การออกแบบระบบเครือข่าย ภายในความเร็วสูงโดยเทคโนโลยีกิกะบิท อีเทอร์เน็ทร่วมกับสวิตช์เลเยอร์ 3

THE DESIGNING OF LOCAL AREA NETWORK INFRASTRUCTURE BY USEFUL GIGABIT ETHERNET TECHNOLOGY WITH LAYER 3

ธวัชชัย มะพะสาธุโร

THAWATCHAI MAPASATHURO

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมไฟฟ้า

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2547

ISBN 974-15-1203-2

การออกแบบระบบเครือข่าย ภายในความเร็วสูงโดยเทคโนโลยีกิกะบิทอีเทอร์เน็ทร่วมกับสวิตช์เลเยอร์3

THE DESIGNING OF LOCAL AREA NETWORK INFRASTRUCTURE BY USEFUL GIGABIT ETHERNET TECHNOLOGY WITH LAYER 3

ธวัชชัย มะพะสาธุโร
THAWATCHAI MAPASATHURO

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า
บัณฑิตวิทยาลัย
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ.2547

ISBN 974-15-1208-2

THE DESIGNING OF LOCAL AREA NETWORK INFRASTRUCTURE BY USEFUL GIGABIT ETHERNET TECHNOLOGY WITH LAYER 3

THAWATCAHI MAPASATHURO

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENT FOR THE DEGREE
MASTER OF ENGINEERING IN ELECTRICAL ENGINEERING
SCHOOL OF GRADUATE STUDIES
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2004

ISBN 974-15-1208-2

หัวข้อวิทยานิพนธ์ การออกแบบระบบเครือข่ายภายในความเร็วสูงโดยเทคโนโลยีกิกะบิทอีเทอร์เน็ทร่วมกับสวิตช์เลเยอร์3

นักศึกษา นายธวัชชัย มะพะสาธุโร

รหัสประจำตัว 43061142

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมไฟฟ้า

พ.ศ. 2547

อาจารย์ผู้ควบคุมวิทยานิพนธ์ รศ. ดร. กอบชัย เดชหาญ

บทคัดย่อ

บทความนี้นำเสนอการออกแบบระบบเครือข่ายกิกะบิทอีเทอร์เน็ทโดยนำฟังก์ชั่นของเครือข่ายท้องถิ่นเสมือน VLAN (Virtual LAN) โดยใช้รูปแบบการสื่อสารแบบ Virtual Trunking Protocol (VTP) ภายใต้การควบคุมการทำงานของ MSFC (Multilayer Switch Feature Card) โดยในขั้นตอนแรกจะทำการสร้าง VLANs เพื่อขจัดปัญหาการแออัดคับคั่งในเครือข่าย เนื่องมาจากการ Broadcast ให้น้อยลง จากนั้น VTP จะทำการส่งผ่าน VLANs name และ VLANs number ที่ได้สร้างไว้ไปยังอุปกรณ์เครือข่ายที่มีอยู่ทั้งหมด โดยมี MSFC ทำหน้าที่ในระดับ Layer 3 เพื่อหาเส้นทางส่งข้อมูลข้ามผ่าน VLANs ระหว่างกัน กอปรกับใช้ฟังก์ชั่น HSRP ในการทำ Redundant backup ให้กับ Layer 3 เพื่อเพิ่มความน่าเชื่อให้กับระบบเครือข่าย

Thesis Title	The Designing of Local Area Network Infrastructure by Useful Gigabit Ethernet Technology with Layer 3
Student	Mr.Thawatchai Mapasathuro
Student ID.	43061142
Degree	Master of Engineering
Programme	Electrical Engineering
Year	2004
Thesis Advisor	Assoc. Prof. Dr. Kobchai Dejhan

ABSTRACT

This paper presents the designing of Gigabit Ethernet Local Area Network infrastructure by coordinate variable of functions as sequence of VLAN through (Virtual LAN) VTP (Virtual Trunking Protocol) and MSFC (Multilayer Switch Feature Card) by VLAN function for traffic broadcast protection and virtual segmentation VTP for transferring VLANs name and number which are defined into all of network equipment via the MFSC of Layer 3 switch that be act as router by to route all of the traffic among VLANs and function of HSRP is for fault tolerance and redundant backup among CPUs and Layer 3 routing function for addition more network stability.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้อย่างดี ด้วยคำแนะนำเกี่ยวกับระบบเครือข่ายสื่อสารข้อมูล และคำปรึกษาที่มีประโยชน์อย่างสูงจากท่านรองศาสตราจารย์ ดร. กอบชัย เดชหาญ ที่ช่วยเหลือตลอดเวลา ซึ่งทำให้กระผมมีความรู้สึกซาบซึ้งในสิ่งต่าง ๆ ที่ท่านได้ให้ความอนุเคราะห์ ขอกราบขอบพระคุณเป็นอย่างสูง

ขอกราบขอบพระคุณ คุณพ่อ พิมพ์ คุณแม่ ฉวี มะพะสาธุโร และคุณแม่ พิศมัย ทวยภา ที่กรุณามอบชีวิต จิตใจ ความมุ่งมั่น ขยัน อดทนในด้านการศึกษาให้แก่ชีวิตกระผม

ขอขอบคุณ คุณชาลิน สุวรรณวงศ์ ที่คอยให้คำชี้แนะ ตลอดจนให้ความรู้ทางด้านระบบเครือข่าย พร้อมทั้งส่งเสริมสนับสนุนในด้านการศึกษาและคอยกระตุ้นเตือนอยู่เสมอ

ขอขอบคุณ คุณภาวินี มะพะสาธุโร ภรรยาที่คอยให้กำลังใจและเสียสละเวลาของครอบครัวเพื่อให้ผลงานวิจัยนี้เสร็จสิ้นได้ด้วยดี

ขอขอบคุณ ธนาคารสแตนดาร์ดชาร์เตอร์ดนครธน จำกัด (มหาชน) ที่ให้การสนับสนุนในเรื่องของการทำงานและอุปกรณ์ในการทำวิจัยนี้

สุดท้ายนี้ขอขอบคุณ พี่ ๆ เพื่อน ๆ และน้อง ๆ ที่ช่วยเหลือ แนะนำ และให้กำลังใจต่อผู้ทำวิจัยจนสำเร็จสมบูรณ์

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบแด่ผู้มีพระคุณทุกท่านที่ได้ประสิทธิประสาทวิชาความรู้และถ่ายทอดประสบการณ์ที่ดีให้แก่ข้าพเจ้า

ธวัชชัย มะพะสาธุโร

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญตาราง (ต่อ)

ตารางที่ หน้า

สารบัญตาราง (ต่อ)

ตารางที่ หน้า

สารบัญรูป

สารบัญรูป(ต่อ)

รูปที่ หน้า

สารบัญรูป(ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 กล่าวนำ

ปัจจุบันเครือข่ายคอมพิวเตอร์ได้มีบทบาทต่อชีวิตประจำวันมากขึ้นทุกขณะ การเจริญเติบโตของเครือข่ายคอมพิวเตอร์เหล่านี้เป็นไปอย่างต่อเนื่อง และยังไม่มีสัญญาณบ่งบอกว่าจะมีการชะลอตัวแต่อย่างใด เครือข่ายแบบท้องถิ่นในองค์กรต่างๆ ตลอดจน บริษัท สถานศึกษาส่วนใหญ่กว่า 80% จะนิยมใช้เครือข่ายอีเทอร์เน็ท ส่วนที่เหลือใช้งานแบบ FDDI/CDDI, ATM และอื่นๆ ด้วยความต้องการการส่งผ่านข้อมูลที่เพิ่มขึ้นอย่างรวดเร็วตามขนาดและจำนวนของเครื่องคอมพิวเตอร์ที่ต่ออยู่บนเครือข่าย ตลอดจนการเติบโตของอินเตอร์เน็ทอย่างรวดเร็ว จึงทำให้เครือข่ายอีเทอร์เน็ท แบบดั้งเดิมที่มีความเร็วในการส่งผ่านข้อมูลอยู่ที่ 10 Mbps เริ่มจะไม่สามารถตอบสนองความต้องการของผู้ใช้ได้อย่างมีประสิทธิภาพ จึงจำเป็นต้องสร้างเครือข่ายมารองรับปริมาณข้อมูลที่สูงขึ้น

กิกะบิทอีเทอร์เน็ท (IEEE802.3z) เป็นมาตรฐานใหม่ของเทคโนโลยีเครือข่ายท้องถิ่น (LAN-Local Area-Network) ที่พัฒนามาจาก เครือข่ายแบบอีเทอร์เน็ทแบบเก่าที่มีความเร็ว 10 Mbps ให้สามารถรับส่งข้อมูลได้ที่ระดับความเร็ว 1 Gbps ทั้งนี้เทคโนโลยีนี้ ยังคงใช้กลไก CSMS/CD ในการร่วมใช้สื่อเดียวกับอีเทอร์เน็ทแบบเก่า หากแต่มีการพัฒนาและดัดแปลงให้สามารถรองรับความเร็วในระดับ 1 Gbps ได้

การออกแบบให้เกิดประโยชน์ในทางปฏิบัติสูงสุดในระบบเครือข่ายทั้งยังให้ความน่าเชื่อถือด้วยการสร้างเครือข่ายที่มีคุณภาพสูงทำให้เกิดความน่าเชื่อถือในระดับสูงด้วย การใช้ประโยชน์กิกะบิทอีเทอร์เน็ทและกิกะบิทอีเทอร์แชนแนล จึงมีความจำเป็นต้องเชื่อมต่อกับสวิตช์กิกะบิทและเป็นการบริการตามความต้องการให้มีทรั้งที่มีความจุสูง (High-Capacity Trunk)

การออกแบบตามทฤษฎีเมื่อนำมาใช้ในทางปฏิบัติ พบว่าบางครั้งการออกแบบเครือข่ายได้ แต่บางครั้งพบว่าการออกแบบเครือข่ายก่อให้เกิดผลการใช้งานที่ค่อนข้างต่ำกว่าเกณฑ์มาตรฐาน ไม่ว่าจะเป็นความน่าเชื่อถือหรือการควบคุมที่ทำได้ยาก เพราะว่าลักษณะเฉพาะหลายประการที่ใช้งานได้หลากหลายจึงก่อให้เกิดความสับสนในการออกแบบ

ถ้าการออกแบบเครือข่ายเข้าใกล้ความเป็นจริงมาก การมีประสิทธิภาพในทางปฏิบัติและมีความน่าเชื่อถือสูงของเครือข่ายก็สามารถบรรลุได้ การเข้าใกล้ที่มีลักษณะลำดับชั้นนี้เรียกว่า 'การออกแบบมัลติเลเยอร์ (multiplayer)' การออกแบบมัลติเลเยอร์คือการใช้ส่วนจำเพาะและสเกลปริมาณผู้ใช้งานมาใช้ในการออกแบบ

วิทยานิพนธ์นี้จึงรวบรวมประสบการณ์ต่างๆ ที่ใช้งานจริงและบรรยายถึงการออกแบบเครือข่ายที่จะเกิดผลในเครือข่าย และบทความนี้จะเป็นการกล่าวถึงพื้นฐานของการออกแบบเครือข่ายที่สามารถสร้างความน่าเชื่อถือและสามารถทำการควบคุม จัดการได้ง่าย

1.2 อธิบายปัญหาที่กำลังศึกษาอยู่ของวิทยานิพนธ์

เนื่องจากในปัจจุบันระบบเครือข่ายคอมพิวเตอร์ท้องถิ่น (Local Area Network) ได้เข้ามีบทบาทอย่างมากต่อการทำงานขององค์กรต่าง ๆ โดยเฉพาะอย่างยิ่งกับองค์กรที่มีขนาดใหญ่นั้นจะมีการจัดแบ่งหน่วยงานออกเป็นหลาย ๆ หน่วยงาน ซึ่งจะต้องมีการรับส่งข้อมูลระหว่างหน่วยงานโดยผ่านระบบเครือข่ายภายในด้วยปริมาณที่สูง รวมถึงมีการเข้าถึงระบบฐานข้อมูลจากเครื่องไคลเอ็นต์ไปยังเครื่องเซิร์ฟเวอร์ ซึ่งถ้าหากระบบเครือข่ายที่ได้รับการออกแบบระบบมาโดยขาดหลักเกณฑ์นั้นจะทำให้ระบบเครือข่ายด้อยประสิทธิภาพลง และทำให้การรับส่งข้อมูลได้ช้าจนเป็นเหตุให้ระบบเครือข่ายล่มไม่สามารถใช้งานได้ จากเหตุการณ์ข้างต้นจึงได้เกิดแนวคิดในการออกแบบระบบเครือข่ายกิกะบิทอีเทอร์เน็ทมาใช้ร่วมกับสวิตช์เลเยอร์ 3 เพื่อทำการจัดแบ่งเครือข่ายท้องถิ่นเสมือน (Virtual LAN) เพื่อรองรับการทำงานและตอบสนองความต้องการของผู้ใช้ให้มีประสิทธิภาพสูงสุด

เนื่องจากระบบเครือข่ายในองค์กรต่างๆยังขาดการออกแบบอย่างเป็นลำดับชั้น(Hierarchy) ที่เหมาะสมตลอดจนขาดหลักเกณฑ์ในการจัดแบ่งเครือข่ายท้องถิ่นเสมือนเพื่อไว้ใช้ในการลดทราฟฟิกชนิดบรอดคาสต์ภายในเครือข่าย ซึ่งจะเป็นผลให้เครือข่ายมีประสิทธิภาพที่ลดต่ำลง กอปรกับความต้องการระบบสำรอง (Redundant backup) เพื่อทำให้ระบบเครือข่ายมีเสถียรภาพมากยิ่งขึ้น จึงทำให้การออกแบบระบบเครือข่ายเป็นหัวใจหลักที่จะทำให้ระะบเครือข่ายมีเสถียรภาพและสามารถบริการผู้ใช้งานได้ตลอดเวลาที่มีการเข้าถึง (Access) เครือข่าย

1.3 หลักการใหม่อะไรที่นำเสนอ

ใช้หลักการออกแบบเครือข่ายเพื่อทำให้เครือข่ายสามารถรองรับมัลติมีเดียได้ โดยได้ออกแบบเครือข่ายให้เป็นลำดับชั้น ซึ่งประกอบด้วยแกนกลาง (Core) ตัวกระจาย (Distribution) และตัวเข้าถึง (Access) จากนั้นทำการออกแบบระบบสำรองทั้งระบบเคเบิล และตัวอุปกรณ์เครือข่ายโดยใช้ฟังก์ชั่นอีเทอร์แชนแนลความเร็วสูง สำหรับการเชื่อมโยงแบ็คโบนหลักและแบ็คโบนรองเข้าด้วยกันเพื่อทำให้การถ่ายโอนข้อมูลได้เร็วขึ้น และใช้ฟังก์ชั่น Spanning tree สำหรับการสำรองเส้นทางของระบบเคเบิล ซึ่งจะทำงานโดยอัตโนมัติในกรณีที่สายเคเบิลหลักชำรุดหรือขาดได้ รวมถึงได้พัฒนาการออกแบบเครือข่ายท้องถิ่นเสมือนเพื่อทำให้ระบบเกิดความเสถียรภาพมากขึ้นโดยการใช้สวิตช์เลเยอร์3 ซึ่งติดตั้งมากับแบ็คโบนเพื่อสร้างเกทเวย์เสมือน (Virtual gateway) และเครือข่ายท้องถิ่นเสมือน (Virtual LAN) เพื่อลดทราฟฟิกชนิดบรอดคาสต์และการแบ่งแยกชนิดของ

