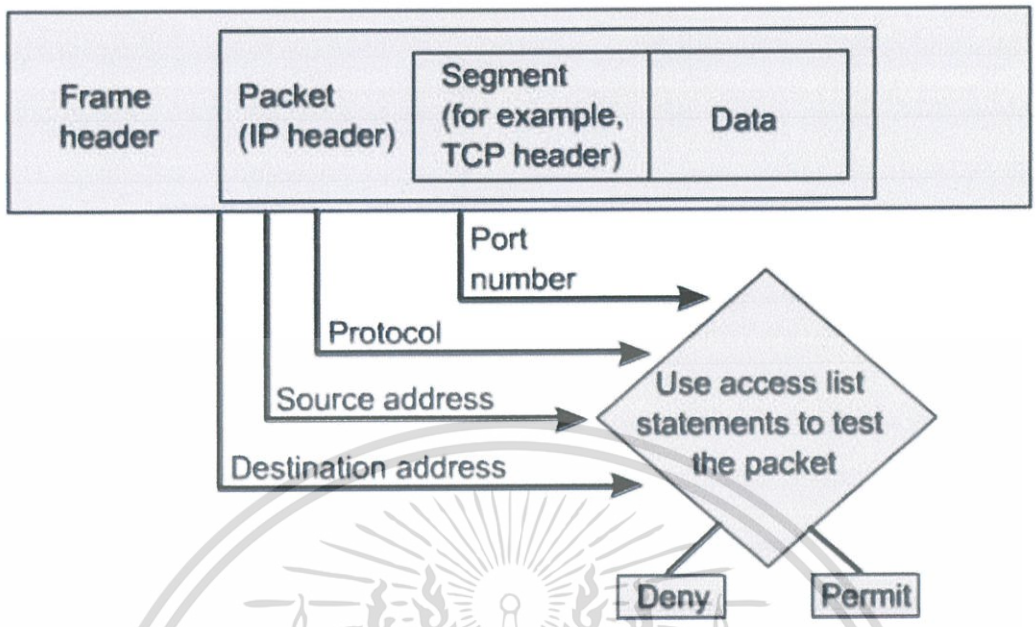
2.5.2 ประโยชน์ของ Access Control Lists

สามารถความคุมเส้นทางที่มาตามพอร์ทต่างๆ หรือ มาตามไอพีแอดเดรสได้ มักจะถูกใช้ในการควบคุม DDR (Dial on Demand Routing) Route Policy Map (การกำหนดนโยบายเส้นทางของ BGP ที่ใช้ Prefix-List ซึ่งหลักการคล้ายคลึงกันกับ ACLs) การทำการการันตีคุณภาพในการให้บริการโดยขึ้นกับประเภทของทราฟฟิก (DiffServ QoS) รวมถึงการทำเนตเวิร์ค Address Translation (NAT) และยังเป็นกลไกการรักษาความปลอดภัยพื้นฐานของระบบเนตเวิร์ค

2.5.3 ภาพรวมของ ACLs

ACLs ที่ถูกคอนฟิกที่เราเตอร์นั้น จะทำการพิจารณาแพคเกตข้อมูลทุกๆ แพคเกตที่วิ่งผ่านและนำไปเปรียบเทียบกับ “กฎ” ที่ได้ตั้งไว้ใน ACLs ซึ่งการเปรียบเทียบ จะเป็นไปตามลำดับขั้น (Sequences) กล่าวคือ กฎแรกสุดหรือเรียกอย่างเป็นทางการว่า (Access Control Entry: ACE) จะถูกนำมาใช้งาน และหากว่าแพคเกตที่วิ่งเข้ามานั้นตรงตาม ACE จะยอมปล่อยผ่านทันทีและกฎข้อต่อๆมา จะไม่นำมาพิจารณาอีก ซึ่งได้ถูกนำมาเป็นระเบียบปฏิบัติข้อหนึ่งที่ว่า “ควรเซตกฎที่ชัดเจนที่สุดในการที่จะยอมปล่อยผ่าน หรือสกัดกั้นไว้ในกฎข้อแรกๆ” ส่วนในข้อต่อๆมาอาจจะมีความคลุมเครือ หรืออนุญาตแพคเกตใดๆ ก็ได้ ซึ่งหากแพคเกตนั้นๆ ตรวจสอบแล้วว่าไม่ตรงกับกฎใน ACE ข้อแรกจะวิ่งมาหากฎข้อต่อๆไป เรียงตามลำดับไปเรื่อยๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.6 การตรวจสอบของ ACLs กับแพคเกตที่วิ่งเข้ามาในเราเตอร์
(อ้างอิงโดย http://www.msit.mut.ac.th/newweb/phpfile/show.php?Qid=1124)

โดยค่าเริ่มต้นแล้วแพคเกตที่วิ่งผ่านเราเตอร์ที่ได้อิมพลีเมนต์ ACLs นี้นั้น หากแพคเกตนั้นๆ ไม่ตรง (Match) กับกฎข้อใดๆ ในกฎแล้วนั้น จะถูก "Explicit Deny All" ดรอปแพคเกตนั้นทิ้งทันที

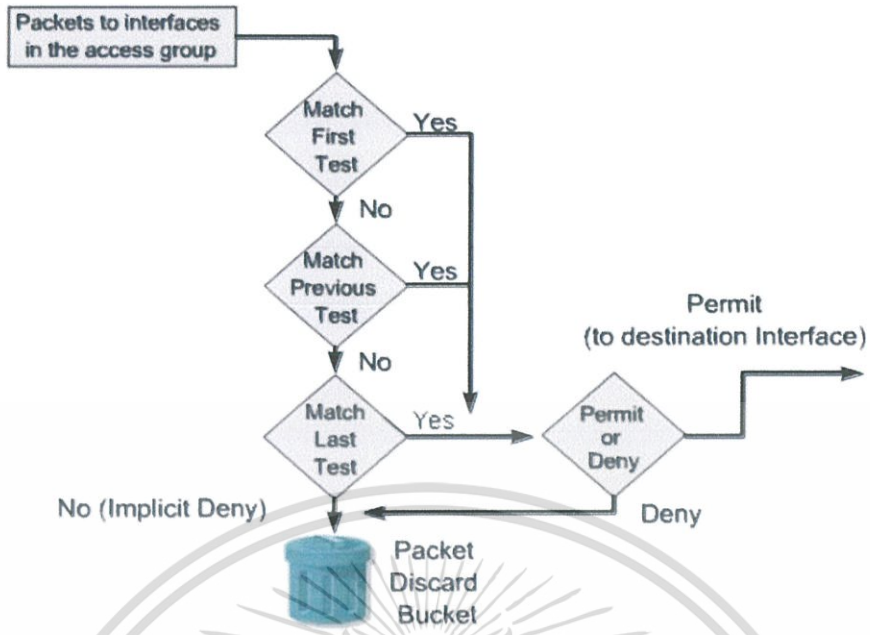
2.5.4 Explicit Deny All

ในกฎพื้นฐานที่สุดของไฟรวอลล์นั้น จะมี "การตั้งท่า (Stance)" ด้านความปลอดภัยภายในระบบเนตเวิร์คอยู่สองอย่างหลักๆ ได้แก่

อะไรที่ไม่ได้รับอนุญาตโดยจัดเจน จะถือว่าได้รับการปฏิเสธ
(หมายถึง Explicit Deny All หรือ หากไม่มีการตั้งกฎที่ Allow สิ่งใดๆ แล้ว จะถือว่า โดยดีฟอลท์นั้น Deny All ทั้งหมด)

อะไรที่ไม่ได้รับการปฏิเสธโดยชัดเจน จะถือว่าได้รับการอนุญาต
(หมายถึง Explicit Allow All หรือ หากไม่มีการตั้งกฎที่ Deny สิ่งใดๆ แล้ว จะถือว่า โดยดีฟอลท์นั้น Allow All ทั้งหมด)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.7 การตรวจสอบแพคเกตที่วิ่งเข้ามาในเราเตอร์จนกระทั่งถึง Explicit Deny All (อ้างอิงโดย http://www.msit.mut.ac.th/newweb/phpfile/show.php?Qid=1124)

2.5.5 Standard and Extended Access Lists

ในการตั้งกฎของ ACLs ในเราเตอร์นั้น สามารถตั้งได้สองรูปแบบคือ Standard Access Lists และ Extended Access Lists ดังนี้

2.5.5.1 Standard Access Lists

Standard Access Lists จะพิจารณา ACE ของแพคเกตจากไอพีแอดเดรสต้นทางเท่านั้น ซึ่งในการตั้งกฎของ ACLs นั้น จะต้องตั้งด้วยหมายเลข ACLs ในลำดับที่ 1-99 และ 1300-1399 เท่านั้น

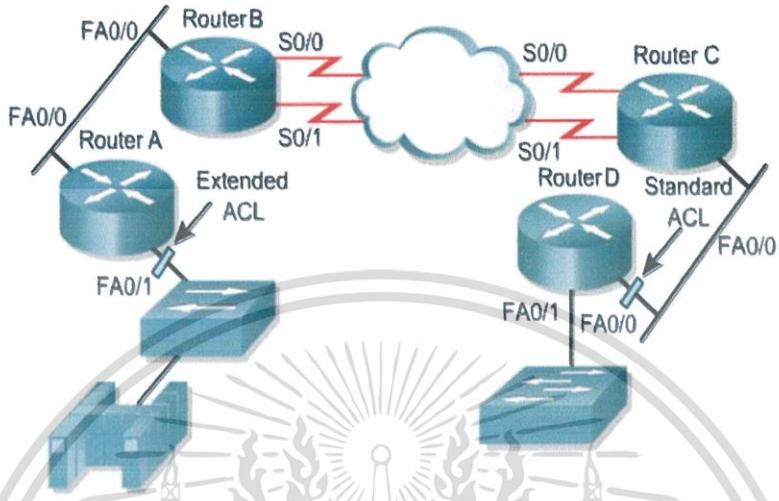
ในการตั้ง ACLs ของ Standard Access Lists ที่ดีควรจะ "ตั้งให้ใกล้กันกับปลายทางให้มากที่สุด" เนื่องจาก หากวาง ACLs นี้ใกล้ต้นทางมากเกินไป อาจจะกลายเป็นการบล็อกตัวเองได้ (เนื่องจากพิจารณาเพียงแค่ ไอพีแอดเดรสของต้นทางเท่านั้น)

2.5.5.2 Extended Access Lists

Extenced Access Lists จะพิจารณา ACE ของแพคเกตจากหมายเลขไอพีแอดเดรสของทั้งต้นทางและปลายทาง ผสมกับโปรโตคอลหรือพอร์ทต่างๆ ร่วมด้วย ซึ่งในการตั้งกฎของ ACLs แบบ Extended Access Lists นี้นั้น จะต้องตั้งด้วยหมายเลข ACLs ในลำดับที่ 100-199 และ 2000-2699 เท่านั้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในการตั้ง ACLs ของ Extended Access Lists ที่ดีควรจะ"ตั้งให้ไกล้กันกับต้นทางให้มากที่สุด" เนื่องจากหากวางACLs นี้ไกลต้นทางมากเกินไป จะทำให้ข้อมูลนั้น วิ่งไปบนเนตเวิร์คโดยเปล่าประโยชน์มากเกินไป



รูปที่ 2.8 ลักษณะการวางของ Access Control Lists ในแต่ละประเภท
(อ้างอิงโดย http://www.msit.mut.ac.th/newweb/phpfile/show.php?Qid=1124)

โดยปกติแล้ว จะอ้างอิงถึง ACLs ต่างๆ ผ่านทางหมายเลขแต่จริงๆ แล้วสามารถที่จะตั้งชื่อหรือสตริงตัวอักษร (String) ให้กับ ACLs เพื่อใช้ในการอ้างอิงให้กับ ACLs นี้ได้อีกด้วย เรียกการตั้งชื่อในลักษณะนี้ว่า "Named Access Control Lists" ซึ่งจะได้กล่าวในอันดับถัดไป

2.5.6 ทิศทางของ ACLs

จะมีการบังคับใช้ ACLs ในสองทิศทางคือ Inbound และ Outbound ซึ่งความแตกต่างของทั้งสองอย่างนี้คือ

Inbound จะถูกใช้ในการรับแพคเกตขาเข้าของอินเทอร์เฟซของเราเตอร์

Outbound จะถูกใช้ในการรับแพคเกตขาออกของอินเทอร์เฟซของเราเตอร์

2.5.7 Wildcard Masks

เป็นการคำนวนเพื่อหา จำนวนบิทที่แมชท์ (Match) กันมากที่สุด ในการที่จะจำเพาะเจาะจงลงไปว่าโฮสต์ใดหรือเครือข่ายย่อยใดๆ ที่จะมีสิทธิ์ในเส้นทางการส่งแพคเกตต่างๆ โดยที่มีการเปรียบเทียบดังต่อไปนี้

- ตำแหน่งบิทที่เป็น 0 หมายถึง "Care Bit" หรือ จำเป็นที่จะต้อง Match ในการเปรียบเทียบ Wildcard Masks

- ตำแหน่งบิทที่เป็น 1 หมายถึง "Don't Care Bit" หรือ ไม่จำเป็นที่จะต้อง Match ในการเปรียบเทียบ Wildcard Masks

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.5.8 หลักการและข้อควรจำเกี่ยวกับ Access Control Lists

บนอินเทอร์เฟซหนึ่งสามารถมี ACLs ได้เพียง 1 ทิศทาง(Inbound หรือ Outbound) และมีได้เพียง 1 Routed Protocol เท่านั้นเช่น ไอพี หรือ ไอพีเอ็กซ์ (IPX) ของ Netware เป็นต้น

เมื่อมีการเติมกฎ หรือ ACE เข้าไปยัง ACLs นั้น ACE ล่าสุด จะตกไปอยู่ลำดับ (Sequences) สุดท้ายสุดเสมอ ทำให้กฎที่ต้องการให้ฟิลเตอร์นี้อาจจะไม่ถูกใช้งานจริงๆ ก็เป็นได้ เนื่องจากกฎข้อแรกๆ ของ ACLs ที่ตรงมากกว่า อาจจะฟิลเตอร์ไปเรียบร้อยแล้ว

ในการแก้ไข ACE นั้นจำเป็นจะต้องลบ ACLs ชุดนั้นๆ ทิ้งก่อน แล้วจึงค่อยๆ ADD ACE ลงไปใน ACLs ทีละกฎ ดังนั้นจะเป็นการดีกว่า หากเราใช้ Text Editor ภายนอก (เช่น Notepad) ในการแก้ไข แล้วจึงนำมา Copy-Paste ลงใน เทอร์มินอลของเราเตอร์

2.6 ทฤษฎีเกี่ยวกับ EtherChannel

EtherChannel หรือที่เรียกว่า Link Aggregation นั้นเป็นคุณสมบัติที่ทำให้สามารถรวมหลาย ๆ อินเทอร์เฟสแบบ Physical เข้าด้วยกันเป็นอินเทอร์เฟสแบบ Logical เพียงอันเดียวได้ ใช้เพื่อแก้ปัญหาความคับคั่ง (Congestion) ในการใช้งานระบบเครือข่าย หรือใช้แก้ปัญหาเมื่อมีปริมาณการใช้งานระบบเครือข่ายมากเกินไปจนทำให้การรับ-ส่งข้อมูลทำได้ช้า เสมือนเป็นการเพิ่มเส้นทางข้อมูลขึ้น จากเส้นทางเดียวเป็นหลาย ๆ เส้นทาง เพื่อที่จะทำการ Shared Traffic ไปในหลาย ๆ เส้นทางนั่นเอง พร้อมทั้งยังเป็นการทำ Redundant ในกรณีที่มีบาง Link ที่เป็นสมาชิกของ EtherChannel เกิดมีปัญหาขึ้นมาได้อีกด้วย