ทราฟฟิกที่จะเข้ามารบกวนระบบเครือข่าย ก่อให้เกิดความปลอดภัยในระบบเครือข่ายได้ระดับหนึ่ง นอกจากนี้การออกแบบดังกล่าวทำให้ลดการ configuration หรือการวางตำแหน่งอุปกรณ์ผิดพลาดหรือทำงานผิดปกติให้น้อยลง การทำเราติ้งโพรโตคอลในเลเยอร์ 3 ไม่ว่าจะเป็น Open Shortest Path First (OSPF) หรือ Enhanced Interior Gateway Routing Protocol (EIGRP) ล้วนต้องการทำโหลดบาลานซิ่ง และ fast convergence โดยการทำระบบสำรอง และ fast convergence โดยการใช้ Hot Standby Router Protocol (HSRP) ดังนั้นในการออกแบบจึงเป็นการเปลี่ยนขนาดของแบนด์วิดท์จากอีเทอร์เน็ทความเร็วสูง เป็นอีเทอร์แชนแนลความเร็วสูง และจากกิกะบิตอีเทอร์เน็ทไป กิกะบิตอีเทอร์แชนแนลได้อย่างมีประสิทธิภาพและประสิทธิผล

1.4 เปรียบเทียบกับหลักการเดิม

ในรูปแบบของเครือข่ายท้องถิ่นแบบเดิม จะเป็นรูปแบบเครือข่ายเดียวโดยขึ้นอยู่กับการเชื่อมโยงแบบกายภาพ (Physical) การส่งผ่านข้อมูลทำให้เกิดความซับซ้อนยุ่งยากในการทำเราติ้งและความจุซึ่งถูกจำกัดด้วยความสามารถในการ route เส้นทางของเราเตอร์ เมื่อมีการส่งข้อมูลที่มีปริมาณมากในโครงข่ายจึงมีโอกาสเกิดการเอ่อล้นของข้อมูล หรือเกิดความผิดพลาดได้ง่าย และในการขยายเครือข่ายทำได้ค่อนข้างยุ่งยากซับซ้อน

ดังนั้นในการออกแบบดังกล่าวจะสามารถแก้ไขปัญหาอันเป็นจุดอ่อนของเครือข่ายท้องถิ่นแบบเดิมได้อย่างสมบูรณ์แบบ

บทที่ 2
การออกแบบโครงข่าย

การใช้ประโยชน์ของแคมปัสกิกะบิทสวิตช์ ก่อให้เกิดประโยชน์ในทางปฏิบัติสูงสุดในเครือข่ายและยังมีความเชื่อถือระดับสูงด้วย กิกะบิทอีเทอร์เน็ทและกิกะบิทอีเทอร์แชนแนล จึงมีความจำเป็นต้องเชื่อมต่อร่วมกับกิกะบิทสวิตช์ ถ้าในทางการออกแบบเครือข่ายเข้าใกล้ความเป็นจริงมากที่สุด ประสิทธิภาพในทางปฏิบัติและมีความน่าเชื่อถือสูงของเครือข่ายก็สามารถบรรลุวัตถุประสงค์ได้ง่าย แต่บางครั้งพบว่าการออกแบบเครือข่ายหลายๆ ครั้งได้ผลลัพธ์ค่อนข้างต่ำ ไม่ว่าจะเป็นความน่าเชื่อถือและการควบคุมที่ทำได้ยาก เพราะว่าลักษณะเฉพาะหลายประการที่ใช้งานได้หลากหลายจึงก่อให้เกิดความสับสนในการออกแบบ วิทยานิพนธ์นี้จึงรวบรวมประสบการณ์ต่างๆ ที่ใช้งานจริงและบรรยายถึงการออกแบบเครือข่ายที่จะเกิดผลในเครือข่ายธรรมดาๆ ที่มีความน่าเชื่อถือและมีการจัดการได้ง่าย

การเข้าใกล้ที่มีลักษณะลำดับชั้นนี้เรียกว่า "การออกแบบ multilayer (ความหนาหลายชั้น)"การออกแบบ multilayer คือการใช้ส่วนจำเพาะและสเกลปริมาณผู้ใช้งานมาใช้ในการออกแบบ ระดับชั้นอินทราเน็ทแคมปัส คือทฤษฎีที่ทำให้การแก้ไขเครือข่ายทำได้ง่ายขึ้น ความฉลาดในการให้บริการในเลเยอร์ 3 ทำให้ลดการ set up การวางตำแหน่งอุปกรณ์ผิดหรือการทำงานผิดปกติให้น้อยลง นอกจากนี้ การทำ routing protocol ในเลเยอร์ 3 ไม่ว่าจะเป็น Open Shortest Path First (OSPF) หรือ Enhanced Interior Gateway Routing Protocol (EIGRP) ล้วนต้องการโหลดบาลานซ์ และการรวมกันอย่างรวดเร็ว (fast convergence)

รูปแบบของ multilayer สามารถเคลื่อนย้ายได้ง่ายเนื่องจากมีการเก็บรักษาเราติ้งเทเบิ้ลของเครือข่ายแคมปัสไว้บนเราเตอร์และฮับ การทำ redundancy และ fast convergence ทำได้โดยการใช้ Hot Standby Router Protocol (HSRP) การเปลี่ยนขนาดของแบนด์วิดท์จากอีเทอร์เน็ทความเร็วสูงเป็นอีเทอร์แชนแนลความเร็วสูง และจากกิกะบิทอีเทอร์เน็ทไปกิกะบิทอีเทอร์แชนแนล ทำได้โดยรูปแบบโมเดลที่สนับสนุนการทำงานดังกล่าวทั้งหมดก็คือแคมปัสโปรโตคอล

รูปแบบของ multilayer ที่กำลังบรรยายถึง มีทางเลือกที่สำคัญ 2 ทางคือการที่มีขนาดเครือข่ายที่เหมาะสมกับขนาดของอาคารและเครือข่ายแคมปัสที่มีขนาดใหญ่ การออกแบบ แบ็คโบนที่มีความแตกต่างกัน 5 ประการทางด้านการปฏิบัติและขนาดของเครือข่าย ได้แสดงในวิทยานิพนธ์นี้แบ็คโบนที่ใช้คือสวิตช์และการเชื่อมต่อในแบ็คโบนของเครือข่ายที่ทำหน้าที่ส่งผ่านข้อมูลจาก client ไปยัง server

2.1 การออกแบบโครงสร้างของสวิตชิ่งแบบหลายระดับชั้น

การพัฒนาทาง ฮาร์ดแวร์ของ สวิตช์เลเยอร์ 2 ทำให้เกิดความต้องการออกแบบการใช้งานก่อนหน้านี้หลายปี การออกแบบเหล่านี้ถูกทำให้มีลักษณะเฉพาะที่เรียกว่า 'flat' เนื่องจากต้องการหลีกเลี่ยงสิ่งที่เกี่ยวกับตรรกที่มีลักษณะลำดับชั้นและการรวบรวมบริการไว้บนเราเตอร์ เช่น ความกว้างของแคมปัสบน VLANs ถูกออกแบบโดยใช้พื้นฐานบนโมเดลการออกแบบของ flat นั่นเอง เช่นเดียวกันกับพัฒนาการของ สวิตช์เลเยอร์ 3 ที่เพิ่มประสิทธิภาพโดยการจัดการส่งต่อแพ็คเก็ตโดยฮาร์ดแวร์ที่ชำนาญเป็นพิเศษ ในการออกแบบเครือข่ายแคมปัสทำได้โดยการวางสวิตช์เลเยอร์ 3 ในส่วนระดับชั้นการแจกจ่าย (Distribution) และใช้แบ็คโบนแคมปัสเลเยอร์ 3 ในขณะที่แคมปัสที่มีขนาดเล็กกว่าจะสามารถจัดการได้ง่ายและถูกกว่า การบริการที่สำคัญอย่าง เช่น ห้าม การบรอดคาส์ทหรือ การกรองโปรโตคอลถูกดำเนินการในสวิตช์เลเยอร์ 2 การทำ Multilayer Access ของ สวิตช์เลเยอร์ 2 และสวิตช์เลเยอร์ 3 ทำให้เกิดเครือข่ายแคมปัสที่มั่นคงและเพื่อช่วยให้การวิเคราะห์การออกแบบเครือข่ายแคมปัสบรรลุผล ซึ่งสามารถทำได้ดังแนวทางด้านล่างนี้

2.1.1 ขอบเขตความผิดพลาด (Failure Domain)

กลุ่มของสวิตช์เลเยอร์ 2 ที่ถูกเชื่อมต่อด้วยกันเรียกว่าขอบเขตของสวิตช์เลเยอร์ 2 ขอบเขตนี้อาจเกิดความผิดพลาดได้เนื่องจากการวางตำแหน่งหรือเวิร์คสเตชันทำงานผิดปกติ ส่งผลให้เกิด error หรือไม่สามารถใช้งานในขอบเขตทางเข้า เพราะไม่สามารถป้องกันให้ข้อมูลอื่นเข้ามาในขอบเขตได้ทั้งหมด เมื่อการ์ดอินเตอร์เฟสของเครือข่าย (NIC) ทำการบรอดคาสต์ ข้อมูลอย่างรวดเร็ว เวิร์คสเตชันที่มี IP ผิดก่อให้เกิดเป็นหลุมดำของแพ็กเก็ต ซึ่งปัญหากล่าวเป็นไปตามธรรมชาติแต่ยากที่จะกำจัดได้ในทางตรรกะศาสตร์ บริเวณของขอบเขตความผิดพลาดจะถูกทำให้ลดน้อยลงได้โดยการจำกัดให้มีสวิตช์เลเยอร์ 2 ตัวเดียว (ถ้าเป็นไปได้) เพื่อทำการจัดวาง VLANs และ trunking VLAN ให้เหมาะสม ในเชิงอุดมคติหนึ่ง VLAN (IP subnet) ถูกจำกัดให้อยู่ในสวิตช์เพียงตัวเดียว การเชื่อมโยงวงจรขาขึ้นของกิกะบิทจากแต่ละสวิตช์ ทำโดยการต่อโดยตรงถึงอินเตอร์เฟสของสวิตช์เลเยอร์ 3 โดยตรง หากต้องการทำโหลดบาลานซ์ทำได้โดย กำหนดให้มี 2 VLANs ในสวิตช์ตัวเดียวกัน

2.1.2 Broadcast Domain

การใช้งานสวิตช์เลเยอร์ 2 ก่อให้เกิดการบรอดคาสต์อย่างท้วมท้น ในขณะที่สวิตช์เลเยอร์ 3 ถูกออกแบบให้มีสร้างโครงสร้างเพื่อลดการบรอดคาสต์ ยิ่งกว่านั้นความฉลาดและคุณลักษณะเฉพาะของโปรโตคอลสวิตช์เลเยอร์ 3 ในอนาคตจะบรรจุ Dynamic Host Configuration Protocol (DHCP) โดยการเปลี่ยนให้เป็นรูปแบบ unicast โดยตรงได้

2.1.3 Spanning-Tree Domain

สวิตช์เลเยอร์ 2 ใช้ spanning tree เพื่อหยุดการวนลูปของข้อมูล (ซึ่งมักเกิดขึ้นเนื่องจากโทโปโลยีในเลเยอร์ 2) โดยเมื่อมีเส้นทางสำรองมันทำงานในโหมด Blocking และหยุดการส่งต่อข้อมูลหากเกิดการลูป การออกแบบในเลเยอร์ 2 นั้นจะใช้โปรโตคอลในเลเยอร์ 3 ทำโหลดบาลานซิ่งและเส้นทางสำรอง ดังนั้นเส้นทางทั้งหมดจึงถูกใช้สำหรับการจราจรในเครือข่าย ส่วนการทำงานของ spanning-tree จะใช้เวลารวมในการทำงาน 30 วินาทีถึง 50วินาที การหลีกเลี่ยงการลูปจึงเป็นส่วนที่สำคัญอย่างยิ่งในเครือข่ายเช่นในแบ็คโบนแคมปัส ซึ่งในการออกแบบดังกล่าวต้องมั่นใจว่าการเชื่อมต่อลิงค์ทั้งหมดทำบนสวิตช์แบ็คโบนหรือบนเราเตอร์เท่านั้น ไม่ใช่เชื่อมต่อที่ VLAN trunk จึงจะสามารถระงับการบรอดคาสต์และขอบเขตผิดพลาดได้ การใช้สวิตช์เลเยอร์ 3 ที่ออกแบบโครงสร้างเพื่อทำให้ลดบริเวณของขอบเขต spanning-tree ได้โดยการใช้โปรโตคอลเลเยอร์สาม เช่น IGRP หรือ OSPF ทำโหลดบาลานซ์ เส้นทางสำรอง และการฟื้นตัวในแบ็คโบน

2.1.4 Virtual Local Area Network (VLAN)

VLAN ทำได้โดยสวิตช์เลเยอร์ 2 ซึ่งทำให้หลายๆ VLANs อยู่ร่วมกันได้โดยแต่ละกลุ่มของ VLAN จะมีลักษณะพิเศษของขอบเขตผิดพลาด ขอบเขตการบรอดคาสต์และขอบเขต spanning-tree ที่เหมือนกัน ดังนั้นแม้ว่า VLANs ถูกทำขึ้นเพื่อแบ่งแยกเครือข่ายแคมปัสทางตรรกะ แต่การใช้อย่างมีประสิทธิภาพของ VLANs ก็ถูกนำมาใช้แพร่หลายทั่วแคมปัสที่มีความซับซ้อนมากขึ้น ดังนั้นการหลีกเลี่ยงการลูปควรจำกัด VLAN ให้อยู่ในสวิตช์เลเยอร์ 2 ตัวเดียวเพื่อให้ความซับซ้อนน้อยที่สุด

2.1.5 IP Subnet

IP subnet ถูกให้คำจำกัดความที่สวิตช์เลเยอร์ 3 ที่มาบรรจบกับสวิตช์เลเยอร์ 2 ข้อได้เปรียบของการทำ subnetting คือที่สวิตช์เลเยอร์ 3 ทำการแลกเปลี่ยนข้อมูล มีการเรียนรู้ทุกเส้นทางที่ผ่านในเครือข่ายทั้งหมด ประโยชน์ที่ได้เช่น IGRP หรือ OSPF ในการออกแบบที่ในเชิงอุดมคติ หนึ่ง IP subnet จะใช้งานใน VLAN เดียวบนสวิตช์ซึ่งเป็นการออกแบบที่ทำได้ง่ายและแก้ไขได้สะดวก

2.1.6 Policy Domain

นโยบายการเข้าถึงถูกให้คำจำกัดความที่เราเตอร์หรือสวิตช์เลเยอร์ 3 ในอินทราเน็ทแคมปัส ที่ประยุกต์นำมาใช้กับ IP subnet โดยนโยบายการเข้าถึงที่เหมือนกันสามารถจัดความสะดวกให้กับกลุ่ม IP subnet และกลุ่มของ VLAN ที่เหมือนกัน

การออกแบบมีอยู่หลายรูปแบบด้วยกัน โดยใช้พื้นฐานการออกแบบบนบล็อกไดอะเกรมที่แสดงดังภาพข้างล่างเช่นเดียวกัน การออกแบบโครงสร้างให้เหมาะสมกับขนาดของโครงข่ายทั่ว

ไปจนถึงโครงข่ายขนาดใหญ่ที่มีอุปกรณ์มากที่สุดถึง 1,000 อุปกรณ์ การออกแบบโครงข่ายให้เหมาะสมกับจำนวนของแคมปัสที่มีมากและอยู่ในหลายอาคาร ซึ่งทั้งคู่อาศัยหลักการพื้นฐานบนบล็อกการสร้างโครงข่ายแบบธรรมดา และเป็นพื้นฐานการการออกแบบโมดูลาร์ โดยเมื่อมีการเพิ่มขนาดโครงข่ายจาก building model เป็น Campus model นั้น ต้องมีการขยายในส่วนแคมปัสแบ็คโบนด้วย การออกแบบแคมปัสแบ็คโบนเพื่อให้ใช้ในลักษณะงานที่ต่างกันดังต่อไปนี้

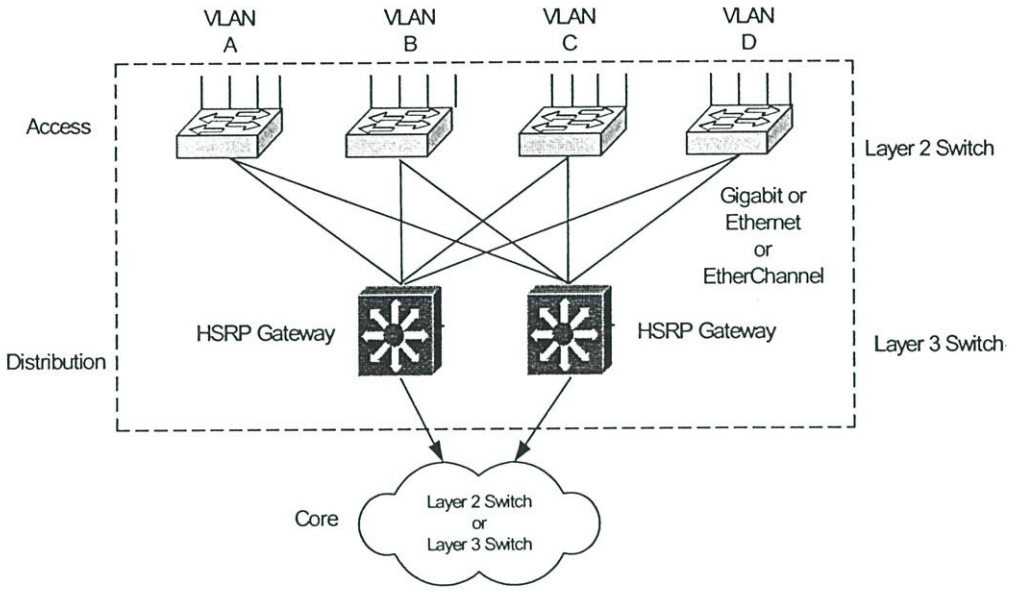
2.2 การออกแบบโมดูลาร์

พื้นฐานการออกแบบมัลติเลเยอร์ที่มีการสำรองเส้นทางดังแสดงในบล็อก ทรั้งกิกะบิทอีเทอร์เน็ทถูกเชื่อมโยงโดยสวิตช์เลเยอร์ 2 ในขณะที่สวิตช์เลเยอร์ 3 ทำหน้าที่ในเลเยอร์การแจกจ่าย (distribution) แนวคิดการออกแบบโมดูลาร์ ได้ประยุกต์สู่การทำเซิร์ฟเวอร์ฟาร์มและการเชื่อมต่อ ด้วย Wide Area Network (WAN)

เส้นทางสำรองและการฟื้นตัวสู่สภาวะปกติทำได้โดยการใช้งาน HSRP ในสวิตช์เลเยอร์ 3 2 ตัวที่อยู่ในระดับชั้น distributionโดยค่า HSRP ที่ตั้งค่าจากโรงงานคือ 10 วินาที แต่ก็สามารถตั้งค่าให้น้อยกว่านี้ได้ในขณะที่ค่าใช้จ่ายของเส้นทางสำรองเพิ่มขึ้นเพียง 15 เปอร์เซนต์ถึง 25 เปอร์เซ็นต์เท่านั้น เนื่องจากสวิตช์เลเยอร์ 2 ในระดับชั้น distribution และแบ็คโบนมีความสมบูรณ์แบบของการทำเส้นทางสำรองอยู่แล้ว ดังนั้นการลงทุนที่เพิ่มขึ้นคือการเพิ่มจำนวนอุปกรณ์ในเครือข่ายเช่นเซิร์ฟเวอร์นั้นเอง

โมเดลในรูปที่ 2.1 แต่ละ IP subnet ถูกกำหนดไว้ในสวิตช์แต่ละตัว การออกแบบนี้ ไม่ได้ใช้ spanning-tree และ VLAN การเชื่อมต่อไปยังกิกะบิททำโดยสวิตช์เลเยอร์ 3 ในเลเยอร์ distribution แม้ว่าโมเดลนี้เป็นแบบธรรมดาทั่วๆ ไป แต่ถ้าต้องการให้มี VLAN มากกว่า 1 VLAN ก็สามารถทำได้และการรองรับเซิร์ฟเวอร์ใน distributed workgroup สามารถได้เช่นกัน

การออกแบบที่เหมาะสมได้เพิ่มส่วนของส่งผ่านข้อมูลที่สมดุล (load balancing) จากสวิตช์ทั้งสองตัวที่เป็นการเชื่อมโยงของเครือข่าย เช่น IP subnet (ใน 2 VLANs) โดยสวิตช์ด้านซ้ายในเลเยอร์ distribution ได้ถูกกำหนดให้เป็น HSRP primary gateway สำหรับ IP subnet หนึ่งและสวิตช์ด้านขวาก็ถูกกำหนดให้เป็น HSRP primary gateway สำหรับอีก IP subnet โดยสวิตช์เลเยอร์ distribution ด้านซ้ายจะรองรับ HSRP สำหรับ IP subnet ที่เป็นเลขคู่เสมอและสวิตช์ด้านขวาจะรองรับ HSRP สำหรับ IP subnet ที่เป็นเลขคี่เสมอ



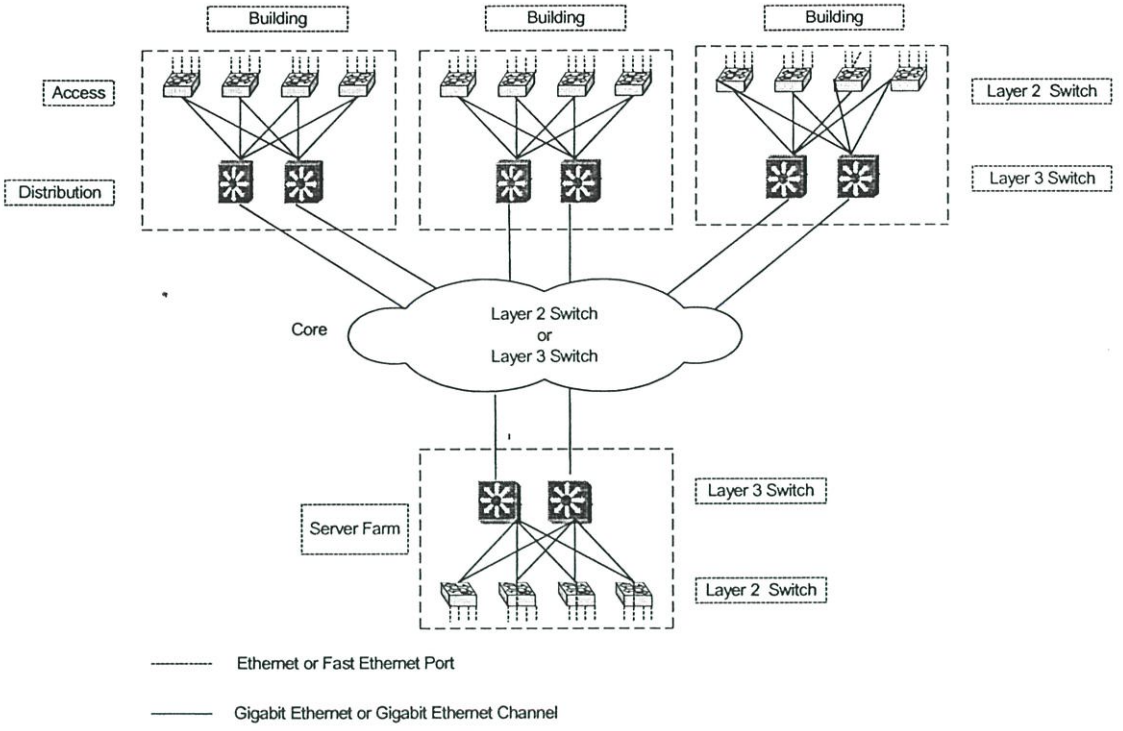
รูปที่ 2.1 Building Block

สำหรับการทำโหลดบาลานซ์ยังสามารถทำได้โดยใช้ multigroup HSRP(MHSRP) ซึ่งทำงานโดยการกำหนด IP subnet เดียวบนสวิตช์ โดยใช้เกทเวย์บนเราเตอร์ที่ต่างกัน 2 addresss สวิตช์เลเยอร์ 3 ทางด้านซ้ายก็จะปฏิบัติงานในฐานะเป็นเกทเวย์ เราเตอร์ของ host subnet ครึ่งหนึ่งและสวิตช์เลเยอร์ 3 ทางด้านขวาก็จะทำงานในฐานะ เป็น เกทเวย์เราเตอร์อีกในครึ่งหนึ่ง

การออกแบบที่บรรยายมานั้น กลุ่มของข้อมูลจากโฮสต์จะเจาะจงให้อยู่ในบล็อกที่ HSRP ทำงานอยู่เสมอ สวิตช์เลเยอร์ 3 ทั้งสองตัวก็จะทำการส่งต่อกลุ่มข้อมูลเหล่านี้ออกไปข้างนอก ถ้าอยากให้การส่งเป็นสัดส่วนที่เท่ากัน ทำได้โดยการกำหนดให้ routing metric ที่ต่ำกว่าในอินเตอร์เฟส VLAN ของเกทเวย์ HSRP เราเตอร์ระบบเมตริกนี้จะถูกส่งไปยังสวิตช์เลเยอร์ 3 ในแบ็คโบน ซึ่งเป็นทางผ่านที่มีค่าคอส์ทต่ำที่สุดเพื่อส่งคืนกลุ่มข้อมูลมายังเส้นทางเดิม โดยอาศัยชื่อที่เหมือนกัน

2.3 การออกแบบ Building

การออกแบบ Building ดังแสดงในรูปที่ 2.2 ประกอบด้วย building บล็อกที่มีเส้นทางสำรองเดียว เมื่อสวิตช์เลเยอร์ 3 ที่เป็นแบ็คโบน ไม่สามารถใช้งานได้ สวิตช์เลเยอร์ 2 ก็จะถูกใช้อย่างมีประสิทธิภาพเพื่อให้สภาวะเชื่อมต่อเส้นทางสำรองไปยังกิกะบิทบนสวิตช์แบ็คโบน ส่วนอีกทางเลือกถ้าต้องการให้หนึ่ง VLAN มีเส้นทางการเชื่อมต่อมากกว่าหนึ่งเส้นทาง สามารถดูเพิ่มเติมจาก ' วิธีการเลือกการออกแบบ Building-Block '



รูปที่ 2.2: Generic Campus Design

การออกแบบ building ให้เหมาะที่สุดคือการปิดการแลกเปลี่ยนเราติ้งโปรโตคอล ที่ผ่านใน subnet ทำโดยใช้คำสั่งบนอินเตอร์เฟสที่สวิตช์ในระดับชั้น distribution การแลกเปลี่ยนเส้นทางทำได้ใน distribution สวิตช์กับคอร์สวิตช์ใน VLANs เท่านั้น การปิดการแลกเปลี่ยน เราติ้งโปรโตคอล ทำให้การทำงานของ CPU ที่สวิตช์ระดับชั้น distribution ลดลง ในขณะที่การแลกเปลี่ยนอื่นๆเช่น Cisco Discovery Protocol (CDP) หรือ HSRP ไม่มีผลต่อการลดการทำงานของ CPU ดังกล่าว

ในการออกแบบ building นั้นเซิร์ฟเวอร์ สามารถต่อกับสวิตช์เลเยอร์ 2 หรือสวิตช์เลเยอร์ 3 ที่เป็นแบ็คโบนได้โดยตรง เพื่อให้ได้ประสิทธิภาพในการทำงานและความต้องการที่มากขึ้น

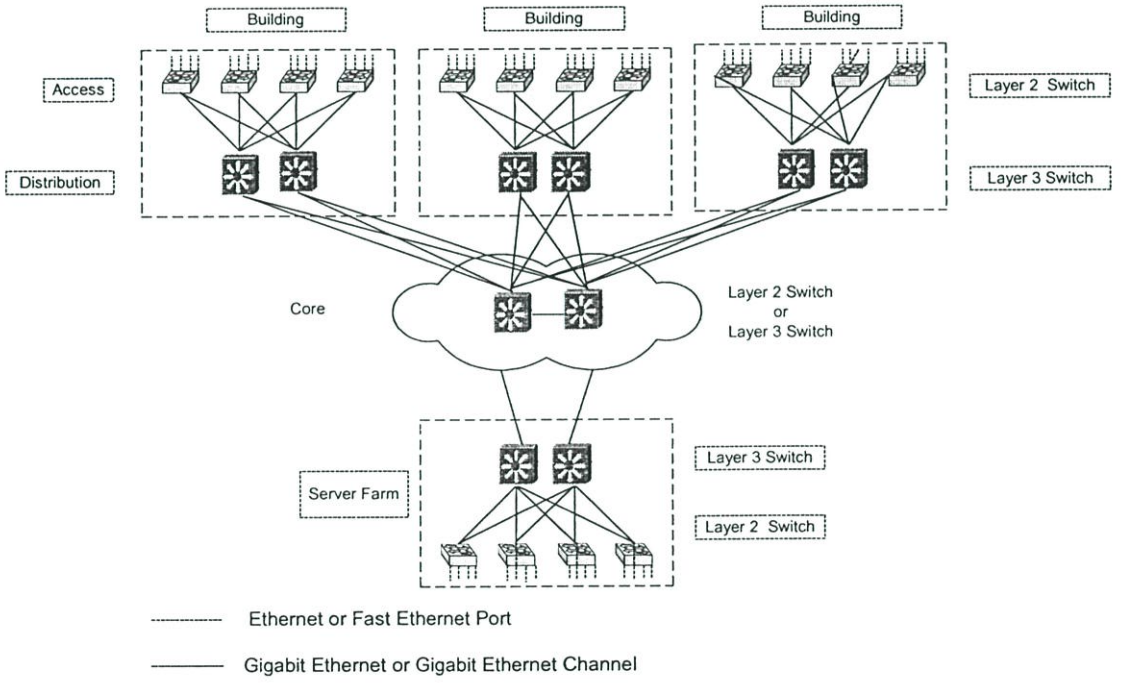
2.4 การออกแบบ Multilayer Campus

การออกแบบ multilayer campus ประกอบด้วย building block หลายๆ ตัวที่ถูกเชื่อมต่อข้ามแคมปัสแบ็คโบน รูปที่ 2.2 เป็นการออกแบบแคมปัสแบบทั่วๆ ไป ให้สังเกตุดูคุณลักษณะพิเศษ 3 ประการคือ การเข้าถึง (access) การกระจาย (distribute) และแกน (core) ในโมเดลทั่วไปสวิตช์เลเยอร์ 2 ถูกใช้ในระดับชั้นการเข้าถึง (access layer) ในขณะที่ สวิตช์เลเยอร์ 3 ถูกนำมาใช้ในเลเยอร์ distribution และ core ด้วย

จุดได้เปรียบประการหนึ่งของการออกแบบแคมปัส คือ scalability การติดตั้งอุปกรณ์ใหม่และเซิร์ฟเวอร์ฟาร์มสามารถเพิ่มได้อย่างโดยไม่ต้องเปลี่ยนแปลงการออกแบบ เส้นทางสำรองของ

บล็อก building ถูกขยายโดยเส้นทางสำรองในแบ็คโบน การแยกแบ็คโบนเลเยอร์ ทำได้โดยการตั้งค่าซึ่งจะประกอบด้วยสวิตช์ที่แยกกันอย่างน้อย 2 ตัวเสมอ ตามทฤษฎีสวิตช์เหล่านี้ควรถูกวางไว้ในอาคารที่ต่างกันเพื่อทำให้เกิดประโยชน์จากการทำเส้นทางสำรองมากที่สุด