2.6.1 การใช้งาน EtherChannel

สามารถใช้งานได้ทั้งบน สวิตช์ เราเตอร์ หรือ server ก็ได้ EtherChannel ไม่ได้เป็นการเพิ่ม Bandwidth นั้นก็เนื่องมาจาก ในการส่งข้อมูลไปยังอุปกรณ์ฝั่งตรงข้ามของ EtherChannel นั้น จะมีการเลือกเส้นทางที่จะใช้ส่งข้อมูลตามเงื่อนไขเพียงเส้นทางเดียวเท่านั้น เพราะฉะนั้น ถ้าแต่ละเส้นทางมี Bandwidth เท่ากับ 100 Mb เมื่อทำ EtherChannel โดยใช้ 2 Link แล้ว Bandwidth ก็ไม่ได้เพิ่มเป็น 200 Mb แต่อย่างใด (เนื่องจากในแต่ละ Link ก็ยังมี Bandwidth เท่ากับ 100 Mb เช่นเดิม) ในการที่จะใช้งาน EtherChannel ให้ได้เห็นผลลัพธ์อย่างชัดเจนนั้น จึงจะต้องใช้กับระบบเครือข่ายที่มีความคับคั่ง (Congestion) ที่ค่อนข้างสูง เพื่อที่จะได้ใช้ EtherChannel นี้ไปช่วยในการ Shared Load เพื่อลดค่า Congestion ลง ซึ่งถ้านำ EtherChannel ไปใช้กับเครือข่ายที่ไม่ได้มีการใช้งานในปริมาณที่มากแล้ว ก็อาจจะไม่เห็นความแตกต่างในการใช้งาน แต่ประโยชน์ของ EtherChannel นั้นยังมีมากกว่าการลดค่า Congestion ลง นั่นก็คือเป็นการสำรองเส้นทางระหว่างอุปกรณ์ที่ใช้ในการทำ EtherChannel ทั้งสองฝั่งนั่นเอง ถ้าเกิดกรณีที่ Link ใดมีปัญหาขึ้นมา ก็ยังมี Link อื่น ๆ ที่สามารถใช้ในการส่งข้อมูลต่อไปได้นั่นเอง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สำหรับเงื่อนไขที่นำมาใช้ในการตัดสินใจว่าจะส่งแพคเกตไปในเส้นทางใดนั้น สามารถเลือกได้จาก Mac Address ไอพีแอดเดรส หรือ หมายเลขพอร์ทLayer 4 และสามารถกำหนดได้ทั้ง Source, Destination หรือทั้ง Source และ Destination มาใช้ในการคำนวนเพื่อที่จะตัดสินใจว่าจะส่งแพคเกตไปในเส้นทางใดได้ โดยเมื่อทำการเลือกเงื่อนไขใดแล้วเงื่อนไขนั้นก็จะนำไปใช้กับทุก ๆ EtherChannel ที่มีการใช้งานอยู่บนสวิตช์ตัวนั้น และการที่จะเลือกว่าจะใช้เงื่อนไขใดก็ควรพิจารณาตามแต่ละสถานการณ์ไป เช่น ถ้าปลายทางที่จะส่งข้อมูลไปมีเพียงแห่งเดียว โดยอาจจะเป็น server เพียงตัวเดียว ก็จะมี Mac Address เดียว ถ้าใช้เงื่อนไข Destination Mac Address ในการพิจารณาแพคเกตก็จะถูกส่งไปในเส้นทางเดียวเสมอ ซึ่งถ้าใช้เงื่อนไข Source Mac Addrss ในการพิจารณาเลือกเส้นทางก็จะให้ผลลัพธ์ในการทำ Load Sharing ที่ดีกว่า (โดย Default สวิตช์จะพิจารณาเลือกเส้นทางจาก Source Mac Address)

เมื่อได้ทำการกำหนดเงื่อนไขแล้ว สวิตช์จะนำข้อมูลตามที่กำหนดในเงื่อนไขมาประมวลผลโดยใช้ Hash Algorithm ที่เป็นแบบเฉพาะของแต่ละโปรโตคอล เพื่อที่จะใช้ในการเลือกว่าจะส่งแพคเกตนี้ไปในอินเทอร์เฟสใดที่เป็นสมาชิกของ EtherChannel นี้ โดยผลลัพธ์ของการประมวลผลจะออกมาเป็นค่าตั้งแต่ 0 ถึง 7 นี่จึงเป็นเหตุผลที่ทำให้แต่ละ EtherChannel สามารถมีอินเทอร์เฟสที่เป็นสมาชิกได้สูงสุดเพียง 8 อินเทอร์เฟสเท่านั้น โดยในแต่ละอินเทอร์เฟสนั้นจะมีหน้าที่รับผิดชอบค่า Hash อย่างน้อย 1 ค่า คือถ้าใช้ EtherChannel 8 อินเทอร์เฟส แต่ละอินเทอร์เฟสก็จะรับผิดชอบค่า Hash ที่คำนวนออกมาอินเทอร์เฟสละ 1 ค่า แต่ถ้าใช้ EtherChannel 4 อินเทอร์เฟส แต่ละอินเทอร์เฟสก็จะรับผิดชอบค่า Hash อินเทอร์เฟสละ 2 ค่า เป็นต้น

Number of Ports in the EtherChannel	Load Balancing
8	1:1:1:1:1:1:1:1
7	2:1:1:1:1:1:1
6	2:2:1:1:1:1
5	2:2:2:1:1
4	2:2:2:2
3	3:3:2
2	4:4

รูปที่ 2.9 จำนวนของอินเทอร์เฟสและจำนวนของค่า Hash
(อ้างอิงโดย http://running-config.blogspot.com/2011/03/etherchannel-cisco-catalyst-switch.html)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 2.9 เป็นการแสดงจำนวนของอินเทอร์เฟสและจำนวนของค่า Hash ที่แต่ละอินเทอร์เฟสต้องรับผิดชอบ ซึ่งจะเห็นว่าในการที่จะทำ EtherChannel ให้ได้ประสิทธิภาพสูงสุดนั้นก็ควรที่จะใช้ 2 4 หรือ 8 อินเทอร์เฟส ในการทำ EtherChannel เนื่องจากจะทำให้แต่ละอินเทอร์เฟสมีหน้าที่รับผิดชอบค่า Hash ในจำนวนที่เท่าๆ กัน

อินเทอร์เฟส EtherChannel นั้น สามารถทำงานได้ทั้งในระดับ Layer 2 และ Layer 3 และจำนวนสูงสุดที่สามารถใช้งานอินเทอร์เฟส EhterChannel ได้นั้นก็ขึ้นอยู่กับสวิตช์ในแต่ละรุ่นไป

2.6.2 โปรโตคอลในการใช้งาน EtherChannel

PAgP – เป็น CISCO Proprietary อุปกรณ์ทั้ง 2 ฝั่งที่ทำการตั้งค่า EtherChannel จะต้องเป็นอุปกรณ์ CISCO ที่รองรับ PAgP เท่านั้น

LACP – เป็นมาตรฐาน IEEE 802.3ad Standard ซึ่งเป็นมาตรฐานของการทำ Link Aggregation โดย LACP จะสามารถสร้างได้อีก 8 พอร์ทเพิ่มเติม

และในการที่จะเลือกโปรโตคอลใดในการทำ EtherChannel นั้น ก็จะต้องไปทำการเลือกโหมดภายในแต่ละอินเทอร์เฟส โดยจะมีโหมดการทำงานให้เลือกดังนี้

Active (LACP) อินเทอร์เฟสที่ตั้งค่าในโหมดนี้จะเป็นฝ่ายเริ่มต้นเจรจาในการทำ EtherChannel แบบ LACP โดยอุปกรณ์ฝั่งตรงข้ามจะต้องทำงานในโหมด Active หรือ Passive เท่านั้น

Passive (LACP) อินเทอร์เฟสที่ตั้งค่าในโหมดนี้จะไม่เป็นฝ่ายเริ่มเจรจา แต่จะรอรับ LACP แพคเกตจากอุปกรณ์ฝั่งตรงข้าม เพื่อที่จะสร้าง EtherChannel ในแบบ LACP โดยอุปกรณ์ฝั่งตรงข้ามจะต้องทำงานในโหมด Active เท่านั้น

Desirable (PAgP) อินเทอร์เฟสที่ตั้งค่าในโหมดนี้จะเป็นฝ่ายเริ่มต้นเจรจาในการทำ EtherChannel แบบ PAgP โดยอุปกรณ์ฝั่งตรงข้ามจะต้องทำงานในโหมด Desirable หรือ Auto เท่านั้น

Auto (PAgP) อินเทอร์เฟสที่ตั้งค่าในโหมดนี้จะไม่เป็นฝ่ายเริ่มเจรจา แต่จะรอรับ PAgP แพคเกตจากอุปกรณ์ฝั่งตรงข้าม เพื่อที่จะสร้าง EtherChannel ในแบบ PAgP โดยอุปกรณ์ฝั่งตรงข้ามจะต้องทำงานในโหมด Desirable เท่านั้น

On เป็นการบังคับให้อินเทอร์เฟสนี้เป็น EtherChannel โดยไม่ต้องมีการเจรจาแลกเปลี่ยน PAgP และ LACP แพคเกตกัน โดยอุปกรณ์ฝั่งตรงข้ามจะต้องทำงานในโหมด on เท่านั้น ถ้าอยู่ในโหมดอื่น ๆ อินเทอร์เฟสของอุปกรณ์ฝั่งตรงข้ามจะอยู่ในสถานะ errdisable

Off เป็นการป้องกันไม่ให้มีการทำ EtherChannel ในอินเทอร์เฟสนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

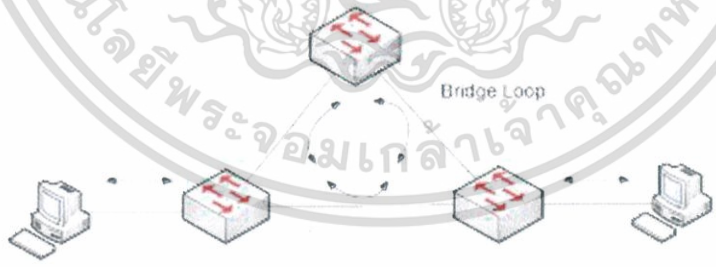
Switch Mode	Peer Mode	คำอธิบาย
active	active	เป็นค่าที่แนะนำสำหรับการใช้ EtherChannel แบบ LACP
active	passive	เป็น EtherChannel แบบ LACP ถ้าการเจรจาสำเร็จ
desirable	desirable	เป็นค่าที่แนะนำสำหรับการใช้ EtherChannel แบบ PAgP
desirable	auto	เป็น EtherChannel แบบ PAgP ถ้าการเจรจาสำเร็จ
on	on	เป็นการทำ EtherChannel โดยไม่ใช้ทั้ง LACP และ PAgP

รูปที่ 2.10 โหมดภายในแต่ละอินเทอร์เฟส

(อ้างอิงโดย http://running-config.blogspot.com/2011/03/etherchannel-cisco-catalyst-switch.html)

2.7 ทฤษฎีเกี่ยวกับ Spanning Tree

มีหน้าที่ช่วยป้องกันการเกิด Bridge loop และก็ช่วยเสริมให้มีเส้นทางสำรอง เช่น สมมุติว่ามีจุดหมายปลายทางอยู่จุดหนึ่งแล้วเส้นทางนี้เกิดมีปัญหาทำให้ระบบใช้งานไม่ได้เลย ก็ทำให้ระบบทั้งหมดมีปัญหาไปด้วย ตัว Spanning Tree ก็จะมีระบบช่วยป้องกันไม่ให้ระบบหยุดการทำงาน ถ้าเส้นทางหนึ่งมีปัญหาก็สามารถไปใช้เส้นทางอื่นได้ Redundancy ของ Spanning Tree ทำให้ระบบมีเสถียรภาพ เพราะใช้ตลอดเวลาก็ไม่มีปัญหา ถึงแม้เส้นทางใดเส้นทางหนึ่งใช้ไม่ได้ก็ตาม Spanning tree ก็จะมีเส้นทางขึ้นมาใช้แทนโดยรวมทำให้มีเสถียรภาพมากขึ้น



รูปที่ 2.11 การเกิดปัญหา Bridge Loop บนเนตเวิร์ค

(อ้างอิงโดย http://running-config.blogspot.com/2011/03/etherchannel-cisco-catalyst-switch.html)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.7.1 แนวคิดการแก้ปัญหา Bridge Loop บนสวิตช์

การใช้ Spanning Tree Protocol (STP) เป็นการป้องกันไม่ให้ทางสำรองย้อนกลับมากลายเป็นเส้นทางที่ทำให้เกิดลูปได้ โดยสถานกรณ์ปกติจะเป็นการบล๊อคบางพอร์ทของสวิตช์ไม่ให้ทำการรับส่งเฟรมได้ชั่วคราว จนกว่าจะมีการเปลี่ยนแปลงโครงสร้างเครือข่ายจะมีการคำนวณใหม่ว่าจะให้ยกเลิกการบล๊อคพอร์ท นั้นออกไปและให้พอร์ทดังกล่าวสามารถรับส่งเฟรมได้หรือไม่

2.7.2 หลักการทำงานของ Spanning Tree

STP เป็นมาตรฐาน IEEE802.1d ซึ่ง Spanning Tree Algorithm คือเริ่มจากการค้นหา Root Bridge (Root Switch) เพื่อทำหน้าที่เป็นศูนย์กลางหลักของ เนตเวิร์ค จากนั้นก็จะพิจารณาพอร์ทสวิตช์แต่ละตัวควรได้รับการเซตให้เป็น Forwarding state ส่วนพอร์ทนอกเหนือจะการถูกเลือกก็จะเป็นการบล๊อค state โดยอัตโนมัติ

2.7.3 กระบวนการทำงานของ Spanning Tree Protocol

2.7.3.1 การเลือก Root Bridge

STP เริ่มต้นด้วยการที่สวิตช์แต่ละอ้างว่าคือ Root Bridge ด้วยการส่ง Message ที่เรียกว่า BPDU (Bridge Protocol Data Unit) แลกเปลี่ยนกับสวิตช์ตัวอื่นๆ เพื่อ "เลือกตั้ง" กันว่าสวิตช์ตัวใดจะชนะการเลือกตั้ง (ใครมีคะแนนน้อยสุด) และได้รับการเลือกให้เป็น "Root Bridge" โดยภายใน BPDU จะมีฟิลด์สำคัญหนึ่งที่เรียกว่า Bridge ID ซึ่ง Bridge ID เป็นค่าตัวเลข 8 byte ที่ประกอบด้วยฟิลด์ดังนี้

- Bridge Priority (2 byte) เป็นค่าลำดับความสำคัญ (priority)ของสวิตช์นั้นเมื่อเทียบกับสวิตช์ตัวอื่น (มีค่าตั้งแต่ 0 - 65,535) by default คือ 32,768 (2^15)
- Mac address (6 byte) เป็น Mac address ประจำตัวสวิตช์เองขึ้นกับ สวิตช์แต่ละโมเดล ซึ่งจะ Hard code ไว้ภายในสวิตช์มาจากโรงงาน และไม่สามารถเปลี่ยนโดยผู้ใช้ได้

BPDU เป็น Frame ประเภทหนึ่งที่ สวิตช์/Bridge รับส่งกันเพื่อแลกเปลี่ยนข่าวสารต่างๆ ที่ใช้การคำนวณ SpanningTree Algorithm ประโยชน์อย่างหนึ่งที่เราได้ก็คือ การแลกเปลี่ยน BPDU กันเพื่อหา Root Bridge โดยพิจารณา จาก Bridge ID โดยปกติสวิตช์จะส่ง Frame นี้ออกไปทุกๆ พอร์ทที่รัน STP โดยเฟรมที่ว่านี้จะมี Mac address ต้นทางเป็นหมายเลข Mac address ของพอร์ทนั้นๆ และหมายเลข Mac address ปลายทางเป็น Multicast address 01-80-c2-00-00-00 ซึ่งเป็น Multicast พิเศษที่รู้จักกันในหมู่ สวิตช์/Bridge ที่รัน STP ทั้งนี้เพื่อให้เฉพาะ สวิตช์/Bridge รับเอาไปประมวลผลต่อ โดยจุดประสงค์เพื่อหา Root Bridge/Root สวิตช์ ของ Layer 2 ใน Domain ปัจจุบัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

BPDU นั้นมีอยู่ด้วยกัน 2 ประเภท คือ

1. Configuration BPDU เป็น BPDU เพื่อใช้ในการคำนวณ STP

2. Topology Change Notification (TCN) BPDU เป็น BPDU ที่ใช้เพื่อประกาศให้สวิตช์/Bridge อื่นๆ ทราบถึงการเปลี่ยนแปลงโครงสร้างเครือข่าย

เมื่อเปิดสวิตช์ขึ้นมา สวิตช์แต่ละตัวจะทำการส่ง BPDU ออกไปโดยเซตฟิลด์ Root Bridge ID ให้เท่ากับค่า Bridge ID (เพื่ออ้างว่าคือ Root Bridge) และเซตฟิลด์ Sender Bridge ID เป็นค่า Bridge ID (เพื่อบอกให้รู้ถึงแหล่งที่มาของ BPDU นั้นๆ ว่าใครเป็นผู้ส่ง) สวิตช์แต่ละตัวเมื่อได้รับ BPDU เข้ามาทางพอร์ทใดๆ ก็ตามแต่ จะนำมาวิเคราะห์ดูว่ามี BPDU ไหนที่มีค่าฟิลด์ Bridge ID ที่ดีกว่า Bridge ID อื่นๆ ที่รู้จักหรือไม่ซึ่งค่า Bridge ID ที่ดี จะต้องมีค่าต่ำที่สุด

หากพบ BPDU ที่มีค่า Bridge ID ที่ดีกว่าจะแทนที่ฟิลด์ Root Bridge ID ในเฟรม BPDU ที่ประกาศออกไปด้วยค่า Bridge ID ที่อยู่ใน BPDU ที่ดีกว่านั้นๆ โดยที่ยังคงเซตค่าฟิลด์ Sender Bridge ID ให้เท่ากับค่า Bridge ID ปัจจุบันเหมือนเดิม ในไม่ช้าเร็วการเลือก Root Bridge ก็จะจบ และทุกๆ สวิตช์/Bridge ก็จะได้สวิตช์ที่มีค่า Bridge ID ที่ดีที่สุด (มีค่าต่ำสุด)หลังจากนั้นพอร์ททุกๆ พอร์ทบน Root Bridge จะได้รับการเซตให้เป็นพอร์ท Designated บน Segment นั้นๆ ไปโดยอัตโนมัติ