การออกแบบ multilayer campus ใช้ประโยชน์ในการบริการเลเยอร์ 3 ได้หลายประการ ไม่ว่าการทำโหลดบาลานซ์และ failure recovery การจราจร ของ IP multicast ถูกจัดการผ่าน Protocol Independent Multicast (PIM) เพื่อจัดการเส้นทางในสวิตช์เลเยอร์ 3 access lists ถูกประยุกต์การใช้งานในเลเยอร์ distribution เพื่อการควบคุมนโยบาย granular การ บรอดคาสต์ถูกจำกัดไม่ให้ทำในแบ็คโบนแคมปัสโดยใช้ลักษณะเฉพาะของโปรโตคอลอย่างเช่น DHCP เพื่อเปลี่ยนกลับให้เป็น unicast ก่อนส่งต่อกลุ่มข้อมูลไปใน บล็อก building



รูปที่ 2.3: Dual Path for Fast Recovery

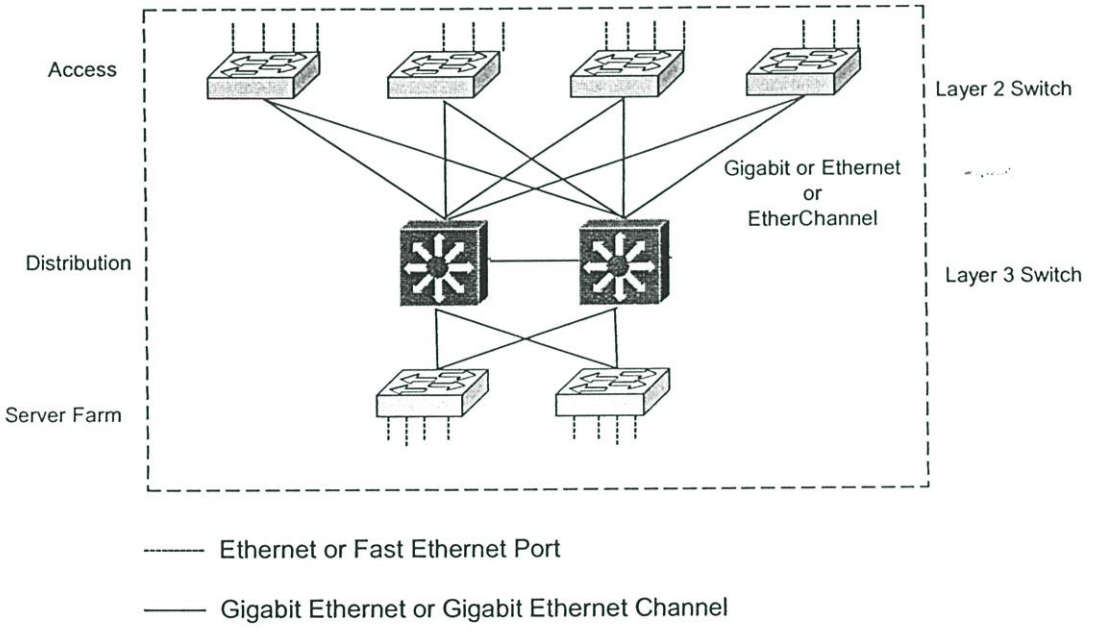
โมเดลแคมปัสทั่วไปดังแสดงในรูปที่ 2.2 ประกอบด้วยแต่ละเส้นทางที่ค่าคอส์ทที่เท่ากัน 2 เส้นทางในทุกโมดูล ในรูปที่ 2.3 แสดงให้เห็นถึงโมเดลภาวะเชื่อมต่อที่มีเส้นทางสำรองสูงสุด ซึ่งในแต่ละโมเดลมีสวิตช์ ในระดับชั้น distribution อย่างละ 2 ตัวที่มีค่าคอส์ทที่เท่ากันในแบ็คโบน โมเดลนี้ทำให้การกู้ความผิดพลาด (failure recovery) ที่รวดเร็วเนื่องจากสวิตช์ในระดับชั้น distribution ที่มีค่าคอส์ทที่เท่ากันค่าในตารางเส้นทาง (routing table) ของทุกเครือข่าย เมื่อเส้น

ทางการเชื่อมต่อหนึ่งเส้นทางไม่สามารถใช้งานได้ เส้นทางทั้งหมดก็จะถูกสับเปลี่ยนทางผ่านไปยังเส้นทางที่เหลืออยู่ในทันทีโดยใช้เวลาประมาณ 1 วินาทีหลังตรวจพบว่าเส้นทางนั้นใช้งานไม่ได้

แนวทางการออกแบบแบ็คโบนแคมปัส มี 5 ประการที่จะอธิบาย ดังต่อไปนี้มีแตกต่างเกี่ยวกับ scalability แบบต่างๆ ในขณะที่ยังรักษาข้อได้เปรียบของการให้บริการในระดับชั้นที่สามเอาไว้

2.4.1 Backbone---Small Campus Design

ค็อลแรพซแบ็คโบนประกอบด้วยสวิตช์เลเยอร์ 3 โดยใช้ 2 ตัวหรือมากกว่าในเครือข่าย การออกแบบอันนี้อาจเหมาะสมสำหรับเครือข่ายแคมปัสขนาดเล็ก ขนาดกลาง หรือเครือข่ายขนาดใหญ่ก็ได้ แต่ไม่แนะนำให้ใช้เครือข่ายแคมปัสที่ใหญ่มาก ความสามารถในการขยายเครือข่ายอันดับแรกที่ต้องคำนึงถึงคือข้อจำกัดในการจัดการบริหารเครือข่าย ซึ่งจะใช้



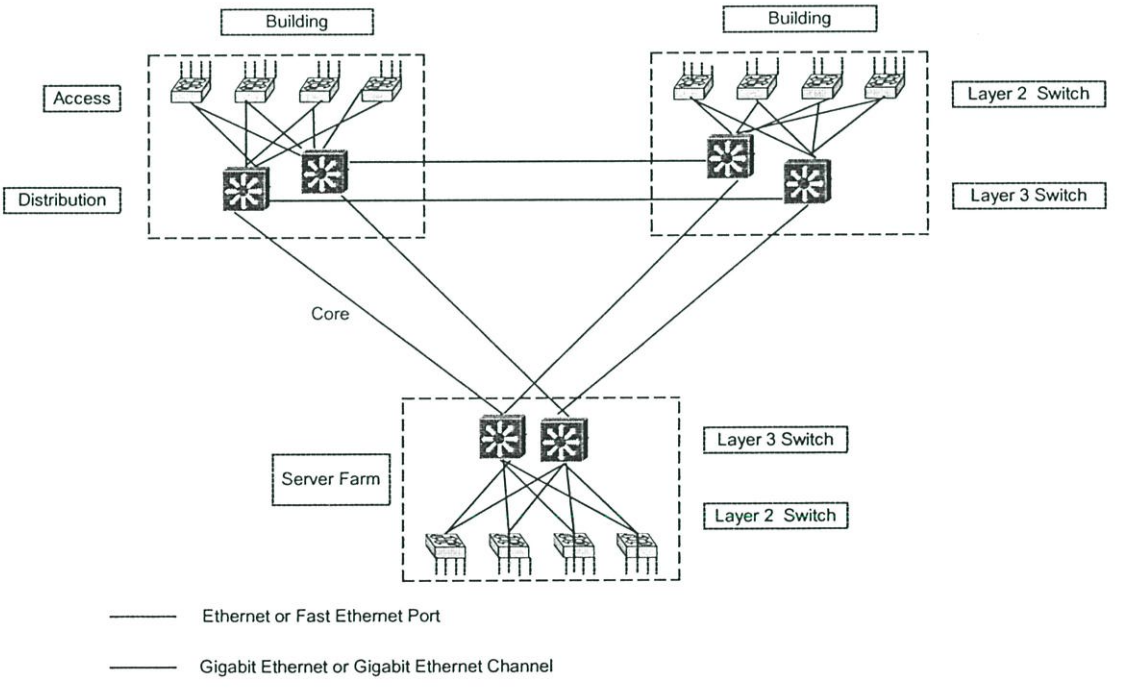
รูปที่ 2.4: Building Design or Collapsed Backbone Model

การพิจารณาการทำงานของสวิตช์เลเยอร์ 3 ในแบ็คโบนที่ต้องรักษา Address Resolution Protocol (ARP) ในทุกกิจกรรมของอุปกรณ์ในเครือข่าย ในการทำ ARP นั้น CPU จะถูกใช้งานค่อนข้างมากและสามารถแสดงผลทั้งหมดของแบ็คโบนได้ ทำให้สามารถแบ่งเครือข่ายแคมปัสขนาดที่ใหญ่กว่า ออกเป็น collapsed modules และทำให้เชื่อมต่อเครือข่ายเหล่านี้ด้วย core layer

รูป 2.4 แสดงรูปของค็อลแรพซแบ็คโบน เซิร์ฟเวอร์ฟาร์มถูกรวมต่อเข้าโดยตรงกับ ค็อลแรพซแบ็คโบน การใช้คำสั่ง passive อินเตอร์เฟสบน subnet อินเตอร์เฟสเพื่อทำให้ overhead ของ routing protocol น้อยลง

2.4.2 การรออกแบบวิทยาเขตขนาดเล็กโดยใช้โครงข่ายหลักแบบ Full-mesh (Full-Mesh Backbone---Small Campus Design)

แบ็คโบนแบบ full-mesh ประกอบด้วยสวิตช์เลเยอร์ 3 สูงถึง 3 โมดูลที่เชื่อมต่อถึงกันทั้งหมด เรียกการเชื่อมต่อแบบนี้ว่า full-connectivity mesh รูปที่ 2.5 แสดงเครือข่ายแคมปัสขนาดเล็กที่ใช้แบ็คโบนแบบ full-mesh การออกแบบแบ็คโบน full-mesh ในอุดมคตินั้นให้นึกถึงการเชื่อมโยง 2 โมดูล หรือ 3 โมดูลเข้าด้วยกัน อย่างไรก็ตามเมื่อส่วนประกอบกว่าหลายส่วนเพิ่มขึ้น จำนวนของลิงค์ก็ถูกต้องการมากขึ้นเพื่อรักษา full-mesh จำนวนของลิงค์ที่เพิ่มขึ้น ทำให้จำนวนของ subnets และ routing เพิ่มขึ้นทำให้เครือข่ายมีความซับซ้อนมากขึ้น



รูปที่ 2.5: Small Campus Network with Full-Mesh Backbone

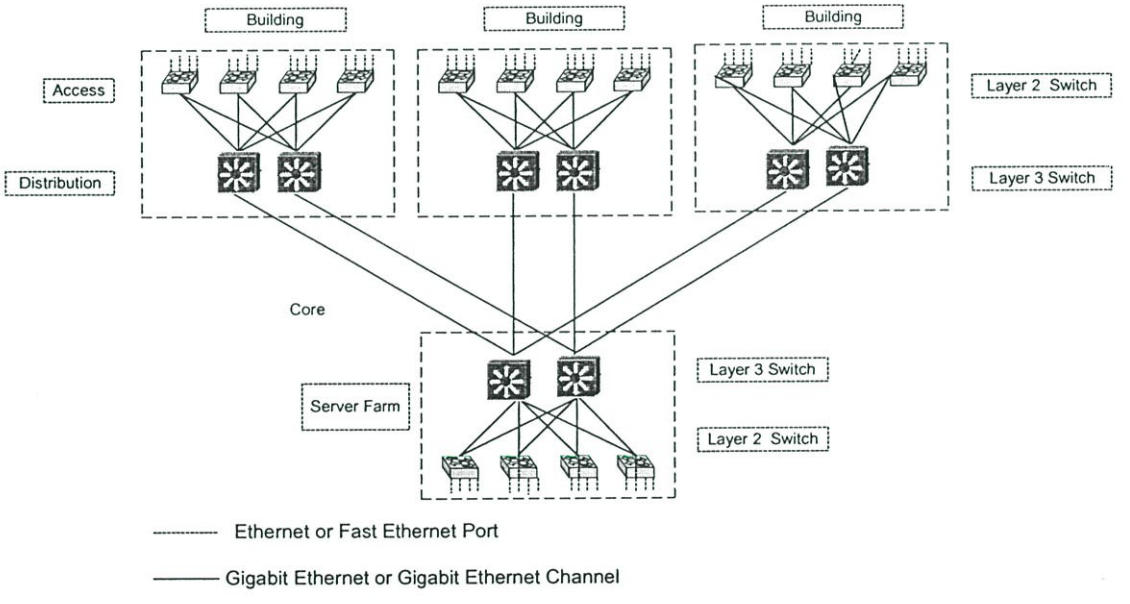
การออกแบบ full-mesh ทำให้การ upgrade แบนด์วิดท์ทำได้ยากขึ้น การ upgrade อาจหมายถึง การ upgrade จากอีเทอร์เน็ทความเร็วสูงไปเป็นกิกะบิตอีเทอร์เน็ท เนื่องจากการ upgrade นี้ทุกส่วนประกอบต้องทำในเวลาเดียวกันทั้งหมดในเครือข่ายแบบ full-mesh ดังนั้น

เพื่อทำให้ทุกอย่างง่ายขึ้นจึงใช้การเชื่อมต่อภายในระหว่างเลเยอร์ 2 หรือเลเยอร์ 3 กับโมดูล distribution แทน

2.4.3 การออกแบบวิทยาเขตขนาดเล็กโดยใช้โครงข่ายหลักแบบ Parlial Mesh (Partial Mesh---Small Campus Design)

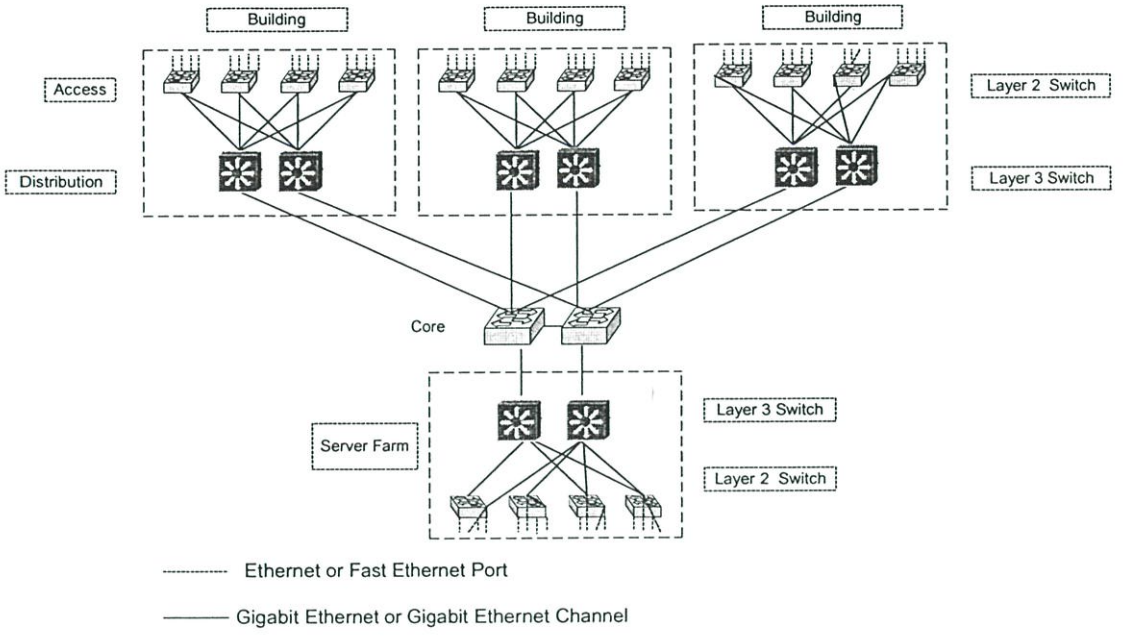
แบ็คโบนแบบ partial-mesh มีลักษณะที่เหมือนกับแบ็คโบน แบบ full-mesh แต่มีบางส่วนของทรั้งค์ที่ถูกเอาออกไป ในรูปที่ 2.6 แสดงถึงลักษณะของแคมปัสแบ็คโบนแบบ partial-mesh ที่เหมาะสมกับแคมปัสมีขนาดเล็ก โดยที่การจราจรทั้งหมดในเครือข่ายจะมีเซิร์ฟเวอร์เป็นศูนย์กลาง มีการวางทรั้งค์ที่มีความจุสูงจากสวิตช์เลเยอร์ 3 ในแต่ละอาคารทำการเชื่อมต่อไปยังสวิตช์เลเยอร์ 3 ในเซิร์ฟเวอร์ฟาร์มโดยตรง