ในกรณีที่มี Root Bridge อยู่แล้ว หากมีการนำสวิตช์ตัวใหม่เพิ่มเข้ามาในเน็ตเวิร์คซึ่ง Bridge ID ของสวิตช์ตัวใหม่ก็จะถูกนำมาพิจารณาใหม่เมื่อครบช่วงเวลาทุกๆ 2 วินาทีที่มีการรับส่ง BPDU กัน

2.7.3.2 การเลือกพอร์ท Root

เมื่อได้ทำการเลือก Root Bridge แล้วต่อไปสวิตช์แต่ละตัวที่ไม่ใช่ Root Bridge ก็จะพิจารณาว่าในพอร์ททั้งหมด พอร์ทใดเป็นเส้นทางที่ใกล้ที่สุดหรือเร็วที่สุดในการเดินทางไปถึง Root Bridge พอร์ทนั้นจะเป็นพอร์ท Root ซึ่งมีได้เพียงพอร์ทเดียวเท่านั้นต่อสวิตช์ 1 ตัว ซึ่ง STP ใช้การพิจารณา "Root Path Cost" มาเป็นตัวสินใจว่าจะให้พอร์ทใดทำหน้าที่เป็นพอร์ท Root ซึ่งต้องมีค่า Cost น้อยที่สุดเมื่อเทียบกับพอร์ทอื่นๆ ซึ่งแต่ละ Link หรือ Connection ของสวิตช์จะมีค่า Path cost ประจำตัวอยู่

Path Cost เป็นค่าอัตราส่วนผกผันกับค่า Bandwidth ของ Link ซึ่งก็คือ Link ที่มี Bandwidth มาก จะมีค่า Path Cost ที่ต่ำและ Link ที่มี Bandwidth น้อยจะมีค่า Path cost ที่สูง ในการพิจารณาค่า "Root Path Cost" นั้นจะได้จากผลบวกของ Path Cost ทั้งหมดนับจาก Root Bridge จนถึงพอร์ทนั้นๆ บน Non-Root Bridge ปัจจุบัน (Cumulative path cost = ผลรวมสะสม)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขั้นตอนการได้มาซึ่ง Root Path Cost มีดังนี้

1. Root Bridge ส่ง BPDU ออกไปโดยเซตค่าฟิลด์ Root Path Cost ให้เท่ากับ 0 เพราะพอร์ทต่อโดยตรงกับ Root Bridge

2. เมื่อสวิตช์ตัวอื่นๆ ได้รับ BPDU จาก Root Bridge จะเพิ่มค่า Path Cost ของพอร์ทที่ชี้ไปยัง Root Bridge บวกเข้าไปในค่าฟิลด์ Root Path Cost ของเฟรม BPDU ที่ได้รับเข้ามา

3. จากนั้นสวิตช์ที่อยู่ติดกับ Root Bridge ก็จะส่งต่อไปยังสวิตช์ตัวอื่นๆ ไปเรื่อยๆ

4. ค่าฟิลด์ Root Path Cost จะได้รับการพวกเพิ่มทุกครั้งในขณะที่ได้รับ BPDU เข้ามาโดยแต่ละสวิตช์ที่อยู่ตามเส้นทาง

2.7.3.3 การเลือกพอร์ท Root

เมื่อมีการเลือก Root Bridge และพอร์ท Root เสร็จแล้ว ต่อไปต้องเลือกพอร์ทที่ทำหน้าที่เป็นพอร์ท Designated ประจำ Segment นั้นๆ เพื่อให้ Active นอกนั้นจะมี Status = การบล๊อค state หมด หลักการที่นำมาใช้เพื่อเลือกหาพอร์ท Designated ก็คือ การพิจารณาว่าพอร์ทไหนมี Root Path Cost ที่ดีกว่า เพราะว่าจะแสดงถึงความเร็วในการส่งข้อมูลมาถึง Root Bridge เมื่อเทียบกับพอร์ทอื่นๆ ใน Segment เดียวกัน

Spanning Tree Protocol จะมีเงื่อนไขในการเลือกพอร์ท Root และพอร์ท Designated ดังนี้

1. เลือกพอร์ทที่มี Root Path cost ต่ำที่สุดก่อน ถ้ามีค่าเท่ากันให้พิจารณาข้อถัดไป

2. สำหรับการเลือกพอร์ท Designated ระหว่างสวิตช์มากกว่าหนึ่งตัว ให้เลือกพอร์ทของสวิตช์ที่มี Bridge ID ต่ำที่สุด ส่วนการเลือกพอร์ท Root บนสวิตช์เดียวกันให้เลือกพอร์ทที่ชี้ไปยังสวิตช์ที่มีค่าของ Bridge ID ต่ำกว่า

3. เลือกพอร์ทที่มีค่าพอร์ท ID ต่ำที่สุด

2.8 ทฤษฎีเกี่ยวกับโปรโตคอลการหาเส้นทาง (Routing Protocol)

คือโปรโตคอลที่ใช้ในการแลกเปลี่ยนตารางการหาเส้นทางระหว่างอุปกรณ์เครือข่ายต่างๆที่ทำงานในระดับเน็ตเวิร์ค Layer (Layer 3) เช่น เราเตอร์ เพื่อให้อุปกรณ์เหล่านี้สามารถส่งข้อมูล (IP packet) ไปยังคอมพิวเตอร์ปลายทางได้อย่างถูกต้อง โดยที่ผู้ดูแลเครือข่ายไม่ต้องแก้ไขข้อมูล ตารางการหาเส้นทางของอุปกรณ์ต่างๆตลอดเวลา

2.8.1 ตารางการหาเส้นทาง (Routing table)

หน้าที่ของเราเตอร์นั้นคือ การส่งผ่านแพคเกตระหว่างเครือข่าย ถ้าเปรียบเทียบระบบเครือข่ายกับระบบไปรษณีย์เราเตอร์ก็เปรียบเสมือนที่ทำการไปรษณีย์ ดังนั้นเราเตอร์ต้องทราบข้อมูลเกี่ยวกับเครือข่ายต่างๆ เช่น เครือข่ายดังกล่าวสามารถส่งแพคเกตไปได้หรือไม่ ถ้าได้จะส่งไปทางใดได้บ้างเป็นต้น ข้อมูลเกี่ยวกับเส้นทางจะถูกเก็บไว้ในตาราง ซึ่งตารางนี้จะมีรายการของ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หมายเลขไอพีของเราเตอร์ต้องการจะส่งต่อแพคเกต จะใช้ข้อมูลในตารางนี้ในการตัดสินใจเลือกเส้นทาง

โดยทั่วไปแล้วในในตารางการหาเส้นทางจะประกอบด้วยส่วนต่างดังต่อไปนี้

- หมายเลขเครือข่าย (Netwrok ID) คือ หมายเลขไอพีหรือหมายเลขเครือข่ายของโฮสต์ปลายทาง
- เครือข่ายย่อยมาสคื (เครือข่ายย่อย mask) คือหมายเลขที่เราท์เตอร์จะใช้ แอนด์ (AND) กับหมายเลขไอพีของโฮสต์ปหลายทางเพื่อคำนวณหาหมายเลขเครือข่าย
- เกตเวย์ (Gateway) คือ หมายเลขไอพีของเราเตอร์ หรือเกตเวย์ที่สามารถส่งแพคเกตข้อมูลถึงเครือข่ายปลายทางได้
- อินเตอร์เฟส (Interface) คือ เน็ตเวิร์คอินเตอร์เฟสหรือเน็ตเวิร์คการ์ดของเราเตอร์ที่สามารถส่งข้อมูลถึงเกตเวย์ดังกล่างได้
- เมทริก (Metric) เป็นตัวเลขที่เป็นหน่วยวัดเกี่ยวกับความยากง่ายในการส่งแพคเกตไปยังเครือข่ายนั้น ส่วนใหญ่จะหมายถึง จำนวนฮ็อป (Hop) หรือ เราเตอร์ที่ต้องส่งแพคเกตผ่านก่อนที่จะถึงเครือข่ายปลายทาง

2.8.2 ประเภทของโปรโตคอลหาเส้นทาง

เราเตอร์จะใช้ข้อมูลที่อยู่ในตารางการหาเส้นทางสำหรับการส่งแพคเกตระหว่างเครือข่าย ส่วนเส้นทางที่จะถูกเลือกนั้นจะขึ้นอยู่กับอัลกอริทึมที่ใช้ ประเภทของโปรโตคอลการหาเส้นทางสามารถแบ่งได้หลายแบบ ขึ้นอยู่กับลักษณะการอัพเดตตารางการหาเส้นทางก็สามารถแบ่งออกได้ป็นสองประเภทคือ

1. โปรโตคอลการหาเส้นทางแบบคงที่หรือสแตติก (Static Routing Protocol)
2. โปรโตคอลการหาเส้นทางแบบเปลี่ยนแปลงได้หรือไดนามิก (Dynamic Routing Protocol)

2.8.2.1 โปรโตคอลการหาเส้นทางแบบคงที่หรือสแตติก (Static Routing Protocol)

คือ การเพิ่มเส้นทางในตารางการหาเส้นทางด้วยผู้ดูแลเนตเวิร์คเพื่อบอกให้เราเตอร์ทราบว่าถ้าต้องการจะส่งข้อมูลไปที่ที่อยู่เครือข่ายย่อยใดจะต้องส่งผ่านเราเตอร์ตัวไหน ค่าที่ถูกป้อนเข้าไปในตารางเลือกเส้นทางนี้มีค่าที่ตายตัว ดังนั้นการเปลี่ยนแปลงที่เกิดขึ้นใดๆ บนเครือข่ายจะต้องให้ผู้ดูแลเนตเวิร์ค เข้ามาจัดการทั้งหมดซึ่งเหมาะสาหรับเครือข่ายที่มีขนาดเล็ก รักษาความปลอดภัยข้อมูล เนื่องจากสามารถแน่ใจว่าข้อมูลข่าวสารจะต้องวิ่งไปบนเส้นทางที่กำหนดไว้ให้ตายตัว ไม่ต้องใช้ซอฟต์แวร์เลือกเส้นทางใดๆทั้งสิ้นและช่วยประหยัดการใช้ bandwidth ของเครือข่ายลงได้มาก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.8.2.2 โปรโตคอลการหาเส้นทางแบบเปลี่ยนแปลงได้หรือไดนามิก (Dynamic Routing Protocol)

คือ ซอฟต์แวร์ที่ติดตั้งมากับเราเตอร์ เพื่อทำหน้าที่แลกเปลี่ยนข้อมูลข่าวสารที่เกี่ยวกับการเลือกเส้นทางระหว่างเราเตอร์ หลักการทำงานคือเราเตอร์จะส่งตารางการหาเส้นทางที่สมบูรณ์ให้กับเราเตอร์เพื่อนบ้าน เรียกว่ามีโปรโตคอลหาเส้นทางที่ใช้ในการแลกเปลี่ยน ตารางการหาเส้นทางโดยที่ผู้ดูแลเครือข่ายไม่ต้องแก้ไขข้อมูลตารางการหาเส้นทางในเราเตอร์เลย เหมาะสำหรับเครือข่ายขนาดใหญ่เพราะเราเตอร์ สามารถจัดการหาเส้นทางเองหากมีการเปลี่ยนแปลงของเครือข่ายเกิดขึ้น โดยโปรโตคอลหาเส้นทางจะมี Distance Vector และ Link State ซึ่งโปรโตคอลหาเส้นทางทั้งสองประเภทจะมีจุดประสงค์ที่เหมือนกันก็คือ การทำให้เราเตอร์ปัจจุบันมีตารางการหาเส้นทางที่ประกอบด้วยเส้นทางที่ดีที่สุดที่สามารถส่งข้อมูลไปถึงซับเนตแอดเดรสปลายทางทั้งหมดได้ แต่สิ่งที่แตกต่างกันก็คือวิธีการที่จะทำให้จุดประสงค์ข้างต้นลุล่วงไปได้

2.8.2.2.1 Distance Vector

คือการที่เราเตอร์เรียนรู้โครงสร้างเนตเวิร์คและที่อยู่เครือข่ายย่อยปลายทางต่างๆ โดยอาศัยการแลกเปลี่ยนตารางการหาเส้นทางกับตารางการหาเส้นทางของเพื่อนบ้าน เพื่อที่จะได้เรียนรู้ว่าเราเตอร์เพื่อนบ้านของรู้จักกับที่อยู่เครือข่ายย่อยอะไรบ้าง เพื่อที่จะอัพเดตตารางการหาเส้นทางว่า ถ้ามีแพคเกตที่มีแอดเดรสปลายทางเป็นที่อยู่เครือข่ายย่อยที่เราเตอร์เพื่อนบ้านรู้จักก็จะส่งต่อแพคเกตนั้นไปให้เราเตอร์เพื่อนบ้านตัวดังกล่าวเลย ซึ่งตัวอย่างโปรโตคอลประเภทนี้ได้แก่ โปรโตคอลหาเส้นทางที่ชื่อ RIP (Routing Information Protocol)

2.8.2.2.2 Link State

สำหรับ link State เราเตอร์จะส่งข้อมูลอินเตอร์เฟสทั้งหมดไปให้กับเราเตอร์เพื่อนบ้าน เพื่อให้เราเตอร์เพื่อนบ้านคำนวนหาเส้นทางที่ดีที่สุดเอง เราเตอร์จะไม่รู้จักแค่เราเตอร์เพื่อนบ้านแต่จะรู้จักเราเตอร์ข้างเคียงด้วยทำให้เราเตอร์สามารถเห็นภาพรวมทั้งหมดของเนตเวิร์คเป็นอย่างดีซึ่งข้อแตกต่างสำคัญของของ Distance Vector กับ link State คือ Distance Vector จะเชื่อเราเตอร์เพื่อนบ้านเป็นหลัก เพื่อนบ้านอัพเดตข้อมูลใดมาก็จะอัพเดตตารางการหาเส้นทางตาม แต่ถ้าเป็น link state เราเตอร์จะพยายามหาแผนผังของเครือข่ายทั้งหมดด้วยตนเองก่อนแล้วค่อยมาหาเส้นทาที่ดีที่สุดภายหลัง ซึ่งตัวอย่างโปรโตคอลประเภทนี้ได้แก่ โปรโตคอลหาเส้นทางที่ชื่อ OSPF (Open shortest part test)

2.8.3 OSPF (Open Shortest Part First)

OSPF (Open Shortest Path First) เป็นโปรโตคอลเราเตอร์ใช้ภายในเครือระบบอัตโนมัติที่นิยมใช้ Routing Information Protocol และโปรโตคอลเราเตอร์ที่เก่ากว่าที่มีการติดตั้งในระบบเครือข่าย OSPF ได้รับการออแบบโดย Internet Engineering Task Force (IETF) เหมือนกับ RIP ในฐานะของ interior gateway protocol

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การใช้ OSPF จะทำให้โฮสต์ที่ให้การเปลี่ยนไปยังตารางการหาเส้นทางหรือปกป้องการเปลี่ยนในเครือข่ายทันที multicast สารสนเทศไปยังโฮสต์ในเครือข่าย เพื่อทำให้มีสารสนเทศในตารางการหาเส้นทางเดียวกัน แต่ต่างจาก RIP เมื่อตารางการหาเส้นทางมีการส่งโฮสต์ใช้ OSPF ส่งเฉพาะส่วนที่มีการเปลี่ยน ในขณะที่ RIP ตารางการหาเส้นทางมีการส่งโฮสต์ใกล้เคียงทุก 30 วินาที OSPE จะ multicast สารสนเทศที่ปรับปรุงเฉพาะ เมื่อมีการเปลี่ยนแปลงเกิดขึ้น