ส่วนหนึ่งในการพิจารณาการออกแบบ partial-mesh คือการจราจรระหว่างเครื่องลูกข่ายที่ต้องการผ่านแบ็คโบนที่เกี่ยวกับทางตรรกถึง 3 ฮอบด้วยกัน ผลกระทบก็คือสวิตช์เลเยอร์ 3 ที่เซิร์ฟเวอร์ฟาร์มใช้งานแบ็คโบนไม่ได้ เมื่อมีการจราจรจาก client-to-client ใดๆ



รูปที่ 2.6: Partial-Mesh Campus Backbone

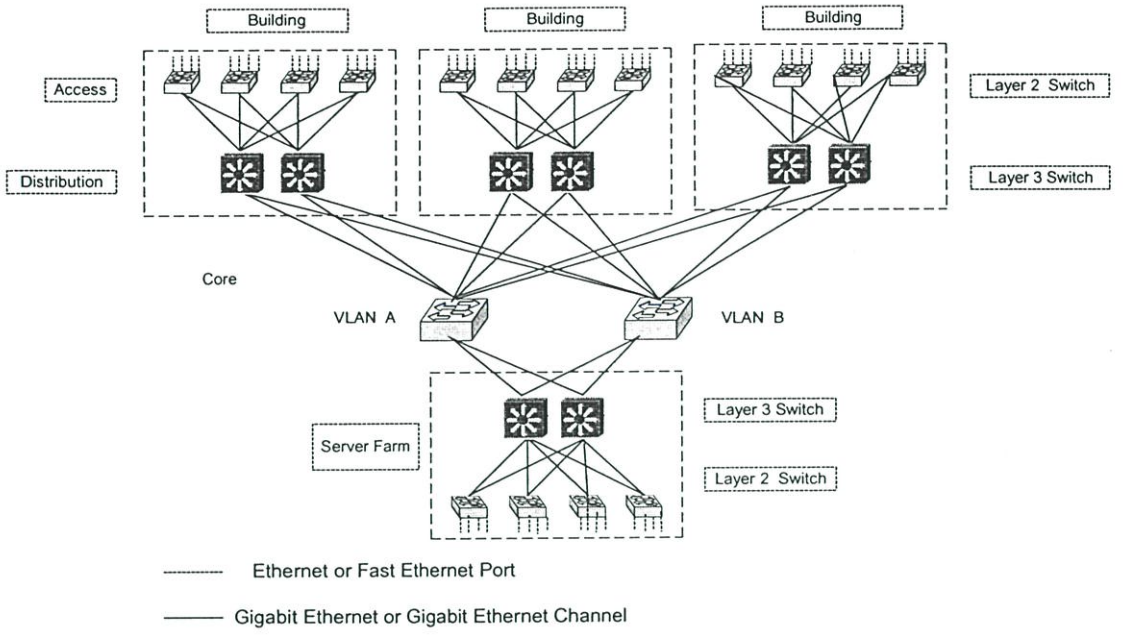
2.4.4 โครงข่ายหลักที่ใช้ สวิตช์ระดับชั้นที่สอง (Layer 2 Switched Backbone)



รูปที่ 2.7: Layer 2 Switched Backbone---Single VLAN

แบ็คโบนที่ใช้สวิตช์เลเยอร์ 2 เหมาะสมที่จะใช้กับแคมปัสที่จำนวนอาคาร มากกว่า 3 หลังที่จะเชื่อมโยงถึงกัน ในขณะที่การเพิ่มสวิตช์ในแบ็คโบน ทำให้จำนวนเส้นทางของการเชื่อมโยงน้อยกว่าและการเพิ่มส่วนประกอบอื่นๆ ในเครือข่ายสามารถทำได้โดยง่าย รูปที่ 2.7 แบ็คโบนมีการเชื่อมต่อของสวิตช์เลอยร์ 2 ตัวเดียวที่มี VLANใช้งานแบบสตาร์โทโปโลยี โดย IP subnet เดียวถูกใช้ในแบ็คโบนและสวิตช์ distribution แต่ละตัวจะทำการส่งการจราจรผ่านไปยังแบ็คโบน subnet เนื่องจากการออกแบบดังกล่าวจะไม่มีโอกาสเกิดลูป ดังนั้น spanning-tree จึงไม่ถูกนำมาใช้ แต่เพื่อป้องกันการลูป spanning-tree ถูกนำมาการเชื่อมต่อแบ็คโบนที่เราเตอร์ อินเตอร์เฟสแทนการเชื่อมต่อที่ VLAN

การหลีกเลี่ยงการลูปด้วย spanning-tree ด้วยสวิตช์เลเยอร์ 2 ถึง 2 ตัวในแบ็คโบน อย่างที่แสดงในรูปที่ 2.7 นั้นสามารถทำได้ง่าย อย่างไรก็ตามข้อจำกัดอันนี้ถูกกำกัดโดย scalability สูงสุดของการออกแบบแบ็คโบนเลอยร์ 2 ทั้งยังจำกัดการ broadcast และ multicast ทั้งหมดในแบ็คโบน โดยกิกะบิทอีเทอร์เน็ทแชนแนล สามารถใช้เพื่อลดขนาดแบนด์วิดท์ระหว่างสวิตช์แบ็คโบน โดยปราศจากการวนลูป

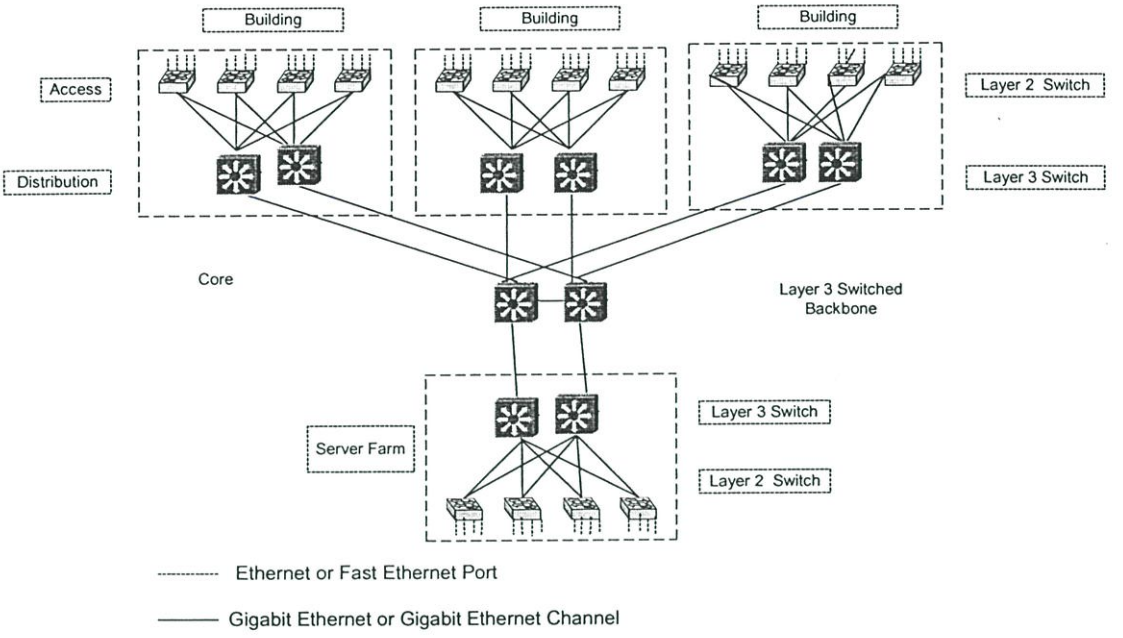


รูปที่ 2.8: Split Layer 2 Campus Backbone

อีกทางเลือกของการออกแบบเพื่อให้มีสภาพการใช้งานที่เป็นประโยชน์และความสามารถที่สูงกว่าได้แสดงในรูปที่ 2.8 ในรูปนี้ สวิตช์เลเยอร์ 2 ได้มีการเชื่อมต่อไปยังเส้นทางสำรองของ VLANs โดยแยกกันสิ้นเชิง ซึ่งสวิตช์ของ VLAN A ไม่มีการเชื่อมต่อกับสวิตช์ VLAN B เลย สวิตช์เลอยร์ 3 แต่ละตัวในระดับชั้น distribution จะมีทางผ่านที่มีค่าคอส์ท เท่ากัน 2 ค่าเพื่อทำการเชื่อมต่อไปยังสวิตช์ระดับชั้น distribution ทุกๆ ตัวเสมอ ซึ่งได้ตั้งค่าไว้บน ตารางเส้นทางเลเยอร์ 3 นั่นเอง ถ้าเส้นทางผ่าน VLAN A ถูกตัด สวิตช์เลเยอร์ 3 จะทำการย้ายการจราจรทั้งหมดข้างต้นผ่านเส้นทาง VLAN B โดยทันที

ข้อได้เปรียบของการออกแบบโดยการแยกแบ็คโบนเลเยอร์ 2 คือเส้นทางผ่านที่เท่ากัน 2 ค่าทำให้การรวมตัวในเส้นทางใหม่ทำได้อย่างรวดเร็ว นอกจากนี้ข้อได้เปรียบในเรื่องที่อาจใช้งานได้มากขึ้นเนื่องจากไม่ต้องส่ง hello packet เพราะไม่ถูกจำกัดเรื่องโปรโตคอล ความพิเศษเพิ่มเติมของการออกแบบแบ็คโบนคู่ก็คือความสัมพันธ์ของการเชื่อมต่อสวิตช์แบ็คโบนกับสวิตช์ใน distribution แต่ละตัว

2.4.5 โครงข่ายหลักที่ใช้ สวิตช์เลเยอร์ 3 (Layer 3 Switched Backbone)

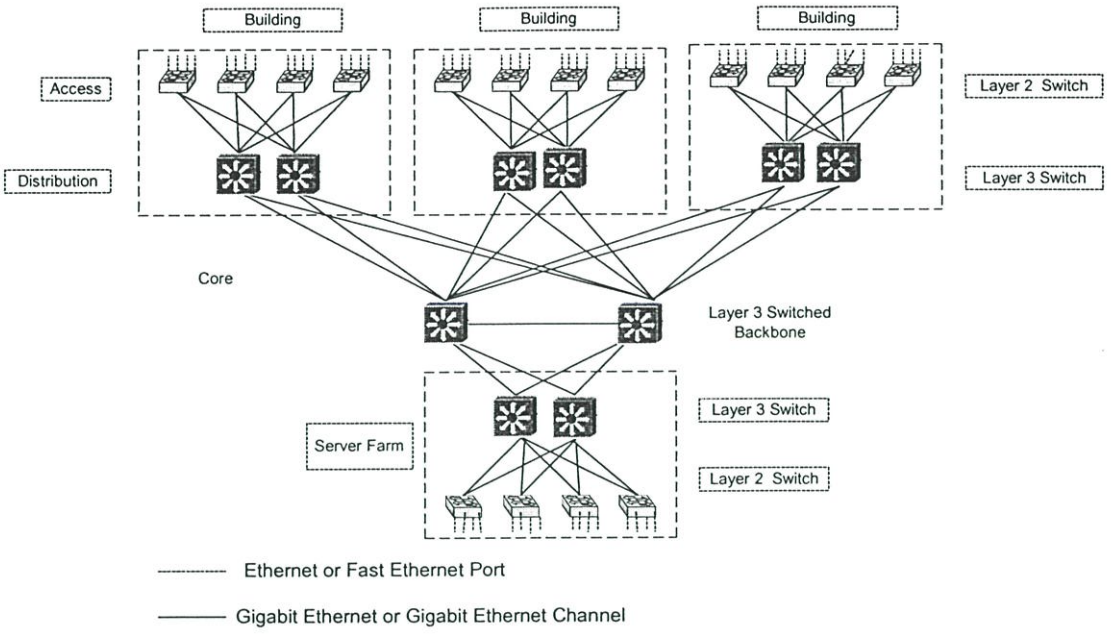


รูปที่ 2.9 Layer 3 Switched Campus Backbone

แคมปัสแบ็คโบนที่สามารถปรับปรุงและปรับเปลี่ยนขนาดได้ง่ายที่สุด ก็คือแคมปัสที่ประกอบด้วยสวิตช์รเลเยอร์ 3 ดังที่ได้แสดงในรูปที่ 2.9 สวิตช์แบ็คโบนทำการเชื่อมต่อกิกะบิทอีเทอร์เน็ทหรือกิกะบิทอีเทอร์แชนแนล ให้ถึงกัน สวิตช์แบ็คโบนเลเยอร์ 3 มีจุดได้เปรียบหลายๆ ประการดังนี้

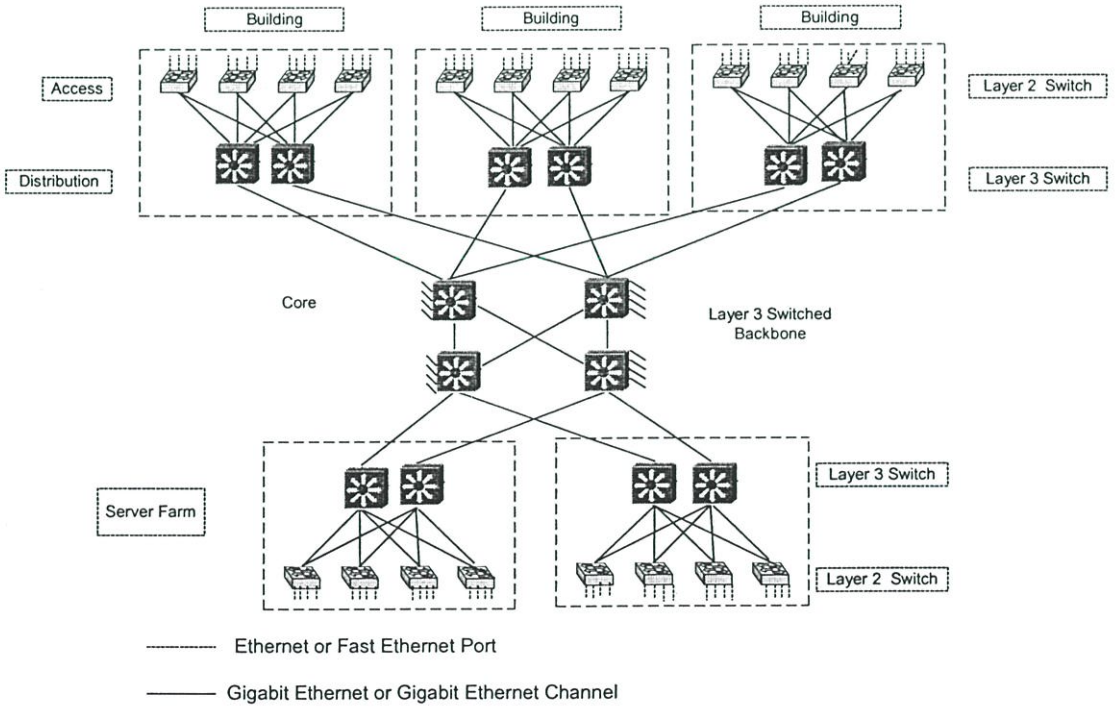
- ลดจำนวนของเราเตอร์ลง
- มีความยืดหยุ่นเนื่องจากไม่มี spanning-tree loops
- การ broadcast และ multicast ควบคุมโดยแบ็คโบน
- Scalability มีขนาดที่ใหญ่ตามความต้องการ

รูปที่ 2.10 ชี้ให้เห็น สวิตช์แคมปัสแบ็คโบนเลเยอร์ 3 ที่มีสวิตช์ในเลเยอร์ distribution เป็นวงจรคู่ จุดสำคัญของการออกแบบอันนี้ก็คือสวิตช์แต่ละตัวในเลเยอร์ distribution จะมีค่าคอส์ทที่เท่ากัน 2 เส้นทางเพื่อทำการเชื่อมต่อไปยังทุกเครือข่ายปลายทาง ดังนั้นเมื่อเส้นทางการเชื่อมต่อใดๆ ไม่สามารถใช้งานได้ก็จะมีการฟื้นตัวของเส้นทางการเชื่อมอื่นอย่างรวดเร็ว การออกแบบนี้จะทำให้ความจุของแบ็คโบนมีสูงเป็นสองเท่าของการออกแบบปกติ



รูปที่ 2.10 แบ็คโบนเลเยอร์ 3 (Dual Paths for Fast Recovery)

รูปที่ 2.11 แสดงให้เห็นถึงการใช้สวิตช์เลเยอร์ 3 เป็นแบ็คโบนแคมปัส (layer 3 switched campus backbone) ในเครือข่ายขนาดใหญ่ โดยสวิตช์แบ็คโบนได้เพิ่มการใช้เราติ้งโปรโตคอล



รูปที่ 2.11: Large-Scale Layer 3 Switched Campus Backbone

อย่างเช่น IGRP หรือ OSPF กันอย่างแพร่ในรูปดังกล่าวประกอบด้วยสวิตช์เลเยอร์ 3 ทั้งหมด 4 ตัว ในการเชื่อมต่อแบบกิกะบิทอีเทอร์เน็ทหรือกิกะบิทอีเทอร์แชนแนล ซึ่งทุกเส้นทางการเชื่อมต่อของแบ็คโบนเป็นการเชื่อมต่อถึงกันหมดโดยไม่มี spanning-tree loop เลย จากภาพไดอะแกรมที่มีอยู่คือการเชื่อมต่อหลายกิกะบิทสวิตช์แบ็คโบน

2.5 Multilayer Switch Feature Card (MSFC)

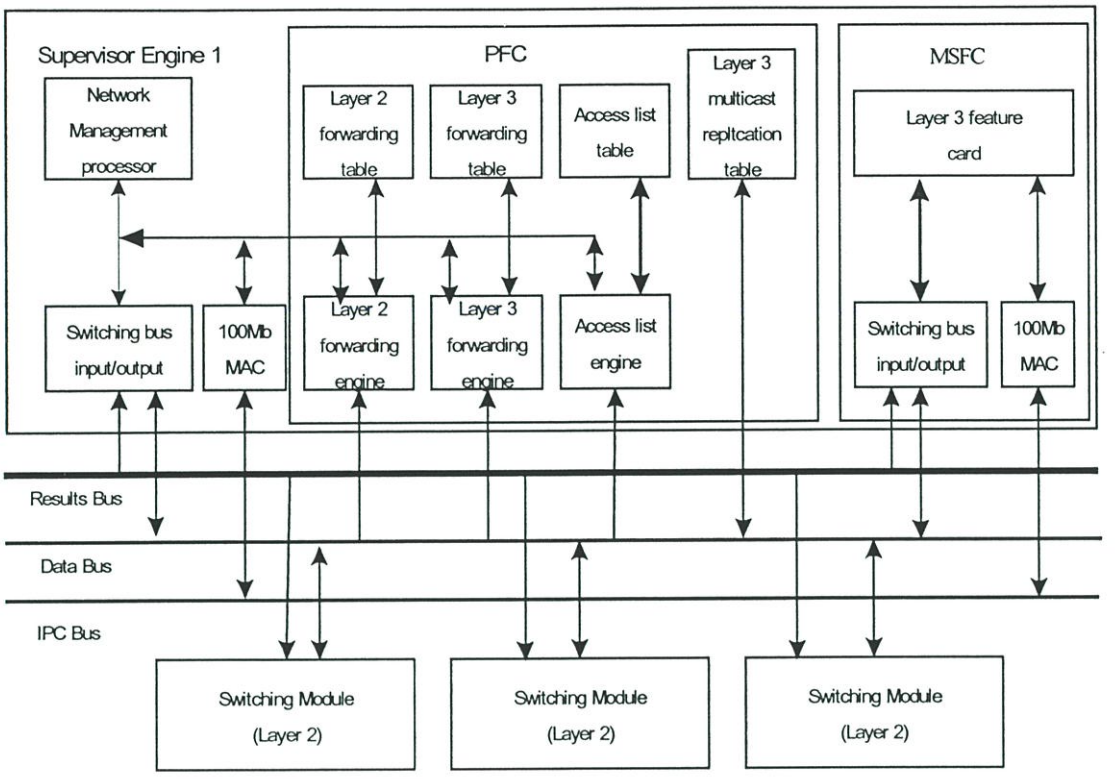
Multulayer Switch Feature Cars (MSFC) ทำหน้าที่จัดหาเส้นทางให้กับ multiplayer switching (MLS) ที่มีความเร็วในการสลับเส้นทางมากที่สุดถึง 15 Million packets per second (Mpps) เพื่อทำการอินเตอร์เฟสกับอีเทอร์เน็ทสวิตช์ โดยการทำงานของ MLS นั้นสามารถรองรับการใช้งานของโปรโตคอลต่างๆ เช่น IP,IP multicast และ Inter Network Packet Exchange (IPX)

PFC จะยึดเอาข้อมูลในตารางสวิตช์เลเยอร์ 3 (layer 3 switch table) เพื่อทำโฟลว์สวิตช์ โดยเมื่อมีข้อมูลใหม่เข้ามาการทำเก็บข้อมูลการจราจรไว้ โดยข้อมูลจะถูกส่งไป update ในแทนเด็ม หลังจากนั้น MLS cache ก็ถูกสร้างขึ้นบน cached information และ MLS cache ก็จะทำการเก็บข้อมูลนี้เพื่อเป็น active flows

MLS หรือสวิตช์เลเยอร์ 3 ทำการรวบรวมเราติ้งของสวิตชิ่ง เพื่อส่งไปยัง throughput ในปริมาณของการส่งที่สูงมาก ผ่านไปยัง inter-processor communication (IPC) bus จากรูป MSFC และ PFC บน supervisor engine MSFC ประกอบด้วย MLS application-specific (ASICs) และ MLS route processor ซึ่งทำหน้าที่ประมวลผลเส้นทาง โดยการคำนวณเส้นทางและทำการส่งต่อข้อมูลไปยังตาราง Forwarding information base (FIB)

แพ็กเกตกลุ่มแรกในตารางก็จะถูกประมวลผลเส้นทางและถูกส่งปลายทางโดยใช้วิธีส่งแบบเดิม ในขณะที่ Supervisor Engine เรียนรู้ข้อมูลทั้งหมดที่จำเป็นต่อการที่จะส่งข้อมูลเหล่านั้นไปทางฮาร์ดแวร์ เพื่อส่งต่อไปยังตัวประมวลผลเส้นทาง supervisor engine จะปฏิบัติการทั้งระดับชั้นทั้งสามและทำการเขียนสันทาง ที่รับมาจากเราเตอร์ใหม่ๆ

MSFC Redundancy สามารถทำการ config card MSFC เพื่อให้ทำงานในโหมด Hot Standby Routing Protocol (HSRP) ได้ โดยจะทำการสำรอง routing อัตโนมัติแก่เครือข่าย HSRP ใช้งานร่วมกันได้กับ IPX และ AppleTalk. HSRP ยะยอมให้ MSFC (router) หนึ่งตัว ทำหน้าที่แทนโดยอัตโนมัติเมื่อ MSFC ตัวอื่นทำงานไม่ได้



รูปที่ 2.12 โครงสร้าง MSFC

ในการใช้ HSRP คุณต้องมีโครงแบบข้างล่างอย่างใดอย่างหนึ่งคือ :

1. มี supervisor engine 2 อันใน single chassis (redundant supervisor engines) โดยที่แต่ละ supervisor engine ต้องมี MSFCและ PFC ถูกติดตั้งไว้

2. มี supervisor engine 2 chassis โดยจะต้องมี supervisor engine 1อันที่ติดตั้ง MSFCและPFC

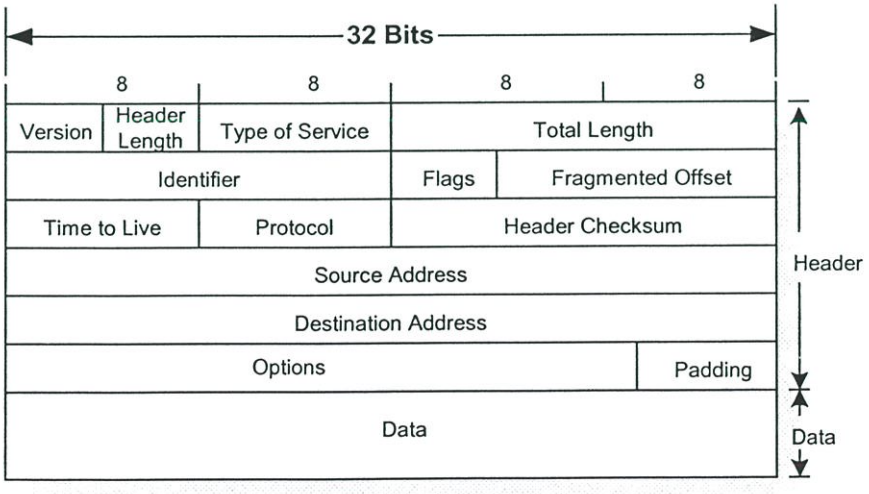
บทที่ 3
การสร้างและการหาเส้นทางการสื่อสาร

บทนี้จะอธิบายถึงการทำ IP Routing ในเลเยอร์สามแบบพื้นฐาน ซึ่งเป็นการใช้เส้นทางการส่งข้อมูลที่ดีที่สุดและการเชื่อมโยงถึงกันในตารางเส้นทาง เพื่อใช้ในการแยกแยะว่าแพ็กเก็ตควรจะเดินทางจากจุด A ไปยังจุด B ได้อย่างไร รวมทั้งต้องมีเทคโนโลยีเครือข่ายสำรองในศูนย์ข้อมูล ถ้าหากส่วนประกอบหลักเกิดการเสียหายขึ้นมา ส่วนประกอบสำรองจะเข้ามาทำงานแทนที่และเริ่มต้นขั้นตอนสลับการทำงาน

ส่วนในเรื่องของระบบเชื่อมต่อการสื่อสารสำรองนั้นคุณสมบัติ Standby Tracking ของ HSRP จะคอยเฝ้าดูอินเตอร์เฟส WAN ในเราเตอร์จากนั้นคอยแยกแยะว่าวงจรสื่อสารที่เชื่อมต่อกับเราเตอร์นั้นใช้งานได้หรือไม่ ถ้าหากซอฟต์แวร์เจอปัญหาของการสื่อสาร ระบบจะโอนไปยังอินเทอร์เฟซ WAN ที่พร้อมทำงานได้ของเราเตอร์สำรอง

โพรโตคอล TCP/IP เป็นโพรโตคอลที่ทำงานอยู่ในชั้นโครงข่ายซึ่งมีการเชื่อมต่อแบบ Connection oriented โดยมีอุปกรณ์การสื่อสารซึ่งเรียกว่า เราเตอร์ (router) ทำหน้าที่ในการส่งผ่านข้อมูลของผู้ใช้ในรูปของ IP ดาต้าแกรม กระบวนการในการตัดสินใจเลือกเส้นทางในการส่ง IP ดาต้าแกรมในแต่ละตัวจึงเป็นประเด็นหลักที่ต้องได้รับการพิจารณาและการออกแบบอย่างมีประสิทธิภาพ เพื่อให้การรับส่ง IP ดาต้าแกรมมีความรวดเร็วและมีความผิดพลาดน้อยที่สุด

3.1 โครงสร้างของ IP Header



รูปที่ 3.1 โครงสร้าง IP ดาต้าแกรม

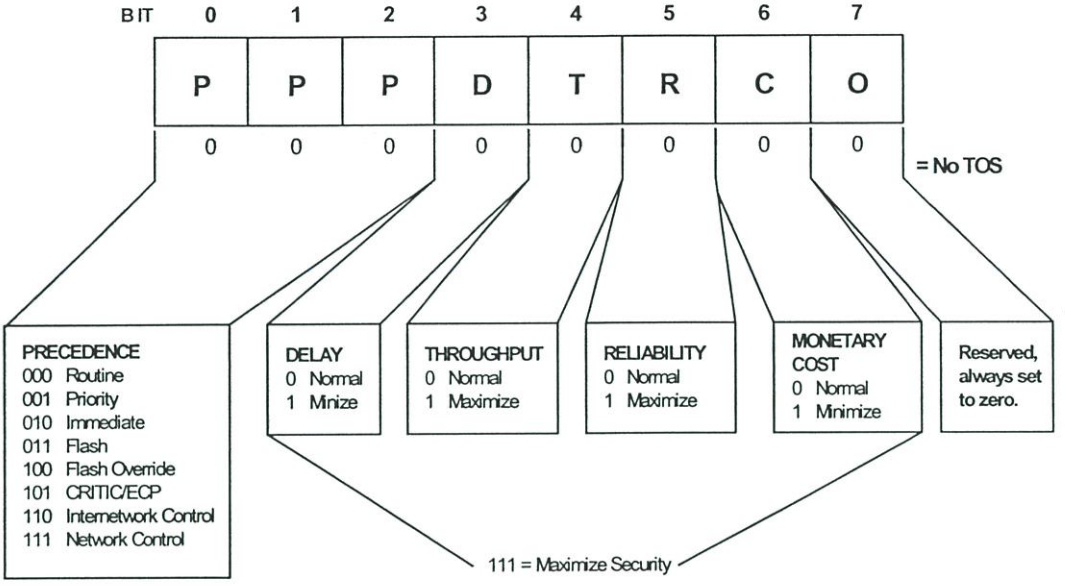
ในรูปที่ 3.1 แสดงถึงรูปแบบโครงสร้างของ IP Header โดยขนาดของ IP Header ปกติจะมีขนาด 20 ไบต์ จากภาพจะแสดงให้เห็นถึงส่วนประกอบของ IP ดาต้าแกรมซึ่งประกอบด้วยองค์ประกอบหลัก 2 ส่วนคือ ส่วนของ Header และส่วนของข้อมูล (data)

- ฟิลด์ Version: ระบุเวอร์ชันของ IP ที่ใช้ในการสร้าง IP ดาต้าแกรมในฟิลด์นี้จะมีขนาด 4 บิตซึ่งปกติจะเซ็ทเป็น 0100 ในระบบของเลขฐานสอง ซึ่งแสดงถึงเวอร์ชัน 4 (IPv4) ซึ่งเป็นเวอร์ชันที่ใช้อยู่ในปัจจุบัน ในตารางที่ 3.1 แสดงให้เห็นถึงเวอร์ชันในแบบต่าง ๆ ที่สัมพันธ์กันกับ RFC

ตารางที่ 3.1 แสดงหมายเลขเวอร์ชันของ IP

Number	Version	RFC
0	Reserved	
1-3	Unassigned	
4	Internet Protocol (IP)	791
5	ST Datagram Mode	1190
6	Simple Internet Protocol (SIP)	
6	IPng	1883
7	TP/IX	1475
8	P Internet Protocol (PIP)	1621
9	TCP and UDP over Bigger Address (TUBA)	1347
10-14	Unassigned	
15	Reserved	