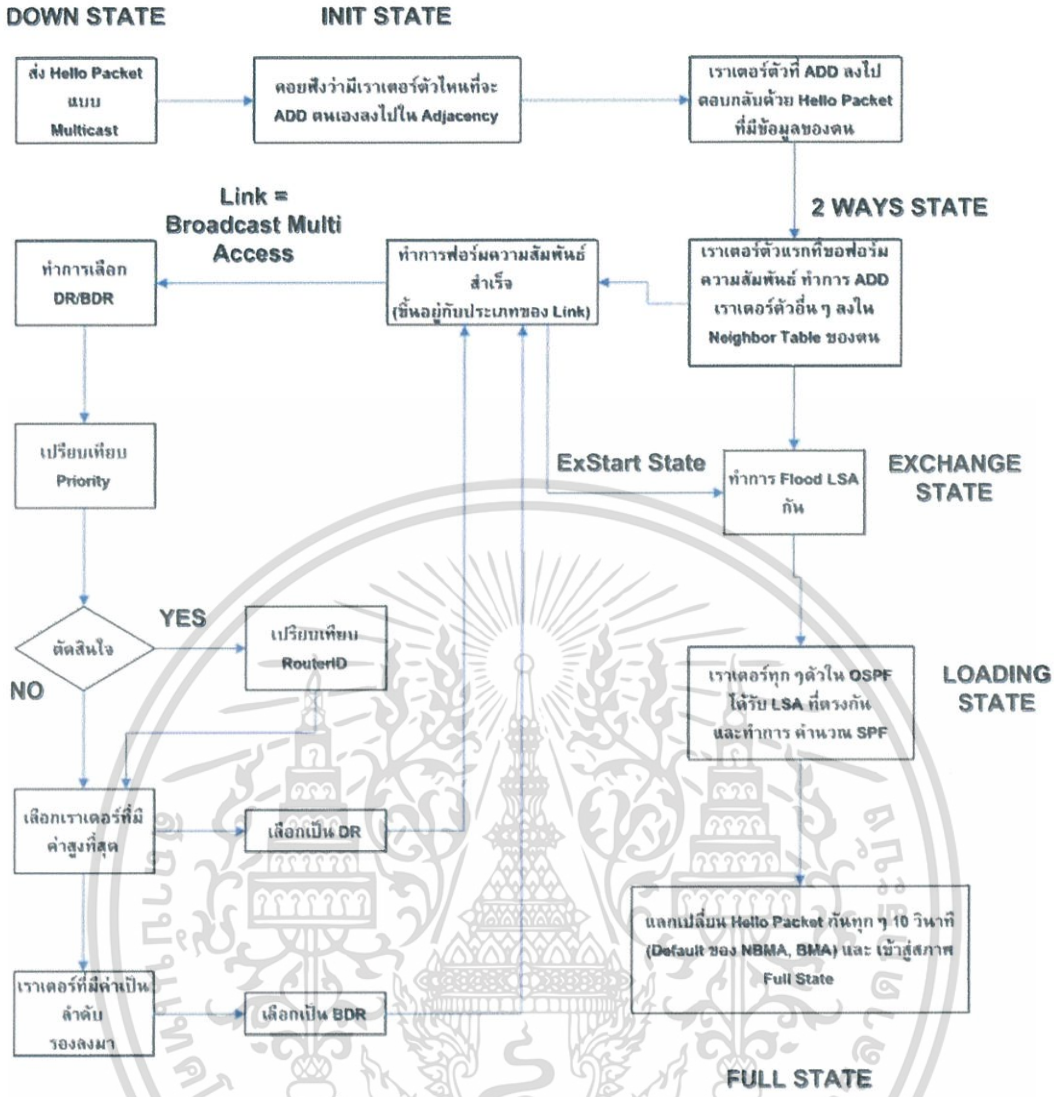
OSPF ไม่ใช้การนับจำนวนของ hop แต่ใช้เส้นทางตามรายละเอียด "line state" ที่เป็นส่วนสำคัญเพิ่มขึ้น ในสารสนเทศของเครือข่าย OSPF ให้ผู้ใช้กำหนด cost metric เพื่อให้โฮสต์ของเราเตอร์กำหนดเส้นทางที่พอใจ OSPF สนับสนุนเครือข่ายย่อย mask ของเครือข่าย ทำให้เครือข่ายสามารถแบ่งย่อยลงไป RIP สนับสนุนภายใน OSPF สำหรับเราเตอร์-to-end ของสถานีการสื่อสาร เนื่องจากเครือข่ายจำนวนมากใช้ RIP ผู้ผลิตเราเตอร์มีแนวโน้มสนับสนุน RIP ส่วนการออกแบบหลักคือ OSPF

2.8.3.1 OSPF Operation

กระบวนการของ OSPF จะเกิดขึ้นตามลำดับต่อไปนี้

1. ค้นหาเราเตอร์ที่รัน OSPF และฟอร์มความสัมพันธ์ด้วยแพคเกต Hello
2. เราเตอร์ต่างเก็บชื่อและสถานะของ Link ไว้ที่ Neighbor Table
3. เลือก DR/BDR (หากเป็น Point-to-Point, Point-to-Multipoint จุดนี้จะถูกข้ามไป)
4. ทำการ Flood LSA เพื่อแลกเปลี่ยนสถานะของ Link และ Interface โดยทำการ Copy LSA และทำการเพิ่มสถานะ จากนั้น Flood ออกไปยัง DR ที่ Multicast Address 224.0.0.6 และให้ DR เป็นผู้ Flood LSA ต่อไปยังเราเตอร์ทุกๆตัวที่ Multicast Address 224.0.0.5
5. Copy LSA ลงไปใน ตารางโครงสร้าง
6. ทำการคำนวณ Shortest Path First ด้วย Diijkstra Algorithms
7. นำเส้นทางที่สั้นที่สุดมาใส่ลงใน Routing Table
8. หากมีการเปลี่ยนแปลงโครงสร้างในระบบ จะทำการ Flood LSA ออกไปทันที (Triggered Update)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.12 แสดงลำดับการทำงานของ OSPF

(อ้างอิงโดย http://www.msit.mut.ac.th/newweb/phpfile/show.php?Qid=883)

2.8.3.2 SPF Calculation

ใน OSPF จะใช้อัลกอรึทึมของ Diijkstra (Link State) ในการคำนวณหาเส้นทางที่สั้นที่สุด โดยพิจารณาจากเส้นทางที่สั้นที่จุดจากจุดหนึ่งไปยังอีกจุดหนึ่ง และเมื่อไปถึงปลายทางแล้ว ก็จะทำ Cumulative Cost หรือ ค่าของ link หรือ bandwidth โดยรวมมาเปรียบเทียบกัน ซึ่งหากว่า เส้นทางใดที่มองจากต้นทางไปยังปลายแล้ว มีค่า Cost ที่ดีที่สุด จะถือว่าเส้นทางนั้นเป็นเส้นทางที่ Shortest Path ซึ่งใน CISCO เราเตอร์นั้น

ซึ่งการค้นหาเส้นทางที่สั้นที่สุด ก็จะนำเอา Cost ของจากขาออกของอินเทอร์เฟซจุดหนึ่งไปถึงอีกอินเทอร์เฟซจุดหนึ่งมาบวกต่อๆ กัน จนกระทั่งถึงอินเทอร์เฟซของเราเตอร์ปลายทาง และนำมาเปรียบเทียบกันกับเส้นทางอื่นๆ เรียกผลรวมในลักษณะนี้ว่า “Cumulative Cost”

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

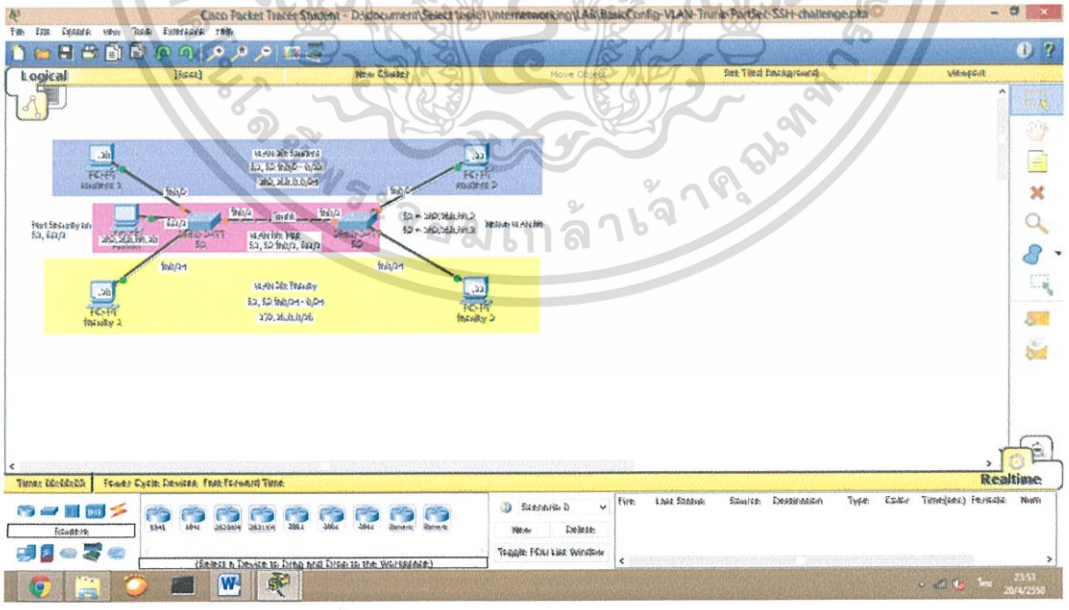
ตารางที่ 2.3 ค่า Cost บน Interface ที่มีผลในการคำนวณ Cumulative Cost

อินเทอร์เฟซและแบนด์วิดธ์	ค่า Cost ของ OSPF
Ethernet 10 Mbps	10
FastEthernet 100 Mbps	1
Serial T1 (1.544 Mbps)	64
Serial 128 Kbps	781
Serial 64 Kbps	1562

2.9 โปรแกรมที่ใช้ในการจำลองระบบเครือข่าย

2.9.1 CISCO PACKET TRACER

เป็นโปรแกรมจำลองการทำงานของอุปกรณ์จริงในระบบเครือข่ายของบริษัท CISCO ซึ่งสามารถจำลองการทำงานของ เราเตอร์ สวิตช์ Access point Hub PC หรือ server รวมไปถึงการเชื่อมต่อแบบต่างๆ เช่น Ethernet Serial หรือ Wireless เป็นต้น ซึ่งผู้ใช้งานสามารถที่จะเชื่อมต่ออุปกรณ์ต่างๆเข้าด้วยกันได้ค่อนข้างง่าย ไม่ซับซ้อน โปรแกรมนี้จึงเหมาะสมสำหรับผู้ที่เริ่มต้นศึกษาหรือเริ่มทำงานทางด้านเครือข่าย และเหมาะเป็นอย่างยิ่งสำหรับผู้ที่ต้องการเตรียมตัวสอบประกาศนียบัตรของ CISCO ในระดับ Associate (CCNA) และครอบคลุมไปจนถึงระดับ Professional ในบางหัวข้อ



รูปที่ 2.13 โปรแกรม Cisco Packet Tracer

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3
การวิเคราะห์และออกแบบระบบ

3.1 การออกแบบโครงสร้างระบบเครือข่าย (Network) ภายในสถานี

ในส่วนของโครงสร้างระบบเครือข่ายภายในสถานีจะประกอบด้วยระบบย่อยต่างๆ ทำให้อุปกรณ์และการตั้งค่าต่างๆ ในแต่ละส่วนแตกต่างกันออกไปเพื่อให้เหมาะสมแก่การทำงานในส่วนนั้นๆ

3.1.1 ระบบเครือข่ายย่อยของระบบต่างๆ

3.1.1.1 ระบบกล้องวงจรปิด(Closed Circuit Television : CCTV)

ระบบการบันทึกภาพเคลื่อนไหวด้วยกล้องวงจรปิด ซึ่งเป็นระบบสำหรับการใช้เพื่อการรักษาความปลอดภัย หรือใช้เพื่อการสอดส่องดูแลเหตุการณ์หรือสถานะการณ์ต่างๆ ที่นอกเหนือจากการรักษาความปลอดภัย โดยสามารถใช้ได้ทั้งสายนำสัญญาณแบบทั่วไป หรือสายใยแก้วในการส่งข้อมูล

3.1.1.2 ระบบการสื่อสารทางเสียงผ่านไอพี (Voice over IP: VoIP)

ระบบการสื่อสารทางเสียงผ่านโครงข่ายอินเทอร์เน็ต หรือโครงข่ายอื่นๆ ที่ใช้อินเทอร์เน็ตโพรโทคอล สัญญาณเสียงจะถูกตัดแบ่งเป็นแพ็คเก็ตวิ่งผ่านไปบนโครงข่ายที่ใช้สำหรับการสื่อสารข้อมูลทั่วไป แทนการใช้วงจรเฉพาะตามวิธีการสื่อสารในระบบโทรศัพท์แบบดั้งเดิม

ในการใช้บริการการสื่อสารทางเสียงผ่านไอพี ผู้ใช้บริการจะต้องเชื่อมต่อกับอินเทอร์เน็ตก่อน หลังจากนั้น สามารถใช้โปรแกรมคอมพิวเตอร์ที่เรียกว่า ซอฟท์โฟน และไมโครโฟนกับหูฟัง เพื่อพูดคุยกับปลายทางได้ ในปัจจุบัน มีอุปกรณ์ที่เรียกว่า อะนาล็อกเทเลโฟนอะแด็ปเตอร์ เข้ามาแทนการใช้คอมพิวเตอร์ ต่อกับอินเทอร์เน็ต และใช้เครื่องโทรศัพท์อะนาล็อกที่ใช้งานตามบ้านหรือสำนักงานทั่วไปในการโทรศัพท์แบบการสื่อสารทางเสียงผ่านไอพีได้ ทำให้ได้รับความสะดวก และความรู้สึกไม่แตกต่างจากการใช้โทรศัพท์แบบดั้งเดิม

การใช้งานการสื่อสารทางเสียงผ่านไอพี สามารถใช้งานได้ทั้งในการโทรศัพท์ถึงปลายทางที่เป็นการสื่อสารทางเสียงผ่านไอพีเช่นเดียวกัน ซึ่งส่วนใหญ่จะไม่มีการเก็บค่าบริการ แต่ทั้งสองข้างจะต้องออนไลน์พร้อมกัน หรือจะโทรไปยังปลายทางที่เป็นหมายเลขโทรศัพท์ปกติ ทั้งโทรศัพท์ประจำที่หรือโทรศัพท์เคลื่อนที่ก็ได้ ในกรณีนี้ จะต้องมีการสมัครเป็นสมาชิกของบริการและชำระค่าบริการล่วงหน้า แต่ค่าบริการจะถูกกว่าการโทรศัพท์ปกติมาก

3.1.1.3 ระบบสกาดา (Supervisory Control and Data Acquisition : SCADA)

ระบบส่วนกลางที่ตรวจสอบและควบคุมโดยรวมทั้งหมดหรือความสลับซับซ้อนของระบบที่กระจายออกไปในพื้นที่ขนาดใหญ่ ส่วนใหญ่การดำเนินการเพื่อควบคุมจะดำเนินการโดย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

อัตโนมัติโดย RTUs หรือ PLCs ฟังก์ชันการควบคุมของแม่ข่ายมักจะถูกจำกัดแค่การแทรกแซงในระดับพื้นฐานหรือการแทรกแซงระดับกำกับดูแล ตัวอย่างเช่น PLC อาจควบคุมการไหลของน้ำหล่อเย็นผ่านส่วนใดๆของสถานี แต่ระบบ SCADA อาจอนุญาตให้ผู้ใช้งานในการเปลี่ยน set point (ในที่นี้คืออุณหภูมิ) สำหรับการไหลได้ และเปิดใช้งานเงื่อนไขการเตือนเช่นการขาดหายของการไหลหรืออุณหภูมิที่สูงเกินไป

3.1.1.4 ระบบข้อมูลผู้โดยสาร

ระบบที่คอยให้ข้อมูลต่างๆ กับผู้โดยสารผ่านทางจอ LED (Light-Emitting Diode) ซึ่งอาจจะทั้งตารางเดินรถ โฆษณา หรือประกาศต่างๆ

3.1.1.5 ระบบสำนักงาน

ระบบที่คอยจัดการอุปกรณ์ต่างๆภายในสำนักงาน ซึ่งอาจจะประกอบด้วย คอมพิวเตอร์ ปริ้นเตอร์ เซิฟเวอร์ ฯลฯ เพื่อให้สามารถติดต่อรับส่งข้อมูลถึงกันได้หมด

3.1.1.6 ระบบควบคุมความปลอดภัยการเข้าออก

ระบบควบคุมการผ่านเข้าออก คือระบบที่มีทำหน้าควบคุมการผ่านเข้าออกประตู และกำหนดสิทธิให้กับแต่ละบุคคล ว่าสามารถเข้าออกประตูใดได้บ้าง ภายในช่วงเวลาใด โดยการใช้บัตรสัมผัส, ใช้ลายนิ้วมือ, รหัสผ่าน หรือใช้ทั้ง 3 อย่างร่วมกัน

3.1.1.7 ระบบประชาสัมพันธ์

ระบบที่คอยกระจายเสียง เปนการนำเครื่องมือทางด้านอิเล็คทรอนิคสมาประยุกต ในการสื่อสารหรือถายทอดขาวสารไดไมวาจะเปนกลุมขนาดเล็กหรือขนาดใหญ โดยเฉพาะในขนาดของกลุมใหญๆ ซึ่งการสงขาวสารโดยวิธีปกติยอมกระทำไดลำบากมาก และไมประสบความสำเร็จ ดังนั้น จุดมุงหมายและบทบาทของระบบกระจายเสียงจึงไดนำมาใชในการถายทอดขาวสารให เกิดประสิทธิภาพและครอบคลุมพื้นที่ที่ตองการ