- ฟิลด์ Header Length: มีขนาด 4 บิตใช้บอกขนาด Header ของ IP โดยจะบอกในรูปของ word ขนาด 32 บิต ซึ่งปกติจะมีขนาดเท่ากับ 5 หรือเทียบเท่ากับ 20 ไบต์ และถ้าหากมีฟิลด์ Option เพิ่มเข้ามาจะทำให้ขนาดของ Header เท่ากับ 24 ไบต์
- ฟิลด์ Type of Service (TOS): มีขนาด 8 บิต ใช้สำหรับบ่งบอกถึงคุณลักษณะหรือรูปแบบการให้การบริการที่แพ็กเก็ต IP ต้องการ ในฟิลด์นี้สามารถแบ่งออกได้เป็น 2 ส่วน คือ ส่วนของ Precedence และส่วนของ TOS ดังในรูปที่ 3.2 ส่วนของ Precedence นั้นมีจำนวน 3 บิตใช้สำหรับจัดลำดับความสำคัญของแพ็กเก็ตซึ่งมีได้ 8 ระดับ ในส่วนของ TOS มีไว้เพื่อใช้ในการเลือกการบริการในการส่งมอบแพ็กเก็ตในรูปของ Delay Throughput Reliability และ Monetary cost



รูปที่ 3.2 ฟิลด์ Type of Service

- ฟิลด์ Total Length: มีขนาด 16 บิตใช้สำหรับระบุขนาดของ IP ดาต้าแกรมทั้งหมดซึ่งรวม Header ด้วย ขนาดของ IP ดาต้าแกรมที่ใหญ่ที่สุดมีค่าเท่ากับ 65,535 ไบต์
- ฟิลด์ Identifier: มีขนาด 16 บิตใช้ในการเชื่อมต่อฟิลด์ Flags และฟิลด์ Fragment Offset สำหรับการแบ่งแพ็กเก็ตออกเป็นแพ็กเก็ตย่อย ๆ ซึ่งแพ็กเก็ตจะถูกทำ fragment เพื่อทำให้เป็นแพ็กเก็ตย่อย ๆ ก็ต่อเมื่อความยาวของแพ็กเก็ตที่มาจากต้นทางมีความยาวมากเกินกว่าค่า Maximun Transmission Unit (MTU) ของดาต้าลิ้งค์ ในแต่ละเส้นทางที่แพ็กเก็ตนี้เดินทางผ่าน เช่น มีแพ็กเก็ตขนาด 5,000 ไบต์ที่จะต้องเดินทางผ่านเครือข่ายร่วมซึ่งมีค่า MTU เป็น 1,500 ไบต์ เพราะฉะนั้นภายในเฟรมหนึ่ง ๆ จะสามารถบรรจุขนาดของแพ็กเก็ตได้สูงสุด 1,500 ไบต์ ทำให้เราเตอร์ซึ่งบรรจุแพ็กเก็ตไปบนดาต้าแกรม ทำการ fragment แพ็กเก็ตแต่ละแพ็กเก็ตให้มีขนาดไม่เกิน 1,500 ไบต์ จากนั้นเราเตอร์จะทำการ mark แพ็กเก็ตซึ่งถูก fragment แล้วด้วยหมายเลขเดียวกันในฟิลด์ Identifier ซึ่งจะทำให้อุปกรณ์ทางด้านรับสามารถระบุได้ว่าแพ็กเก็ตที่ถูก fragment นั้นเป็นแพ็กเก็ตเดียวกัน
- ฟิลด์ Flags: เป็นฟิลด์ที่มีขนาด 3 บิตโดยที่บิตแรกไม่มีการใช้งานและกำหนดให้เป็น 0 เสมอ บิตที่สองเรียกว่าบิต Don't Fragment (DF) มีไว้เพื่อกำหนดว่า IP ดาต้าแกรมนี้อนุญาตให้ทำ fragment ได้หรือไม่ ถ้า Host ต้นทางกำหนดให้ DF=0 ก็หมายถึงอนุญาตให้เราเตอร์ระหว่างทางทำการ fragment ได้ถ้ามีความจำเป็น แต่ถ้าหากเซ็ท DF=1 หมายความว่าห้ามทำการ fragment ในกรณีนี้ถ้าหากเราท์เตอร์ไม่สามารถส่งดาต้าแกรมต่อไป

ได้หากไม่มีการทำ fragment เราเตอร์ก็จะทิ้งดาต้าแกรมนั้นไป และส่งความผิดพลาดที่เกิดขึ้นกลับไปยังโฮสต์ต้นทาง บิตที่สามเรียกว่าบิต More Fragments (MF) เป็นบิตที่ถูกเซ็ทโดยเราเตอร์เมื่อมีการทำ fragment กับ IP ดาต้าแกรมนั้น โดยจะมีค่า MF=0 เพื่อแสดงว่า fragment นั้นเป็นส่วนสุดท้ายของ IP ดาต้าแกรมและจะเซ็ทให้ MF=1 เพื่อแสดงว่ายังมี fragment อื่นตามมาอีก เพราะฉะนั้นฟิลด์ flag จึงเป็นตัวระบุให้โฮสต์ปลายทางทราบจุสิ้นสุดของ IP ดาต้าแกรมมีข้อสังเกตว่า เมื่อ fragment ในแต่ละส่วนอาจจะถูกส่งผ่านเครือข่ายด้วยเส้นทางที่แตกต่างกัน และ fragmnet เหล่านี้อาจเดินทางมาถึงจุดหมายในลำดับที่ผิดไปจากเดิมได้ ดังนั้นหากโฮสต์ปลายทางได้รับ fragment ที่บอกว่าเป็น fragment สุดท้าย แต่แท้จริงแล้วโฮสต์ปลายทางได้รับ fragment ของ IP ดาต้าแกรมยังไม่ครบถ้วนสมบูรณ์ ซึ่งจะเห็นได้ว่า การใช้เพียงฟิลด์ Identifier และ Flag จะไม่เพียงพอสำหรับโฮสต์ ปลายทางที่จะนำ fragment มาประกอบกันได้อย่างถูกต้อง เพราะขาดข้อมูลที่บอกถึงลำดับการเรียงต่อของ fragment ปัญหานี้สามารถแก้ไขได้โดยอาศัยฟิลด์ Fragment Offset ที่จะได้กล่าวต่อไป

- ฟิลด์ Fragment Offset: ทำหน้าที่ชี้หรือระบุตำแหน่งเริ่มต้นของส่วนย่อยแต่ละส่วนภายใน IP ดาต้าแกรมฟิลด์นี้มีขนาด 13 บิต โดยค่าที่ใช้มีหน่วยเป็นจำนวนเท่าของ 8ไบท์ เมื่อโฮสต์ปลายทางอ่านค่าฟิลด์นี้ประกอบกับฟิลด์ Total length ของ fragment ที่ได้รับแต่ละตัว ก็จะทำให้สามารถตรวจสอบว่าได้รับ fragment ของ IP ดาต้าแกรมครบถ้วนหรือไม่
- ฟิลด์ Time to Live (TTL): มีขนาด 8 บิตมีหน้าที่กำหนดจำนวนเราเตอร์สูงสุดที่ IP ดาต้าแกรมสามารถเดินทางผ่านได้ หรือกล่าวในอีกนัยหนึ่งได้ว่าเป็นการกำหนดอายุของ ดาต้าแกรมที่อนุญาตให้อยู่ในเครือข่ายได้ ขั้นตอนในการทำงาน คือ เมื่อโฮสต์ต้นทางทำการส่งดาต้าแกรมออกไปจะตั้งค่าเริ่มต้นให้กับฟิลด์ TTL ค่าหนึ่ง (โดยทั่วไปใช้ 32 หรือ 64) ทุกครั้งที่ดาต้าแกรม เดินทางผ่านเราท์เตอร์ตัวหนึ่งค่าของ TTL จะถูกปรับลดลงหนึ่งหน่วย หากเมื่อใดเราเตอร์พบดาต้าแกรมที่ค่า TTL ลดลงจนเป็น 0 เราเตอร์จะตัดดาต้าแกรม นั้นทิ้งไปพร้อมกับแจ้งให้โฮสต์ต้นทางทราบ การทำเช่นนี้จะทำให้สามารถป้องกัน IP ดาต้าแกรมที่รับส่งผิดพลาดได้
- ฟิลด์ Protocol: เป็นฟิลด์ที่มีขนาด 8 บิต ใช้ระบุว่าดาต้าแกรมที่ได้รับเป็นโปรโทคอลที่ใช้เชื่อมโฮสต์กับโฮสต์หรือเป็นระดับชั้น Transport แบบใด ดังแสดงตัวอย่างของโพรโตคอลบางรูปแบบในตารางที่ 3.2
- ฟิลด์ Header Checksum: มีขนาด16 บิตเป็นฟิลด์ที่ทำหน้าที่ตรวจสอบความถูกต้องของ IP header โดยมีลักษณะการทำงานดังนี้ เมื่อโฮสท์ต้นทางทำการสร้างดาต้าแกรมขึ้นจะคำนวณค่า header checksum โดยนำ header ทีละ 16 บิตมาบวกกันแบบหนึ่งต่อหนึ่ง

คอมโพแนนซ์ จากนั้นนำผลที่ได้มาทำหนึ่งต่อหนึ่งคอมโพแนนซ์อีกครั้ง จึงจะได้เป็นค่าที่บรรจุลงใน header checksum โดยที่ด้านรับจะตรวจสอบความผิดพลาดของ header โดยนำ header ทีละ 16 บิตมาบวกกับค่าในฟิลด์ header checksum แบบหนึ่งต่อหนึ่งคอมโพแนนซ์ หากผลลัพธ์ที่ได้มีค่าเป็นหนึ่งทั้งหมด แสดงว่าไม่มีความผิดพลาดเกิดขึ้น หากไม่ใช่ก็แสดงว่ามีความผิดพลาดเกิดขึ้นกับ header ในกรณีนี้ IP ดาต้าแกรมจะถูกตัดทิ้งโดยไม่มีการแจ้งความผิดพลาดที่เกิดขึ้น ซึ่งโพรโตคอลในชั้นที่สูงกว่าต้องตรวจสอบปัญหานี้ด้วยตัวเอง

- ฟิลด์ที่อยู่ต้นทางและที่อยู่ปลายทาง: คือที่อยู่ IP ของต้นทางและของปลายทาง มีขนาด 32 บิต

ตารางที่ 3.2 ตัวอย่างค่าภายในฟิลด์โพรโตคอล

Protocol Number	Host-to-Host Layer Protocol
1	Internet Control Message Protocol (ICMP)
2	Internet Group Management Protocol (IGMP)
3	Gateway to Gateway Protocol (GGP)
4	IP in IP
6	Transmission Control Protocol (TCP)
8	Exterior Gateway Protocol (EGP)
17	User Datagram Protocol (UDP)
35	Inter-Domain Policy Routing Protocol (IDPR)
45	Inter-Domain Routing Protocol (IDRP)
46	Resource Reservation Protocol (RSVP)
47	Generic Routing Encapsulation (GRE)
54	NBMA Next Hop Resolution Protocol (NHRP)
88	Cisco Internet Gateway Routing Protocol
89	(IGRP)
	Open Shortest Path First (OSPF)

- ฟิลด์ Option: เป็นส่วนที่เพิ่มเติมเมื่อมีการใช้งานบางอย่าง เช่น การทดสอบเครือข่ายและตรวจหาจุดผิดพลาดของระบบ ฟิลด์นี้จะมีขนาดไม่ตายตัวขึ้นอยู่กับชนิดของ

option ที่เลือกใช้ เช่น Loose source routing Strict source routing Record route และ Timestamp เป็นต้น

- ฟิลด์ Padding: เป็นส่วนต่อท้ายฟิลด์ Option เพื่อทำให้มีขนาดครบ 32 บิต โดยทำการเติมศูนย์ต่อท้ายให้จนครบจำนวน 32 บิต

3.2 IP Routing

IP Routing เป็นกระบวนการค้นหาเส้นทางในการส่งผ่านข้อมูลจากต้นทางไปยังที่หมายปลายทางโดยผ่านการส่งต่อของอุปกรณ์ IP ที่อยู่ในเน็ตเวิร์กซึ่งจะช่วยกันทำหน้าที่ส่งต่อข้อมูลไปจนกว่าข้อมูลจะถึงปลายทาง กลไกสำคัญที่ทำให้ IP เป็นโปรโทคอลสำหรับขนส่งข้อมูลไปยังทุกๆที่ในโลกบนอินเตอร์เน็ตที่ดีที่สุดในขณะนี้คือการที่ IP มีกระบวนการ IP Routing นี้เอง สิ่งที่น่าสนใจที่สุดของ IP Routing คือการที่ต้นทางและปลายทางของการสื่อสารนั้นในบางโอกาสต่างก็อยู่กันแสนไกล การสื่อสารข้อมูลแต่ละครั้ง ข้อมูลจะต้องเดินทางผ่านโครงข่ายอันสลับซับซ้อนมากมาย แต่ในที่สุดข้อมูลก็สามารถส่งถึงกันได้ในเวลาอันรวดเร็วเป็นที่น่าอัศจรรย์ โครงข่ายอินเตอร์เน็ตคงไม่อาจเกิดขึ้นได้หากไม่มีโพรโตคอล IP ที่ช่วยขนส่งข้อมูลไปบนเครือข่ายอย่างมีประสิทธิภาพ การเข้าใจถึงกระบวนการ IP Routing จะช่วยให้เราเข้าใจคุณสมบัติของอินเตอร์เน็ตได้เป็นอย่างดี กระบวนการ IP Routing นี้ได้ถูกออกแบบมาอย่างชาญฉลาดและรัดกุมพอสมควรในอันที่จะให้บรรลุภารกิจในการส่งข้อมูล หลักการพื้นฐานของ IP Routing เริ่มต้นข้อกำหนดที่เรียบง่ายดังนี้

อุปกรณ์ที่ใช้ในเน็ตเวิร์ค จำแนกได้เป็น 2 ประเภทคือ

- Host โฮสต์เป็นอุปกรณ์ที่ทำหน้าที่ให้กำเนิดข้อมูลในกรณีเป็นผู้ส่ง หรือทำหน้าที่รับข้อมูลไปใช้งานในกรณีเป็นผู้รับ การสื่อสารข้อมูลใดๆจะต้องเป็นการสื่อสารจากโฮสต์ไปยังโฮสต์เสมอ สำหรับ IP Packet แล้วข้อมูลในเฮดเดอร์ที่ปรากฏอยู่ในฟิลด์ที่อยู่ต้นทางและที่อยู่ปลายทาง ซึ่งเรียกว่า IP Address จะเป็นหมายเลขระบุตำแหน่งของโฮสต์ต้นทางและโฮสต์ปลายทางเท่านั้น
- Router เราเตอร์เป็นอุปกรณ์สำคัญอย่างยิ่งสำหรับ IP ที่จะทำให้การขนส่งข้อมูลเป็นไปอย่างสมบูรณ์ เราเตอร์ทำการส่งผ่านข้อมูลจากเน็ตเวิร์กหนึ่งไปยังอีกเน็ตเวิร์กหนึ่ง ตำแหน่งของเราเตอร์จะอยู่ในจุดที่เชื่อมต่อระหว่างสองเน็ตเวิร์กเข้าด้วยกัน ด้วยข้อกำหนดของ IP ข้อมูลจะส่งไปถึงกันโดยตรงข้ามเน็ตเวิร์คไม่ได้ จะต้องอาศัยเราเตอร์เป็นผู้ทำหน้าที่ส่งผ่านข้อมูลไปให้ ดังนั้นเน็ตเวิร์คของ IP ถึงแม้มิได้ต่อถึงกันในทางกายภาพแต่ก็สามารถสื่อสารกันได้โดยอาศัยเราเตอร์เป็นตัวเชื่อมประสานเข้าด้วยกัน