3.1.1.8 ระบบเครือข่ายไร้สารสาธารณะ

ระบบที่ช่วยให้ผู้โดยสามารถใช้อุปกรณ์อิเล็กทรอนิกส์ในการแลกเปลี่ยนข้อมูลหรือการเชื่อมต่ออินเทอร์เน็ตแบบไร้สายโดยใช้คลื่นวิทยุ

3.1.1.9 ระบบอาณัติสัญญาณรถไฟ

ระบบกลไก สัญญาณไฟ หรือระบบคอมพิวเตอร์ ในการเดินขบวนรถไฟเพื่อแจ้งให้พนักงานขับรถไฟทราบสภาพเส้นทางข้างหน้า และตัดสินใจที่จะหยุดรถ ชลอความเร็ว หรือบังคับทิศทาง ให้การเดินรถดำเนินไปได้อย่างปลอดภัย รวดเร็ว และมีประสิทธิภาพ โดยเฉพาะในการเดินรถสวนกันบนเส้นทางเดียว หรือการสับหลีกเพื่อให้รถไฟวิ่งสวนกันบริเวณสถานีรถไฟ หรือควบคุมรถไฟให้การเดินขบวนเป็นไปตามที่กำหนดไว้กรณีที่ใช้ระบบอาณัติสัญญาณแบบคอมพิวเตอร์

ระบบอาณัติสัญญาณรถไฟจะควบคุมและกำหนดทิศทางการเคลื่อนที่ และระยะเวลาในการเดินรถ ของขบวนรถที่อยู่บนทางร่วมเดียวกัน รวมทั้งการสับหลีกบริเวณสถานี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รถไฟ โดยการทำงานของอุปกรณ์ต่างๆ ในระบบ จะออกแบบให้ทำงานสัมพันธ์กัน เพื่อให้พนักงานขับรถไฟสามารถตัดสินใจเดินรถได้อย่างมั่นใจ

3.1.1.10 ระบบเวลา

ระบบที่คอยให้บริการข้อมูลเวลากับระบบต่างๆให้สามารถใช้ข้อมูลเวลาที่ถูกต้องและตรงกันทั้งหมด เพื่อการทำงานที่เที่ยงตรงและแม่นยำในทุกๆส่วนการทำงานทั้งสถานี

3.1.2 แบนด์วิดท์ (Bandwidth) ภายในสถานี

ข้อมูลที่ผ่านอุปกรณ์ต่างๆภายในสถานียังคงมีจำนวนไม่มากนั้นทำให้สามารถที่เลือกใช้สื่อในการส่งข้อมูลตามที่เหมาะสมในแต่ละส่วนได้ โดยแต่ละระบบต้องการแบนด์วิดท์ดังนี้

- ระบบกล้องวงจรปิด 1 Gbps
- ระบบการสื่อสารทางเสียงผ่านไอพี 100 Mbps
- ระบบสกาดา 100 Mbps
- ระบบข้อมูลผู้โดยสาร 100 Mbps
- ระบบสำนักงาน 100 Mbps
- ระบบควบคุมความปลอดภัยการเข้าออก 100 Mbps
- ระบบประชาสัมพันธ์ 100 Mbps
- ระบบเครือข่ายไร้สารสาธารณะ 2 Gbps
- ระบบอาณัติสัญญาณรถไฟ 100 Mbps
- ระบบเวลา 100 Mbps

ทำให้ในส่วนของ สวิทช์หลัก (Main switch) ที่คอยรวมระบบต่างๆเข้าด้วยกัน แบนด์วิดท์จะต้องลองรับทุกระบบคือ 3.8 Gbps และทำการสำรองเข้าไปอีก 20% รวมเป็น 4.5 Gbps พร้อมทั้งทำการเชื่อมต่อสายไฟเบอร์ออฟติกเข้าไปเพิ่มอีก 1 เส้นทาง เพื่อป้องกันการเกิดปัญหาที่สื่อใดสื่อหนึ่งในเส้นทาง ดังรูปที่ 3.1

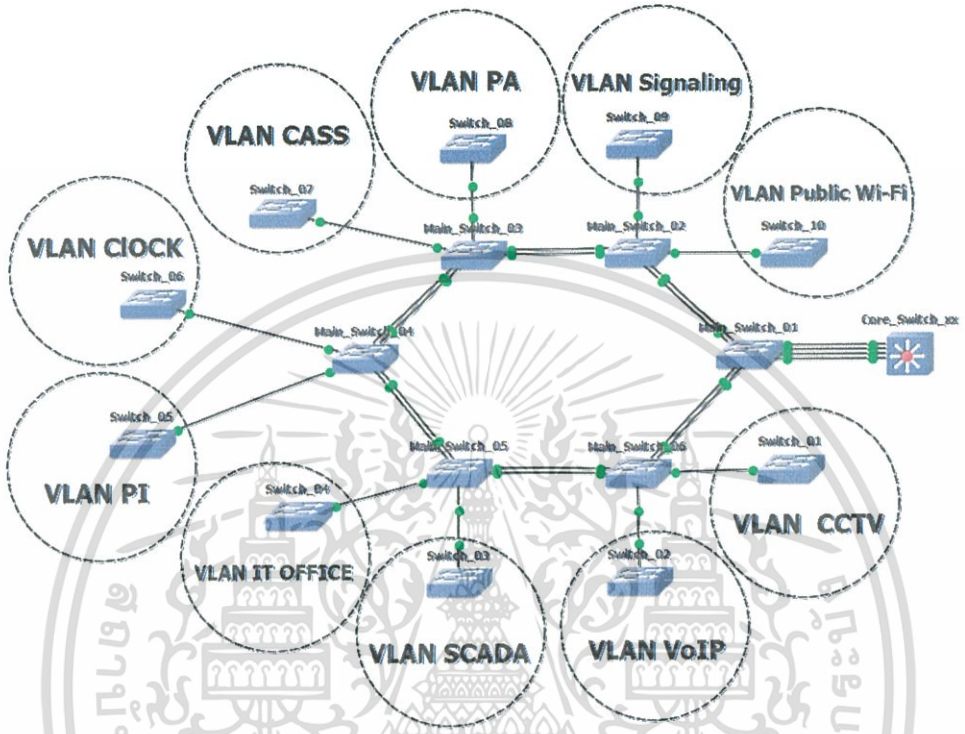
รูปที่ 3.1 การเชื่อมต่อสายไฟเบอร์ออฟติกระหว่างสวิทช์หลักภายในสถานี

3.1.3 การเชื่อมต่อระบบเครือข่ายกลางกับระบบเครือข่ายย่อยของระบบต่างๆ

โครงสร้างเครือข่ายที่เลือกใช้จะเป็นโครงสร้างเครือข่ายแบบวงแหวน (Ring Topology) เนื่องจากโครงสร้างเครือข่ายแบบวงแหวนนั้นสามารถที่จะรองรับการทำงานที่ต้องการในระบบขนส่งทางรางได้เหมาะสมที่สุด ซึ่งก็คือการที่โครงสร้างเครือข่ายแบบวงแหวนสามารถที่จะรองรับความแน่นอนในการส่งข้อมูลได้ว่าการส่งข้อมูลจะไปถึงปลายทางได้อย่างปลอดภัยที่สุด หรือก็คือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อเกิดปัญหาที่เส้นทางใดเส้นทางหนึ่งในการส่งข้อมูล โครงสร้างเครือข่ายแบบวงแหวนสามารถที่จะส่งข้อมูลไปยังอีกเส้นทางหนึ่งที่ได้ ทำให้ระบบทั้งหมดยังคงสามารถที่จะทำงานต่อไปได้ และมีเวลาพอที่จะให้ผู้เชี่ยวชาญเข้าไปซ่อมแซ่มระบบส่วนที่มีปัญหา



รูปที่ 3.2 โครงสร้างระบบเครือข่ายกลางภายในสถานี

3.2 การออกแบบโครงสร้างระบบเครือข่ายระหว่างสถานี

ในส่วนของโครงสร้างระบบเครือข่ายระหว่างสถานีจำเป็นต้องมีความสามารถรองรับการรับส่งของข้อมูลจำนวนมากที่จะส่งผ่านไปยังสถานีอื่นๆจึงเลือกใช้สาย Fiber Optic Single Mode แบบเดียวกับที่ใช้กับระบบเครือข่ายกลางภายในสถานี และต้องมีความสามารถที่จะค้นหาเส้นทาง (Routing) เพื่อไปยังปลายทางได้เช่นกัน จึงต้องเลือกใช้ สวิตช์ Layer 3

3.2.1 แบนด์วิดท์ระหว่างสถานี

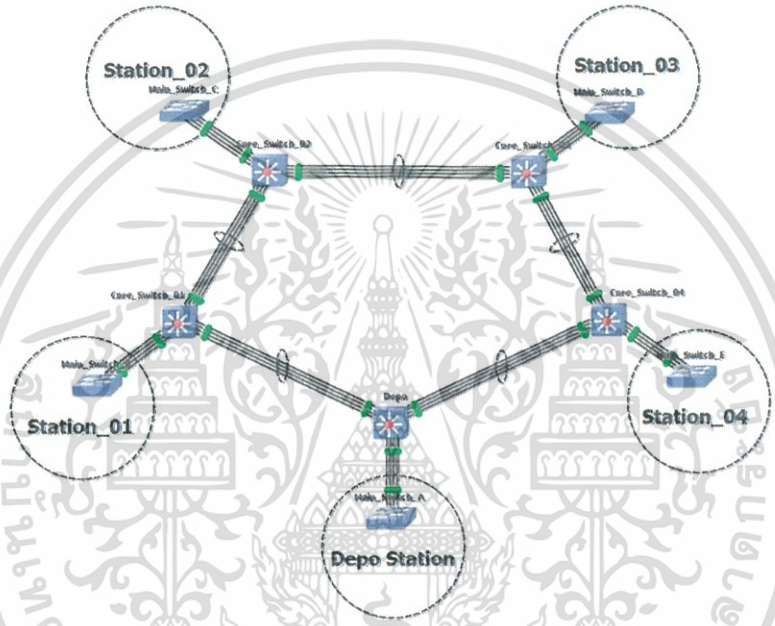
ข้อมูลที่ผ่านอุปกรณ์ระหว่างสถานีจะมีจำนวนที่มากกว่าอุปกรณ์ภายในสถานีมาก ทำให้ต้องมีสื่อที่รองรับการส่งข้อมูลมากขึ้น และต้องรองรับการเกิดปัญหาที่สื่อใดสื่อหนึ่งด้วยเช่นกัน โดยในที่นี้จะทำการเพิ่มสายไฟเบอร์ออฟติกเข้าไปอีก 1 เท่าตัวของการส่งข้อมูลภายในสถานี กลายเป็น 4 สายไฟเบอร์ออฟติก โดยแต่ละสายรองรับแบนด์วิดท์ 4.5 Gbps ดังรูปที่ 3.3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 3.3 การเชื่อมต่อสายไฟเบอร์ออฟติกระหว่างสวิทช์หลักระหว่างสถานี

3.2.2 การเชื่อมต่อระบบเครือข่ายกลางแต่ละสถานีเข้าด้วยกัน

เราจะทำการจำลองสถานีขึ้นมา 5 สถานีโดยที่ 1 ใน 5 สถานีนั้นจะทำหน้าที่เป็นสถานีใหญ่ด้วย และเป็นโครงสร้างเครือข่ายแบบวงแหวนเช่นกัน ดังรูปที่ 3.4



รูปที่ 3.4 โครงสร้างระบบเครือข่ายทั้งหมด

3.3 การออกแบบการแจก ไอพีแอดเดรส (IP address)

ไอพีแอดเดรสเป็นสิ่งจำเป็นในการระบุตัวตนของอุปกรณ์แต่ละชิ้น เพื่อใช้รู้ถึงต้นทางและปลายทางในการรับส่งข้อมูล โดยเราเตอร์จะทำหน้าที่เป็น DHCP (Dynamic Host Configuration Protocol) คอยแจกไอพีแอดเดรส ให้กับทุกอุปกรณ์ภายในสถานีที่ต้องการไอพีแอดเดรส โดยไอพีแอดเดรสที่แจกให้กับระบบนั้นจะเป็น ไอพีส่วนตัว (private IP) ซึ่งก็คือไอพีแอดเดรสที่ไม่สามารถนำมาใช้ติดต่อสื่อสารบนอินเตอร์เน็ตได้ สามารถใช้ติดต่อสื่อสารได้เฉพาะภายในกลุ่มเครื่องข่ายเท่านั้น โดยจะเลือกใช้ไอพีแอดเดรสในคลาส เอ เนื่องมาจากอุปกรณ์ทั้งหมดในขนส่งทางรางมีจำนวนมากและต้องมีการรองรับอุปกรณ์ต่างๆภายในอนาคตด้วย โดยไอพีแอดเดรสในคลาส เอ จะเริ่มต้นที่ 10.0.0.0 ถึง 10.255.255.255 ซึ่งมีทั้งหมด 16,777,216 เลขหมาย ซึ่งในแต่ละระบบจะมีการแจกไอพีแอดเดรสดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- ระบบกล้องวงจรปิด 10.x.0.0 - 10.x.1.255
- ระบบการสื่อสารทางเสียงผ่านไอพี 10.x.2.0 - 10.x.3.255
- ระบบสกาดา 10.x.4.0 - 10.x.5.255
- ระบบสำนักงาน 10.x.6.0 - 10.x.7.255
- ระบบข้อมูลผู้โดยสาร 10.x.8.0 - 10.x.9.255
- ระบบเวลา 10.x.10.0 - 10.x.11.255
- ระบบควบคุมความปลอดภัยการเข้าออก 10.x.12.0 - 10.x.13.255
- ระบบประชาสัมพันธ์ 10.x.14.0 - 10.x.15.255
- ระบบอาณัติสัญญาณรถไฟ 10.x.16.0 - 10.x.17.255
- ระบบเครือข่ายไร้สารสาธารณะ 10.x.18.0 - 10.x.19.255

โดยที่ x คือ หมายเลขสถานี

3.4 การออกแบบ VLAN (Virtual Local Area Network)

เนื่องจากความต้องการที่จะแยกแต่ละระบบออกเป็นคนละเน็ตเวิร์ค เราจึงนำ VLAN เข้ามาจัดการเพื่อให้สามารถที่จะสร้างเครือข่ายของระบบต่างๆ บนอุปกรณ์ตัวเดียวกันได้ โดยจะมีการกำหนดหมายเลข VLAN และ ชื่อของเน็ตเวิร์คตามระบบ ดังรูป

IOS Command Line Interface

```
Core_SW_Depo#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa2/1, Fa3/1, Fa4/1, Fa8/1
                                                Fa9/1
11   CCTV                             active
12   VOIP                             active
13   Office_IT                        active
14   Passenger                        active
15   CASS                             active
16   SCADA                            active
17   PAS                              active
18   Signaling                        active
19   Public_Wifi                      active
20   Clock                            active
29   Routing                          active    Fa0/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Core_SW_Depo#
Core_SW_Depo#
Core_SW_Depo#
Core_SW_Depo#
Core_SW_Depo#
```

รูปที่ 3.5 ลำดับ VLAN กับรายชื่อระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.5 การออกแบบโปรโตคอลการหาเส้นทาง (Routing Protocol)

เนื่องจากเป็นการหาเส้นทางเครือข่ายภายใน ดังนั้นเราจึงจะเลือกโปรโตคอลที่ใช้สำหรับการหาเส้นทางภายใน(Interior Routing Protocol) โดยโปรโตคอลที่จัดอยู่ในประเภทนี้อย่างเช่น RIP (Routing Information Protocol), IGRP (Interior Gateway Routing)และ OSPF (Open Shortest Path First) โดยโปรโตคอลทั้งสาม นั้นแบ่งได้เป็นสองกลุ่มคือ Distance Vector ซึ่งโปรโตคอลที่จัดอยู่ในกลุ่มนี้คือ RIP และ IGRP ส่วน Link State นั้นมีโปรโตคอลคือ OSPF โดยเป้าหมายของการหาเส้นทางในระบบนั้น จำเป็นต้องมีการปรับตัวของการเปลี่ยนแปลงโครงสร้างเครือข่ายคอมพิวเตอร์ที่ต้องมีความรวดเร็วที่สุด ซึ่งคุณสมบัติตรงนี้กลุ่มของ Link State นั้นมีประสิทธิภาพที่ดีกว่า Distance Vector ดังนั้นเราจึงเลือก ใช้โปรโตอลหาเส้นทาง กลุ่ม Link State ซึ่งโปรโตคอลนั้นคือ OSPF

3.6 การออกแบบ ACLs (Access Control Lists)

ความต้องการของระบบนั้นไม่ต้องการให้ระบบแต่ละระบบส่งข้อมูลหาถึงกันได้ แต่จะอนุญาตเพียงบางส่วนที่เข้าถึงได้ ซึ่งการพิจารณาแพคเกตข้อมูล (Package data) ที่วิ่งผ่านว่าเป็นไปตามกฎที่ได้ตั้งไว้ใน ACLs หรือเปล่า โดยสามารถทำได้ที่เราเตอร์ ซึ่งเป็นอุปกรณ์ที่ใช้ในกางหาเส้นทาง ซึ่งหากตรวจสอบแล้วว่าไม่ตรงเงื่อนไขที่ได้รับอนุญาต ก็จะไม่ส่งแพ็คเก็ตข้อมูลนั้นต่อไป

ซึ่งการทำงานของ ACLs นั้นก็คือดูว่าแพ็คเก็ตที่ส่งมานั้นมีไอพีที่ตรงกับ access group ไหนจากนั้นก็จะทำการพิจารณาว่าจะให้ผ่านหรือปฏิเสธ ดังนั้นเพื่อให้การทำงานมีประสิทธิภาพเราควรจะให้มีเงื่อนไขให้พิจารณาน้อย แต่ครอบคลุมมากที่สุด โดยเรากำหนดจะให้ VLAN แต่ละอันจะทำการอนุญาติ เฉพาะ VLAN ที่เป็นระบบเดียวกันในแต่ละสถานี และมีการอนุญาติพอร์ต 67 และ 68 สำหรับการทำ DHCP

```
Extended IP access list catv
    10 permit udp any any eq bootps
    20 permit udp any any eq bootpc
    30 permit ip 10.1.0.0 0.0.1.255 any
    40 permit ip 10.2.0.0 0.0.1.255 any
    50 permit ip 10.3.0.0 0.0.1.255 any
    60 permit ip 10.4.0.0 0.0.1.255 any
    70 permit ip 10.5.0.0 0.0.1.255 any
Extended IP access list voip
    10 permit udp any any eq bootps
    20 permit udp any any eq bootpc
    30 permit ip 10.1.2.0 0.0.1.255 any
    40 permit ip 10.2.2.0 0.0.1.255 any
    50 permit ip 10.3.2.0 0.0.1.255 any
    60 permit ip 10.4.2.0 0.0.1.255 any
    70 permit ip 10.5.2.0 0.0.1.255 any
Extended IP access list scada
    10 permit udp any any eq bootps
    20 permit udp any any eq bootpc
    30 permit ip 10.1.4.0 0.0.1.255 any
    40 permit ip 10.2.4.0 0.0.1.255 any
    50 permit ip 10.3.4.0 0.0.1.255 any
```

รูปที่ 3.6 ค่าของ access group

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

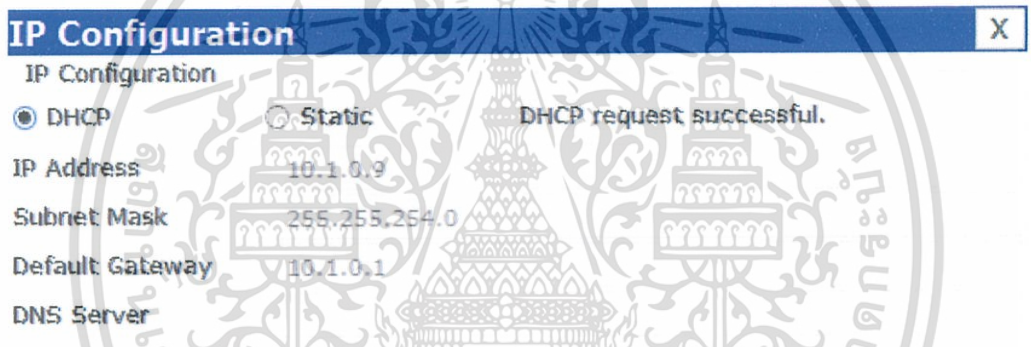
บทที่ 4
ผลการทดลอง

ในหัวข้อนี้จะกล่าวถึงรายละเอียดผลการทดลองของระบบเครือข่ายการสื่อสารที่ได้ทำการตั้งค่าไว้ โดยจะแบ่งการผลทดลองเป็น 5 ส่วนคือ

1. การทดลองการแจกไอพีโดย DHCP
2. การทดลอง Spanning Tree
3. การทดลอง Ether Channel
4. การทดลองโปรโตคอลหาเส้นทาง
5. การทดลอง Access Contorl Lists

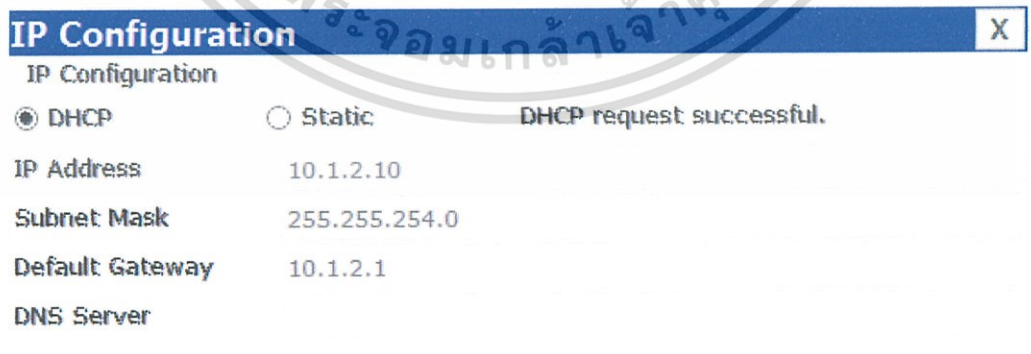
4.1 การทดลองการแจกไอพีแอดเดรสโดย DHCP

1. ระบบกล้องวงจรปิด (Closed Circuit Television : CCTV)



รูปที่ 4.1 ไอพีแอดเดรสของระบบกล้องวงจรปิด

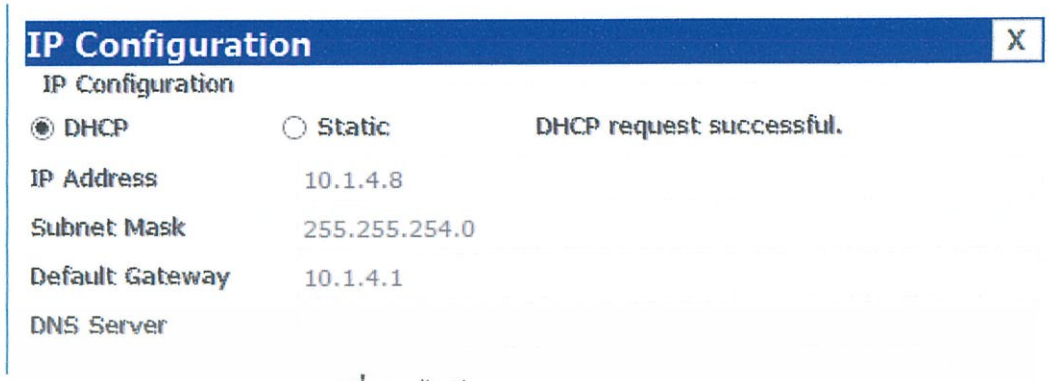
2. ระบบการสื่อสารทางเสียงผ่านไอพี (Voice over IP : VoIP)



รูปที่ 4.2 ไอพีแอดเดรสของระบบการสื่อสารทางเสียงผ่านไอพี

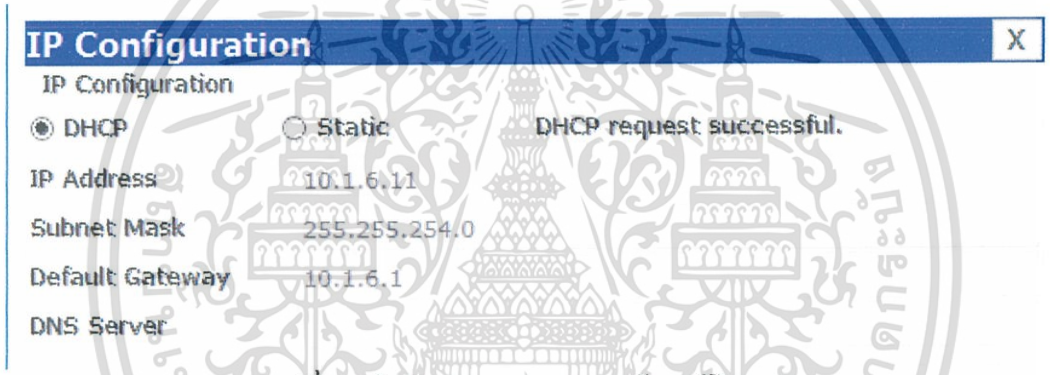
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. ระบบสกาดา (Supervisory Control and Data Acquisition : SCADA)



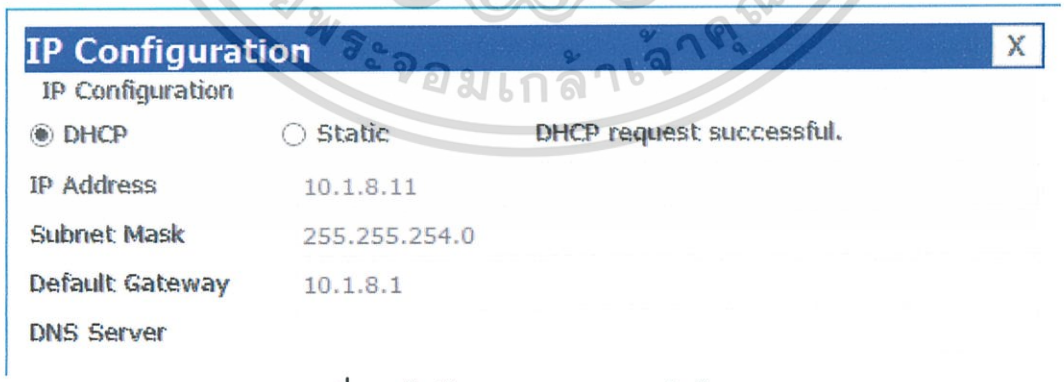
รูปที่ 4.3 ไอพีแอดเดรสของระบบสกาดา

4. ระบบข้อมูลผู้โดยสาร



รูปที่ 4.4 ไอพีแอดเดรสของระบบข้อมูลผู้โดยสาร

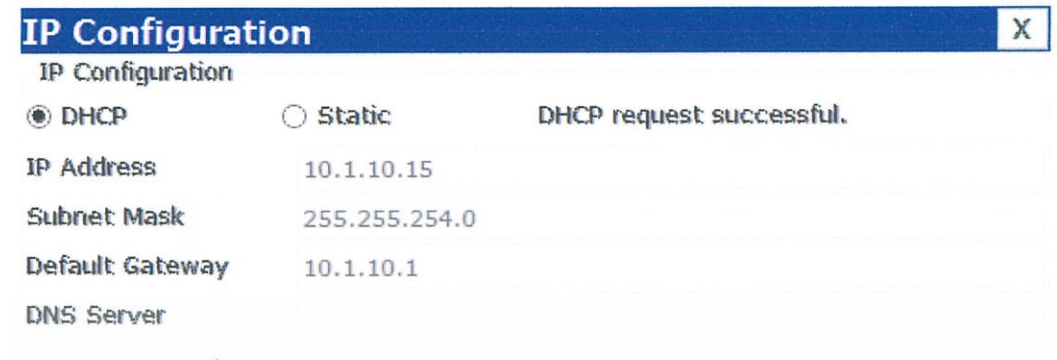
5. ระบบสำนักงาน



รูปที่ 4.5 ไอพีแอดเดรสของระบบสำนักงาน

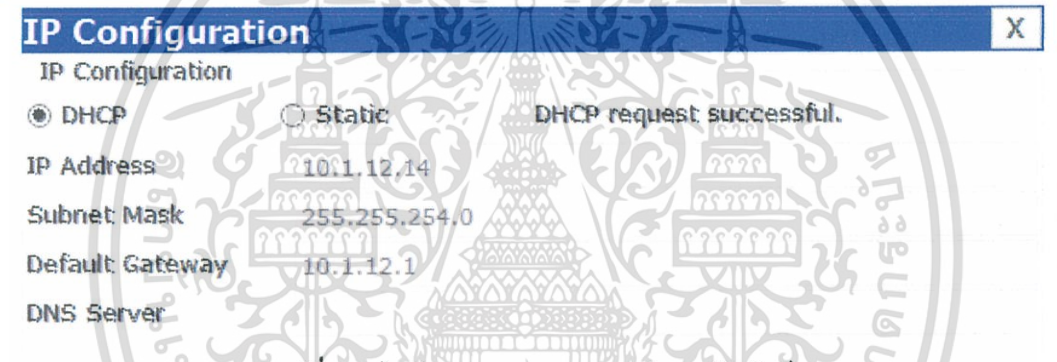
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6. ระบบควบคุมความปลอดภัยการเข้าออก



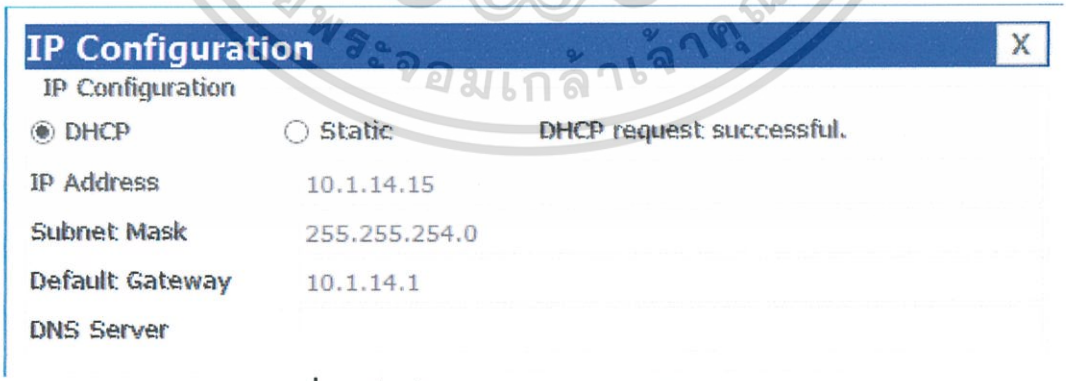
รูปที่ 4.6 ไอพีแอดเดรสของระบบควบคุมความปลอดภัยการเข้าออก

7. ระบบประชาสัมพันธ์



รูปที่ 4.7 ไอพีแอดเดรสของระบบประชาสัมพันธ์

8. ระบบเครือข่ายไร้สายสาธารณะ



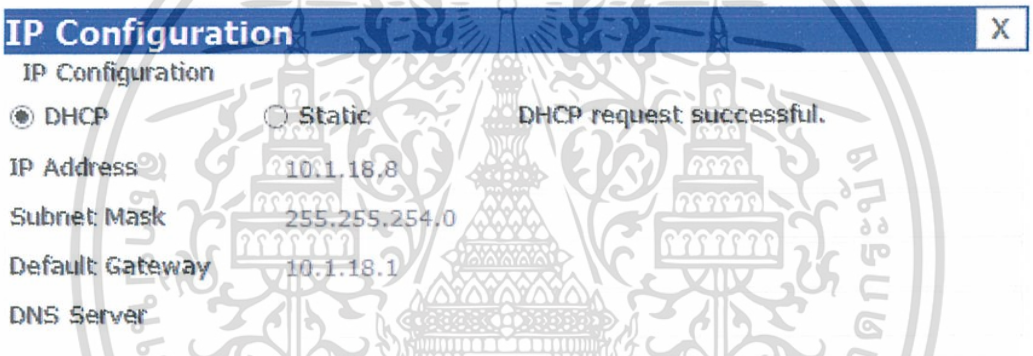
รูปที่ 4.8 ไอพีแอดเดรสของระบบ Wifi สาธารณะ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

9. ระบบอาณัติสัญญาณรถไฟ

รูปที่ 4.9 ไอพีแอดเดรสของระบบอาณัติสัญญาณรถไฟ

10. ระบบเวลา



รูปที่ 4.10 ไอพีแอดเดรสของระบบเวลา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

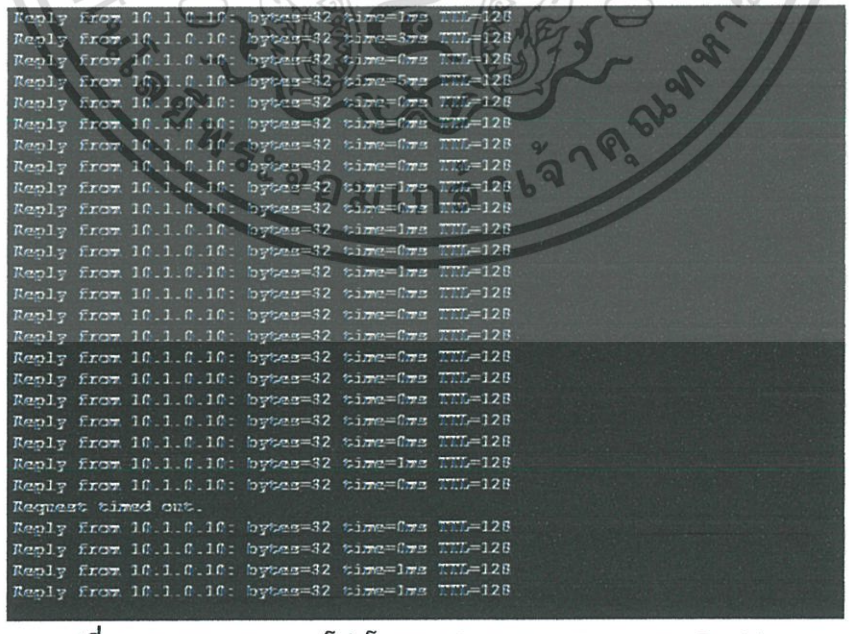
4.2 การทดลอง Spanning Tree

ในการนี้จะเป็นการทดสอบ Spanning Tree เพื่อดูความแตกต่างระหว่าง Spanning Tree แบบปกติและ Spaning Tree แบบ Rapid โดยเราจะใช้คำสั่ง ping ในการทดสอบโดยดูว่าหากระบบมีปัญหา จะเพื่อสังเกตุการเกิดการสูญหายของ Packet

4.2.1 การใช้โปรโตคอล Spanning Tree แบบปกติ

รูปที่ 4.11 ผลการทดลองโปรโตคอล Spanning Tree แบบปกติ

4.2.2 การใช้โปรโตคอล Spanning Tree แบบ Rapid

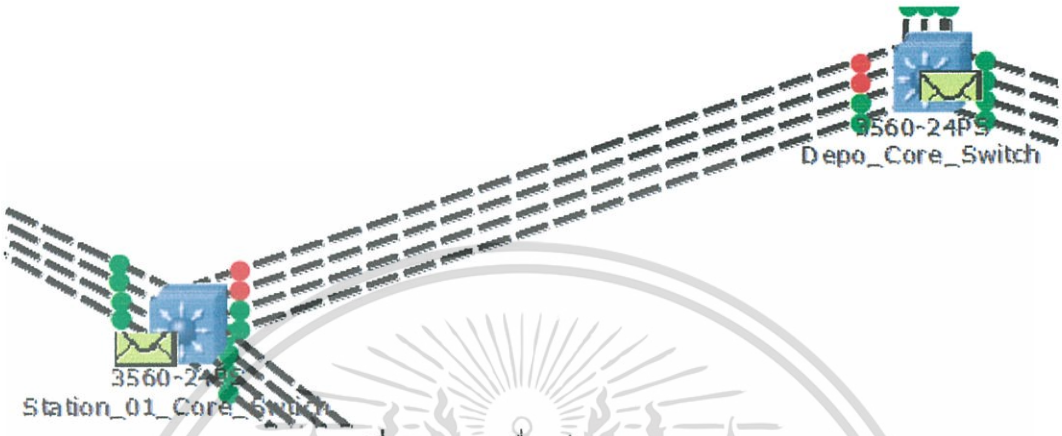


รูปที่ 4.12 ผลการทดลองโปรโตคอล Spanning Tree แบบ Rapid

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

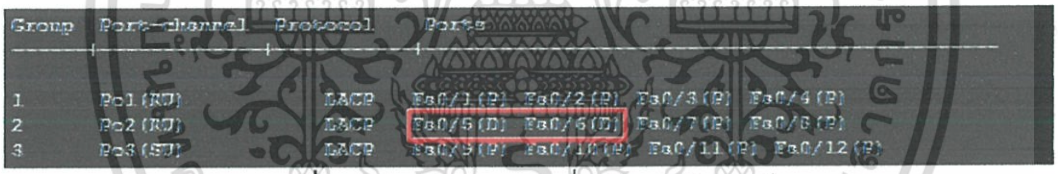
4.3 การทดลอง Ether Channel

Ether Channel คือการทำให้สายที่เชื่อมต่อหลายๆเส้น ระหว่างสวิตช์สองตัวที่เชื่อมเข้าหากันมองเป็นเส้นเดียวกัน โดยในการทดลองนี้ก็จะทำการพิสูจน์ว่าเมื่อทำ Ether Channel แล้วหากสายมีปัญหาย่อมสามารถที่จะส่งข้อมูลได้

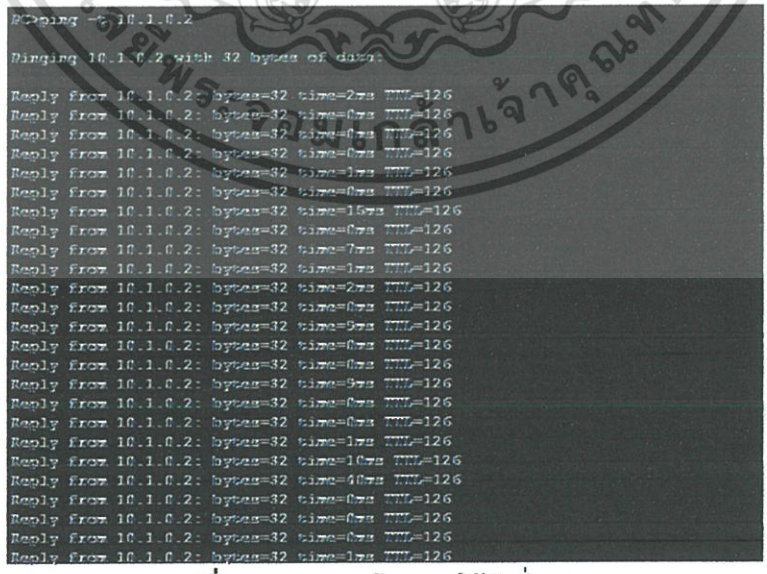


รูปที่ 4.13 การเชื่อมต่อของ Ether Channel

จากรูป 4.13 สวิทช์ที่ Station_01_Core_Switch นั้นพอร์ท fa0/5 และ fa0/6 ได้เกิดปัญหาดังรูปที่ 4.14



รูปที่ 4.14 สถานะของการเชื่อมต่อระหว่างพอร์ท



รูปที่ 4.15 ทดสอบโดยการใช้คำสั่ง ping

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.4 การทดลองโปรโตคอลการหาเส้นทาง

ในการทดลองนี้จะทำการทดสอบว่าโปรโตคอลระหว่าง RIPv2 และ OSPF เมื่อมีการเปลี่ยนเส้นทางเมื่อมีโครงสร้างที่เปลี่ยนไปจากปัญหาการเชื่อมต่อโดยเราจะทำการทดสอบโดยคำสั่ง ping โดยจะดูว่าโปรโตคอลแต่ละตัวจะสามารถส่งข้อมูลถึงกันใหม่โดยใช้เวลากี่วินาที โดยจะทำการทดลอง 10 ครั้ง

4.4.1 RIPv2

ระยะเวลาการ Re-Routing ดังตารางที่ 4.1

ตารางที่ 4.1 ผลการทดลองที่ 4.4.1

ครั้งที่	1	2	3	4	5	6	7	8	9	10
เวลาที่ใช้ (วินาที)	10.7	11.8	13.2	19.7	23.8	20.5	10.4	15.9	31.0	28.1

4.4.2 OSPF

ระยะเวลาการ Re-Routing ดังตารางที่ 4.2

ตารางที่ 4.2 ผลการทดลองที่ 4.4.2

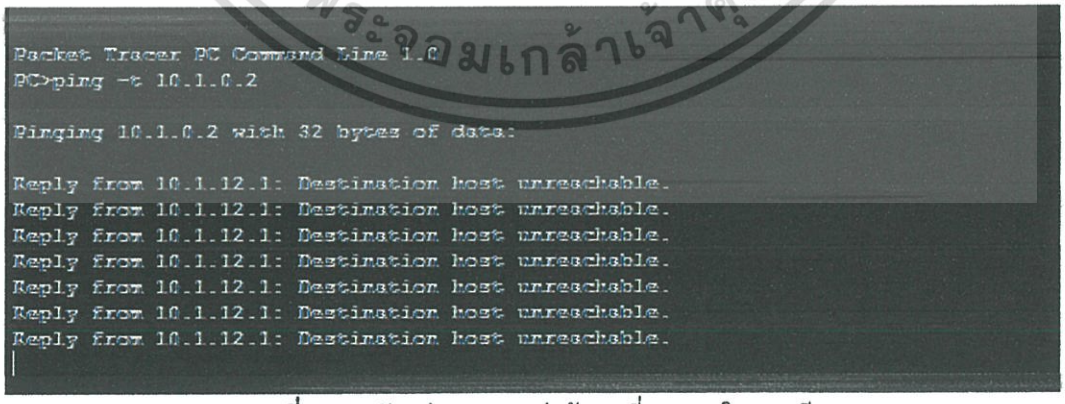
ครั้งที่	1	2	3	4	5	6	7	8	9	10
เวลาที่ใช้(วินาที)	7.0	7.9	7.1	6.7	7.5	13.1	-	14.1	7.2	7.7

4.5 การทดลอง Access Contorl Lists

4.5.1 การส่งข้อมูลไปหาเครื่องที่ต่าง VLAN กัน ภายในสถานี

การทดสอบการส่งข้อมูลไปหาเครื่องที่ต่าง VLAN กัน ภายในสถานี โดยในการทดสอบจะเลือกมา 3 ตัวอย่าง ซึ่งเป้าหมายคือแต่ละกรณีจะต้องไม่สามารถที่จะส่งข้อมูลไปหากันได้ เพื่อให้เป็นไปตามข้อกำหนด ที่ได้ไว้ในข้างต้น

กรณีที่ 1 จาก เครื่อง 10.1.12.2 ไปยัง 10.1.0.2



รูปที่ 4.16 ตัวอย่างผลการส่งข้อมูลที่ 1 ภายในสถานี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กรณีที่ 2 จากเครื่อง 10.1.4.2 ไปยัง 10.1.6.2

```
Packet Tracer PC Command Line 1.0
PC>ping -t 10.1.6.2

Pinging 10.1.6.2 with 32 bytes of data:

Reply from 10.1.4.1: Destination host unreachable.
Reply from 10.1.4.1: Destination host unreachable.
Reply from 10.1.4.1: Destination host unreachable.
Reply from 10.1.4.1: Destination host unreachable.
Reply from 10.1.4.1: Destination host unreachable.
Reply from 10.1.4.1: Destination host unreachable.
Reply from 10.1.4.1: Destination host unreachable.
```

รูปที่ 4.17 ตัวอย่างผลการส่งข้อมูลที่ 2 ภายในสถานี

กรณีที่ 3 จากเครื่อง 10.1.16.2 ไปยัง 10.1.4.3

```
Packet Tracer PC Command Line 1.0
PC>ping -t 10.1.4.3

Pinging 10.1.4.3 with 32 bytes of data:

Reply from 10.1.16.1: Destination host unreachable.
Reply from 10.1.16.1: Destination host unreachable.
Reply from 10.1.16.1: Destination host unreachable.
Reply from 10.1.16.1: Destination host unreachable.
Reply from 10.1.16.1: Destination host unreachable.
Reply from 10.1.16.1: Destination host unreachable.
```

รูปที่ 4.18 ตัวอย่างผลการส่งข้อมูลที่ 3 ภายในสถานี

4.5.2 การส่งข้อมูลไปหาเครื่องที่ต่าง VLAN กัน และต่างสถานี

การทดสอบการส่งข้อมูลไปหาเครื่องที่ต่าง VLAN กัน ต่างสถานี โดยในการทดสอบจะเลือกมา 3 ตัวอย่าง ซึ่งเป้าหมายคือแต่ละกรณีจะต้องไม่สามารถที่จะส่งข้อมูลไปหากันได้ เช่นเดียวกับการทดสอบก่อนหน้านี้

กรณีที่ 1 จากเครื่องที่ 10.1.12.2 ไป 10.2.2.2

```
PC>ping -t 10.2.2.2

Pinging 10.2.2.2 with 32 bytes of data:

Reply from 10.1.12.1: Destination host unreachable.
Reply from 10.1.12.1: Destination host unreachable.
Reply from 10.1.12.1: Destination host unreachable.
Reply from 10.1.12.1: Destination host unreachable.
Reply from 10.1.12.1: Destination host unreachable.
Reply from 10.1.12.1: Destination host unreachable.
Reply from 10.1.12.1: Destination host unreachable.
```

รูปที่ 4.19 ตัวอย่างผลการส่งข้อมูลที่ 1 ต่างสถานี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กรณีที่ 2 จากเครื่องที่ 10.5.6.2 ไป 10.1.16.2

```
PC>ping -t 10.1.16.2

Pinging 10.1.16.2 with 32 bytes of data:

Reply from 10.5.6.1: Destination host unreachable.
Reply from 10.5.6.1: Destination host unreachable.
Reply from 10.5.6.1: Destination host unreachable.
Reply from 10.5.6.1: Destination host unreachable.
Reply from 10.5.6.1: Destination host unreachable.
Reply from 10.5.6.1: Destination host unreachable.
Reply from 10.5.6.1: Destination host unreachable.
```

รูปที่ 4.20 ตัวอย่างผลการส่งข้อมูลที่ 2 ต่างสถานี

กรณีที่ 3 จากเครื่องที่ 10.2.2.2 ไป 10.3.14.2

```
PC>ping -t 10.3.14.2

Pinging 10.3.14.2 with 32 bytes of data:

Reply from 10.2.2.1: Destination host unreachable.
Reply from 10.2.2.1: Destination host unreachable.
Reply from 10.2.2.1: Destination host unreachable.
Reply from 10.2.2.1: Destination host unreachable.
Reply from 10.2.2.1: Destination host unreachable.
Reply from 10.2.2.1: Destination host unreachable.
```

รูปที่ 4.21 ตัวอย่างผลการส่งข้อมูลที่ 3 ต่างสถานี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5
สรุปและวิจารณ์ผลการทดลอง

5.1 บทสรุปโครงงาน

โครงงานนี้เป็นการศึกษาและออกแบบในเรื่องเครือข่ายการสื่อสารของระบบขนส่งทางราง โดยใช้ Cisco packet tracer เป็นโปรมแกรมในการจำลองเครือข่ายการสื่อสารขึ้นมา ซึ่งจำลองขึ้นมา 4 สถานีย่อย 1 สถานีหลัก และมีจำนวนทั้งหมด 10 ระบบ โดยเครือข่ายการสื่อสารที่ออกแบบและสร้างขึ้นมาจะรองรับการทำงานในเรื่อง ความเสถียรในการส่งข้อมูล, โปรโตคอลหาเส้นทาง, Access Control Lists, แบนด์วิดท์ที่เหมาะสม, Spannig Tree, การแจกจ่ายไอพีแอดเดรส และ Virtual Local Area Network โดยผลการทดลองในบทที่ 4 จะแสดงให้เห็นขึ้นการรองรับเหล่านี้ แต่ผลการทดลองที่ได้มาอาจมีบางส่วนที่ให้ผลการทดลองไม่เหมือนกันค่าจริงในระบบขนส่งทางราง เนื่องมาจากอุปกรณ์ในโปรแกรม Cisco packet tracer ไม่มีอุปกรณ์บางตัวที่ใช้จริงในระบบขนส่งทางราง ทำให้ผลการทดลองที่ได้ในบางส่วนไม่ถูกต้องสมบูรณ์ทั้งหมด

5.2 ปัญหาที่พบในระหว่างดำเนินงาน

1. อุปกรณ์เครือข่ายในโปรแกรม Cisco packet tracer มีไม่ครบ
2. สามารถในการตั้งค่าอุปกรณ์ของโปรแกรม Cisco packet tracer มีจำกัด
3. สามารถในการทดลองการส่งข้อมูลของโปรแกรม Cisco packet tracer มีจำกัด
4. ข้อมูลที่ใช้ในการศึกษาเรื่องเครือข่ายการสื่อสารในระบบขนส่งทางรางค่อนข้างหายาก

5.3 แนวทางแก้ไขและพัฒนาต่อ

1. หาโปรแกรมจำลองเครือข่ายการสื่อสารโปรแกรมอื่น
2. เอาการออกแบบและการตั้งค่าอุปกรณ์ต่างๆไปทดสอบกับอุปกรณ์จริง
3. เพิ่มการทำงานอื่นๆของเครือข่าย เพื่อเพิ่มประสิทธิภาพของเครือข่ายให้มากขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรณานุกรม

[1] 2557. เลขที่อยู่ไอพี. [Online]. เข้าถึงได้จาก : http://th.wikipedia.org/wiki/เลขที่อยู่ไอพี

[2] 2557. DHCP (Dynamic Host Configuration Protocol). [Online]. เข้าถึงได้จาก: http://cpe.rmutt.ac.th/comnet/pr/2552-2/Sec2-Tuesday/Ch14/Docs/Chapter%2014%20Dynamic%20Host%20Configuration%20Protocol%20(DHCP)

[3] 2557. VLAN (Virtual Local Area Network). [Online]. เข้าถึงได้จาก : http://th.wikipedia.org/wiki/แลน

[4] 2557. VTP (Virtual Trunking Protocol). [Online]. เข้าถึงได้จาก : http://www.msit.mut.ac.th/newweb/phpfile/show.php?Qid=1055

[5] 2557. ACLs (Access Control Lists). [Online]. เข้าถึงได้จาก : http://www.msit.mut.ac.th/newweb/phpfile/show.php?Qid=1124

[6] 2557. Ether Channel. [Online]. เข้าถึงได้จาก : http://running-config.blogspot.com/2011/03/etherchannel-cisco-catalyst-switch.html

[7] 2557. OSPF. [Online]. เข้าถึงได้จาก : http://www.msit.mut.ac.th/newweb/phpfile/show.php?Qid=883

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

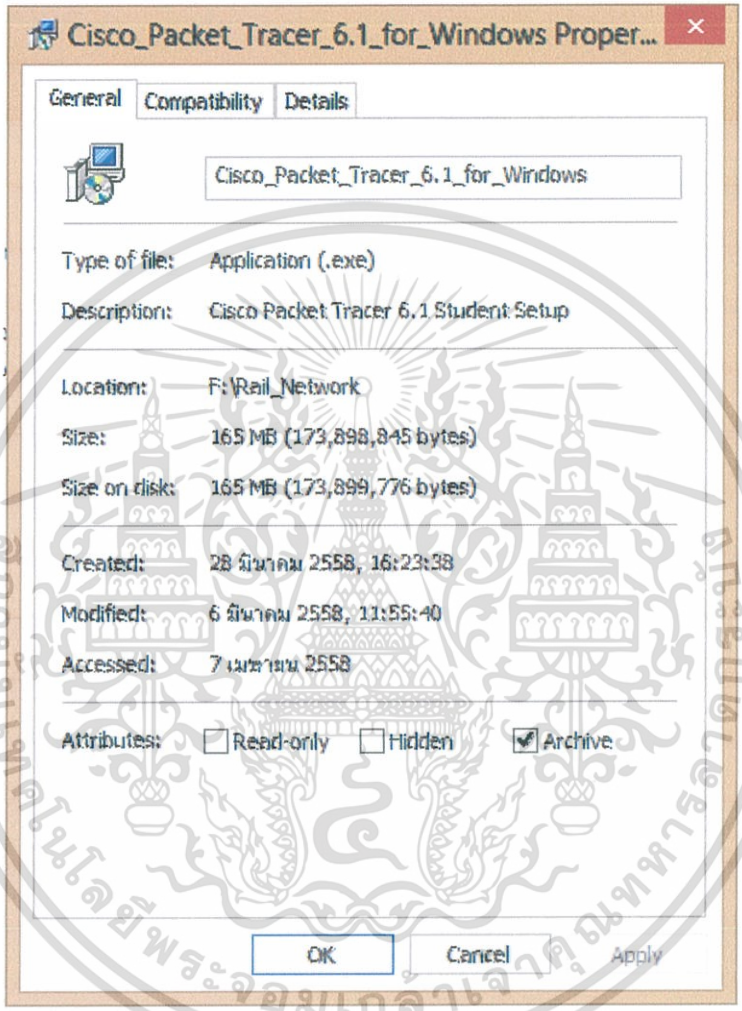
ภาคผนวก ก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

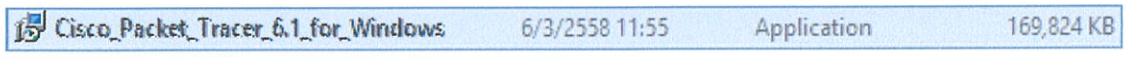
การติดตั้งโปรแกรม CISCO PACKET TRACER

โปรแกรมบนระบบปฏิบัติการ Windows สามารถอธิบายได้ดังนี้

1. เมื่อทำการดาวน์โหลด Cisco_Packet_Tracer_6.1_for_Windows.exe เรียบร้อย ไฟล์จะมีขนาดและฟอร์แมตไฟล์ดังรูป

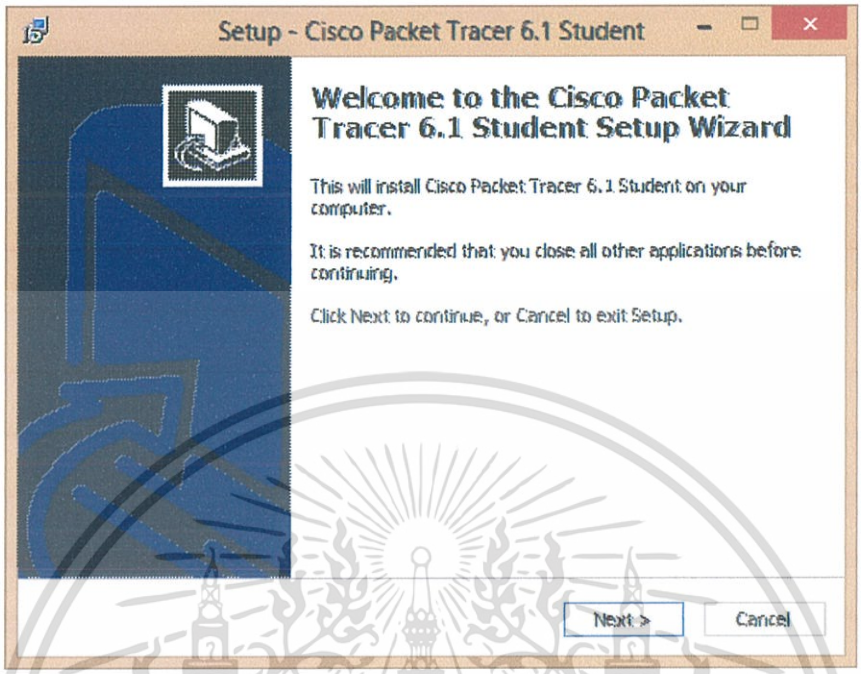


2. double-click ไฟล์ Cisco_Packet_Tracer_6.1_for_Windows.exe เพื่อเริ่มต้นติดตั้งโปรแกรม



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

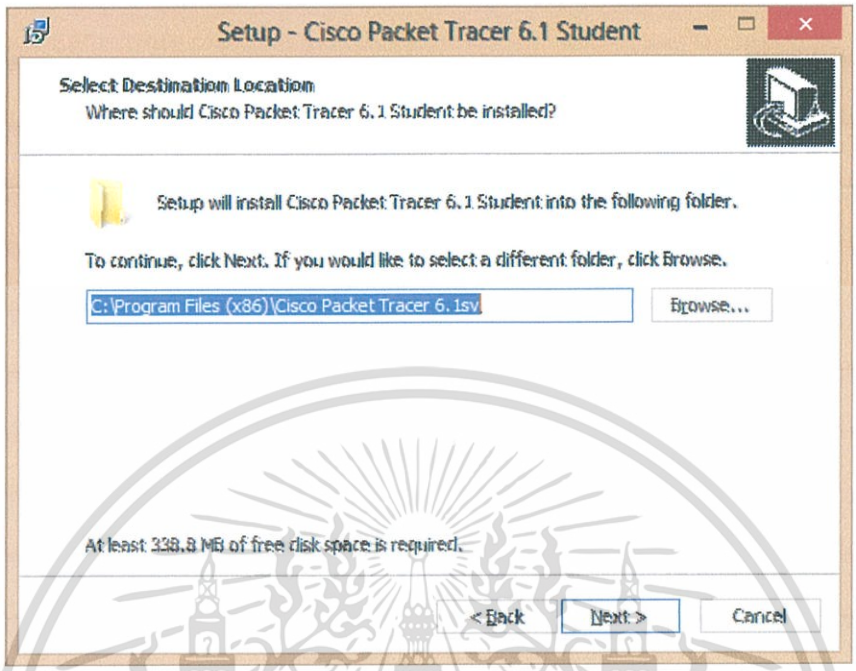
3. click Next >



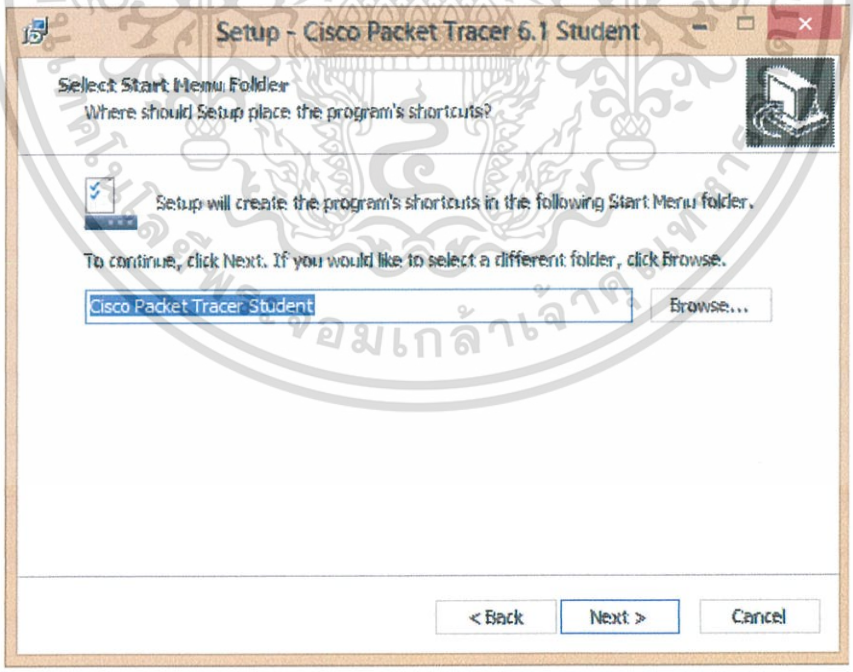
4.ยอมรับข้อตกลงในการใช้ซอฟต์แวร์ click Next >

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.เลือกตำแหน่งไฟล์ที่ติดตั้งโปรแกรม click Next >

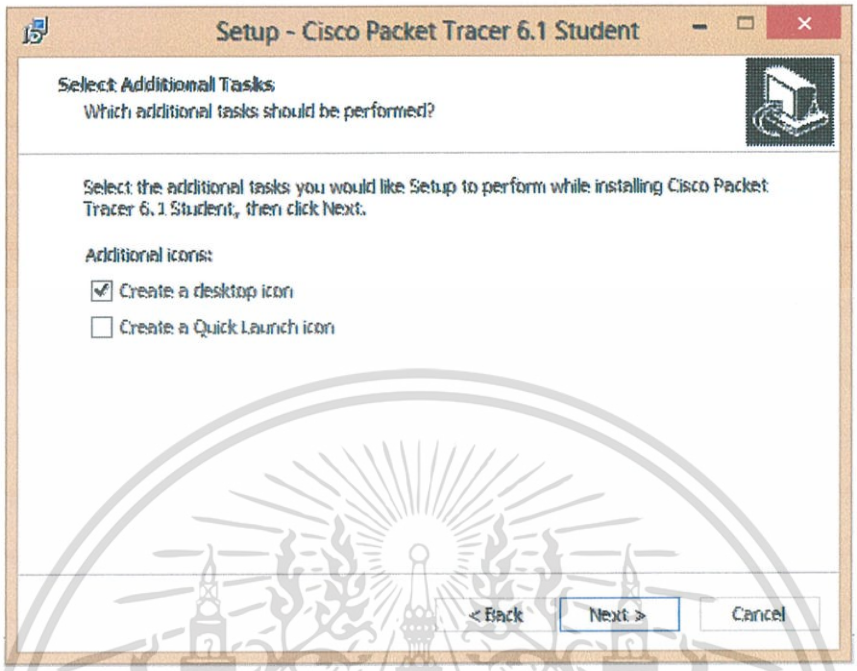


6.เลือกการแสดง Shortcuts click Next >

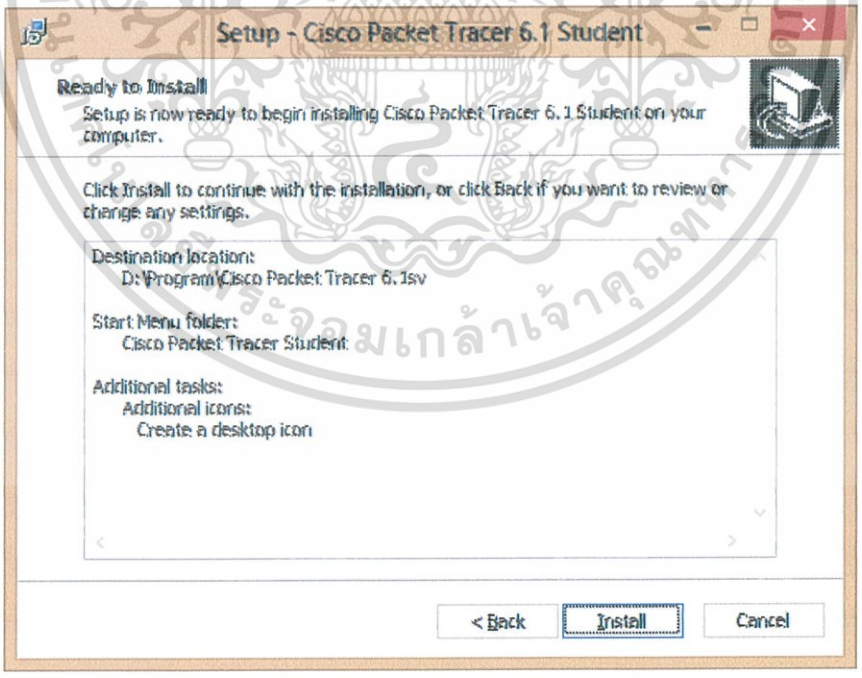


เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

7.ให้แสดง icon บน desktop click Next >

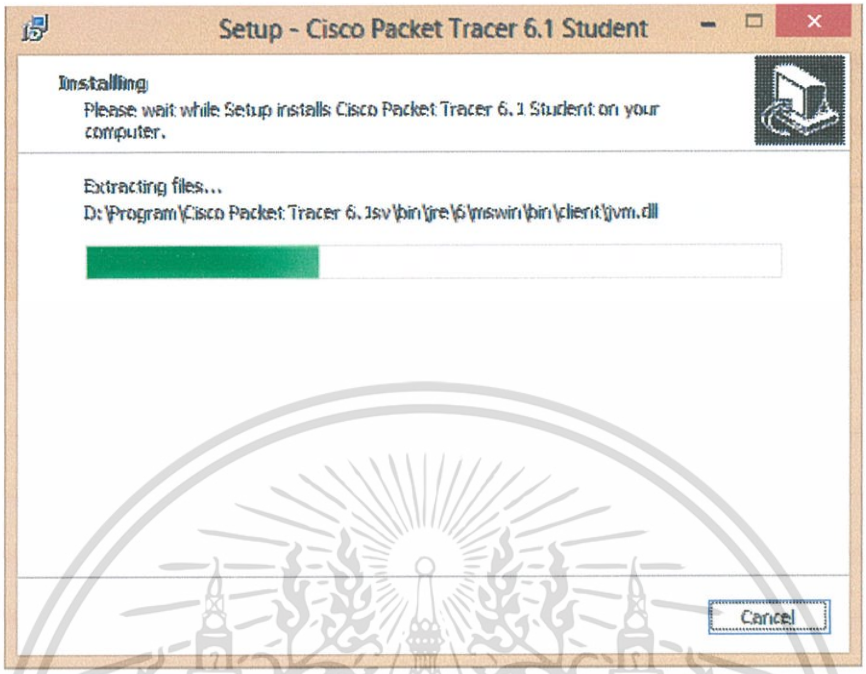


8.แสดงสรุปข้อมูลก่อน Install click Install

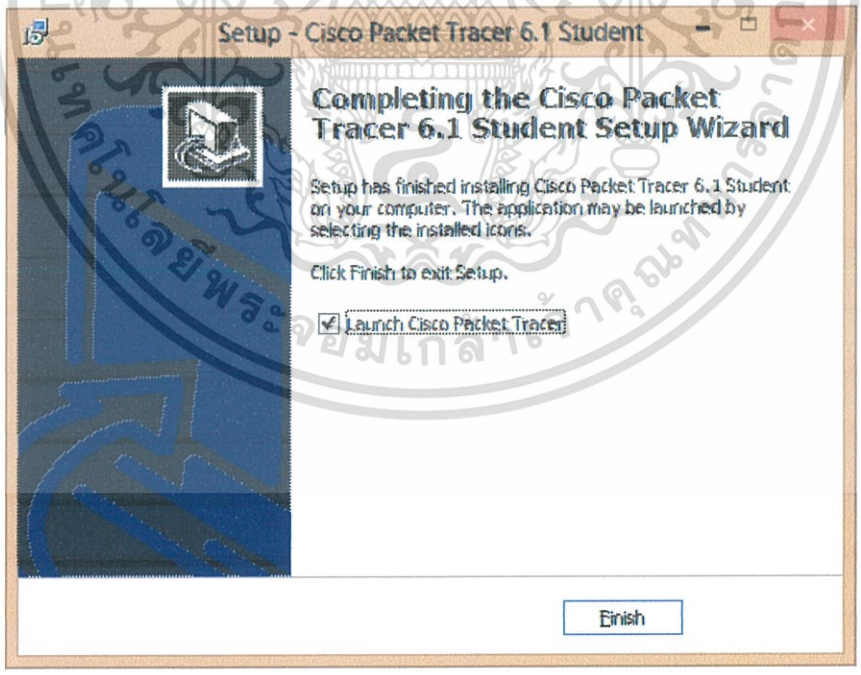


เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

9.โปรแกรมกำลังติดตั้ง



10. click 



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้