ก่อนที่จะอธิบายกลไกเบื้องต้นของกระบวนการ IP Routing ขออธิบายถึงส่วนสำคัญอีกส่วนหนึ่งที่เกี่ยวข้องกับกระบวนการนี้พอเป็นสังเขปเพื่อทำความเข้าใจในเรื่องของ IP Routing เนื่องจากจะมีการกล่าวถึงในส่วนนี้พอสมควรนั่นคือเน็ตเวิร์ค ในที่นี้จะกล่าวถึงเฉพาะเน็ตเวิร์คในความหมายของ IP (IP Network) เท่านั้น ไม่รวมถึงเน็ตเวิร์คประเภทอื่น ใน IP นั้นจะมีการระบุหมายเลขประจำโฮสต์โดยใช้ที่อยู่ IP เพื่อระบุตำแหน่งของต้นทางและปลายทาง โดยในที่อยู่ IP นั้นนอกจากจะระบุตำแหน่งของโฮสต์แล้ว ยังใช้ระบุตำแหน่งของเน็ตเวิร์คที่โฮสต์นั้นเชื่อมต่ออยู่ด้วย ทั้งนี้โพรโตคอล IP มีกระบวนการที่จะแยกหมายเลขประจำตัวของโฮสต์และของเน็ตเวิร์กออกจากกัน เพื่อทำให้อุปกรณ์ทั้งหลายสามารถพิจารณาได้ในทันทีว่าจะส่งข้อมูลที่ได้รับมานั้นไปในทิศทางใด

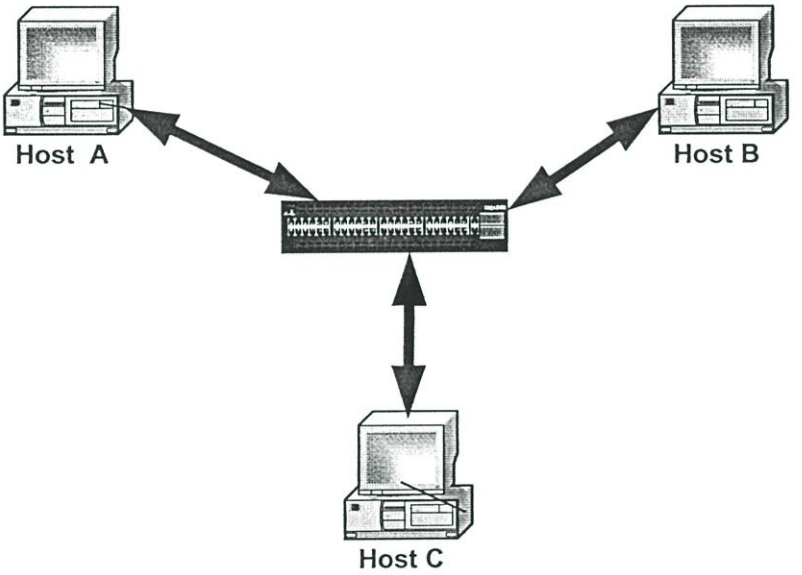
เนื่องจาก IP เป็นโพรโตคอลที่อยู่ในระดับชั้นที่สูง จะต้องอาศัยการทำงานที่สอดคล้องกันของโพรโตคอลที่อยู่ในระดับชั้นที่ต่ำกว่าด้วย หมายเลขเน็ตเวิร์คของ IP เป็นค่าที่เป็นลอจิคัล คือ กำหนดขึ้นเองหรืออาจเปลี่ยนแปลงได้โดยมิได้ผูกติดกับอุปกรณีทางกายภาพ แต่อย่างไรก็ตาม การกำหนดหมายเลขเน็ตเวิร์คของ IP ก็จำเป็นต้องสอดคล้องกับหมายเลขเน็ตเวิร์กของระดับชั้นล่างด้วยเช่นกัน นั่นหมายความว่าถึงแม้ว่าในระดับชั้นที่ต่ำกว่าเช่นระดับชั้นลิ้งค์จะเชื่อมต่อถึงกันอย่างสมบูรณ์ แต่ถ้ามีการกำหนดค่าของ IP เน็ตเวิร์คไม่ถูกต้องก็จะไม่สามารถสื่อสารได้ ในทางกลับกันถึงแม้มีการกำหนดค่า IP เน็ตเวิร์คที่ถูกต้องแต่เน็ตเวิร์กไม่สามารถสื่อถึงกันได้ในระดับชั้นลิ้งค์ ก็ไม่สามารถสื่อสารได้เช่นกัน

3.2.1 **หลักการพื้นฐานของ** IP Routing

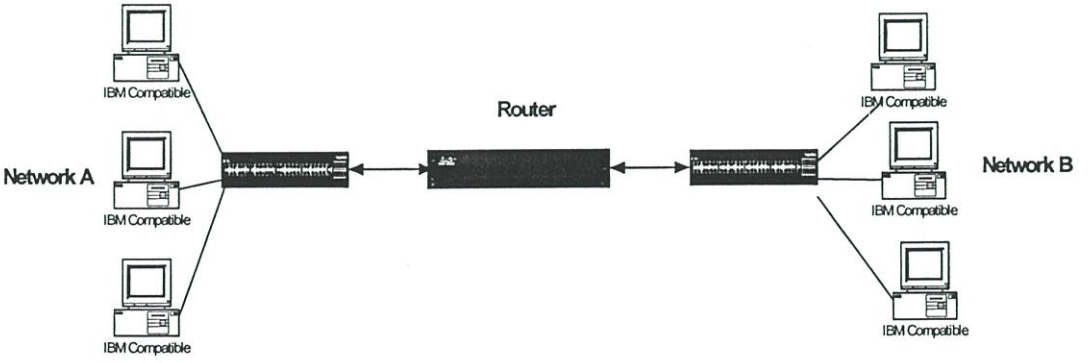
IP Routing โดยใช้ Default Router กระบวนการ IP Routing เริ่มต้นด้วยหลักพื้นฐานที่ไม่สลับซับซ้อนและเข้าใจได้ไม่ยากคือ

รูปที่ 3.3 การสื่อสารในการเชื่อมต่อแบบจุดต่อจุด

1. ถ้าโฮสต์ต้นทางและปลายทางต่อถึงกันโดยตรงเช่นการเชื่อมต่อแบบจุดต่อจุด ตามปรากฏในรูปที่ 3.3 IP ข้อมูลหรือดาต้าแกรมนั้นจะถูกส่งไปยังโฮสต์ปลายทางโดยตรง
2. ถ้าโฮสต์ต้นทางและปลายทางต่อเชื่อมร่วมอยู่ในเน็ตเวิร์คเดียวกัน เช่น อีเธอร์เน็ตหรือโทเค็นริงดังแสดงในรูปที่ 3.4 IP ดาต้าแกรมก็จะส่งไปยังโฮสต์ปลายทางโดยตรง
3. ถ้าไม่เป็นไปตามข้อที่ 1 และ 2 IP ดาต้าแกรมจะถูกส่งไปยังดีฟอลต์เราเตอร์ เพื่อทำการส่งต่อข้อมูลไปยังปลายทางต่อไป
4. เมื่อเราเตอร์ได้รับ IP ดาต้าแกรมจากข้อ 3 แล้วตรวจสอบดู หากพบว่าโฮสต์ปลายทางต่อร่วมอยู่บนเน็ตเวิร์คเดียวกันกับเราเตอร์ ให้ทำการส่งดาต้าแกรมไปที่โฮสต์นั้น หากไม่ได้ต่อร่วมกันก็ส่งดาต้าแกรมไปที่เราเตอร์ตัวต่อไป และกลับไปที่ขั้นตอนในข้อ 2 ใหม่จนกว่า IP ดาต้าแกรมจะเดินทางถึงปลายทางหรือหมดเวลาในการส่ง

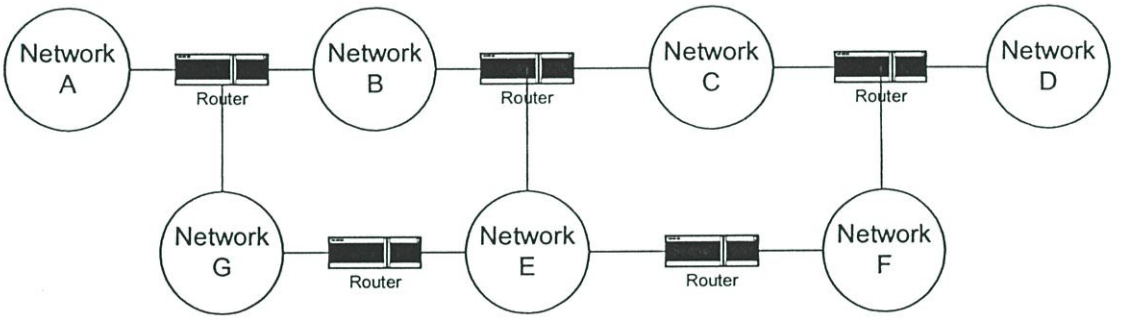


รูปที่ 3.4 การสื่อสารในเน็ตเวิร์คที่ต่อร่วมกัน (Shared network)



รูปที่ 3.5 การสื่อสารระหว่าง 2 เน็ตเวิร์ค

หากเน็ตเวิร์คมีเพียง 2 เน็ตเวิร์คเหมือนในภาพที่ 3.3 มีเพียงแค่ดีฟอลต์เราเตอร์ก็คงจะเพียงพอและการทำงานในการส่ง IP ดาต้าแกรมข้ามระหว่างเน็ตเวิร์คก็คงจะไม่ยุ่งยากมากนักและคงเป็นไปตามขั้นตอนข้างต้น หากสังเกตจะเห็นว่าตัวเราเตอร์เองนั้นจะมีเน็ตเวิร์กที่ต้องติดต่อด้วย 2 ฝั่งคือ เน็ตเวิร์ค A และเน็ตเวิร์ค B ซึ่งมีทิศทางการเคลื่อนที่ของข้อมูลเพียงเส้นทางเดียวมีเราเตอร์เพียงตัวเดียว ไม่ว่าปลายทางของข้อมูลจะไปที่ใดหากมิใช่อยู่ในเน็ตเวิร์คเดียวกันแล้วดาต้าแกรมทั้งหมดก็ต้องส่งผ่านเราเตอร์อยู่ดีโดยไม่ต้องทำการวิเคราะห์ใดๆ การที่ดาต้าแกรมถูกส่งข้ามเน็ตเวิร์ค 1 ครั้งที่เรียกว่า 1 ฮอบ (hop) เปรียบเสมือนระยะในการเดินทางของข้อมูล จากภาพตัวอย่างดาต้าแกรมเดินทางจากโฮสต์ต้นทางเพียง 1 ฮอบก็ถึงโฮสต์ปลายทาง การส่งต่อข้อมูลโดยเราเตอร์ก็มีเพียงส่งไปและส่งกลับระหว่างเน็ตเวิร์ค A และเน็ตเวิร์ค B เท่านั้น แต่หากระยะทางถึงโฮสต์ปลายทางจะต้องเดินทางมากกว่า 1 ฮอบแล้ว เราเตอร์ก็จะทำงานยุ่งยากซับซ้อนเพราะจะมีเน็ตเวิร์คอื่นๆ ที่ไม่ได้เชื่อมต่อโดยตรงและต้องส่งข้อมูลผ่านเราเตอร์หลายตัวและมีหลายเส้นทางที่ดาต้าแกรมสามารถเดินทางไปได้ ดังนั้นการส่งต่อดาต้าแกรมของเราเตอร์จึงเป็นปัจจัยสำคัญในการกำหนดประสิทธิภาพของ IP Routing



รูปที่ 3.6 การเชื่อมต่อกันของหลายเน็ตเวิร์ค

การเดินทางของดาต้าแกรมโดยกระบวนการ IP routing นั้นทำงานอยู่บนพื้นฐานของการส่งข้อมูลทีละฮอบ (hop-by-hop) คือเราเตอร์เองจะทำงานโดยรู้จักเฉพาะเน็ตเวิร์กที่ต่ออยู่กับตัวเองเท่านั้น หากโฮสต์ปลายทางมมิได้อยู่ในเน็ตเวิร์คที่ต่อเชื่อมอยู่ก็จะทำการส่งข้อมูลต่อไปอีกฮอปให้แก่เราเตอร์ตัวต่อไปส่งต่อและถือว่าหมดหน้าที่ต่อดาต้าแกรมนั้นแล้วเพราะส่งข้อมูลต่อไปเรียบร้อยแล้ว ส่วนจะถึงปลายทางหรือไม่นั้นเป็นอีกเรื่องหนึ่ง และเราเตอร์ตัวอื่นๆ ที่อยู่ระหว่างทางก็เช่นกันก็จะส่งต่อดาต้าแกรมไปเรื่อยๆ เช่นนั้นทีละฮอบจนกว่าจะถึงปลายทางหรือหมดเวลา

เพื่อให้กระบวนการ IP Routing ดำเนินไปอย่างมีประสิทธิภาพจึงมีการเพิ่มความสามารถของเราเตอร์ให้มากขึ้นกล่าวคือ ในกรณีที่โฮสต์ปลายทางมิได้อยู่ในเน็ตเวิร์กที่ต่อยู่กับตัวเองนั้น

แทนที่จะทำการส่งต่อข้อมูลไปยังดีฟอลต์เราเตอร์ทั้งหมด ก็ให้เราเตอร์ทำการพิจารณาเน็ตเวิร์กปลายทางว่าอยู่ที่ใดแล้วจึงทำการส่งต่อดาต้าแกรมนั้นไปยังเราเตอร์ที่อยู่ใกล้กับเน็ตเวิร์กนั้นที่สุด (ใช้จำนวนฮอบในการส่งข้อมูลน้อยที่สุด) เพื่อการนี้จึงจำเป็นต้องมีข้อมูลให้แก่ตัวเราเตอร์ว่าเน็ตเวิร์คใดควรจะส่งข้อมูลไปยังเราเตอร์ใด ข้อมูลเหล่านี้จะเก็บอยู่ในตารางเส้นทาง (Routing Table) ซึ่งจะประกอบด้วยข้อมูลดังนี้

- Destination IP Address: หมายถึงแอดเดรสของโฮสต์หรือเน็ตเวิร์คปลายทาง
- IP Address of a next-hop router: หมายถึง IP Address ของเราเตอร์ตัวอื่นที่ต่อโดยตรงอยู่บนเน็ตเวิร์คเดียวกัน
- Flags: จะเป็นข้อมูลส่วนที่ขยายความเพิ่มเติมของ Destination IP Address และ Next-hop router
- Interface: หมายถึงอินเตอร์เฟซของเราเตอร์ที่จะต้องใช้เพื่อการส่งดาต้าแกรมออกไป

เมื่อเราเตอร์มีตารางเส้นทางแล้ว กระบวนการในการที่จะส่งต่อดาต้าแกรมจากเราเตอร์ตัวหนึ่งไปยังตัวต่อไปจะต้องนำข้อมูลในเราต์ติ้งเทเบิลไปร่วมพิจากรณาด้วยดังนี้

1. ค้นหาข้อมูลในตารางเส้นทางเพื่อหา IP Address ที่ตรงกันพอดีกับ IP Address ของโฮสต์ปลายทางของดาต้าแกรม หากพบข้อมูลดังกล่าวให้ส่งไปยังแอดเดรสที่ระบุอยู่ในฟิลด์ของ Next-hop router ทันที หากไม่พบข้อมูลให้ทำต่อในข้อที่ 2
2. ค้นหาในเราต์ติ้งเทเบิ้ลเพื่อหาเน็ตเวิร์กแอดเดรสที่ตรงกับเน็ตเวิร์กแอดเดรสของโฮสต์ปลายทาง หากพบข้อมูลดังกล่าวให้ส่งไปยังแอดเดรสที่ระบุอยู่ในฟิลด์ของ Next hop router ทันที หากไม่พบข้อมูลให้ทำต่อในข้อที่ 3
3. ค้นหาในตารางเส้นทางเพื่อหาข้อมูลรายการที่ระบุว่า " default " และให้ส่งต่อไปยังแอดเดรสที่ระบุอยู่ในฟิลด์ของ Next-hop router

กระบวนการที่กล่าวมานี้จะทำให้การส่งต่อข้อมูลเป็นไปในทิศทางที่เหมาะสมและมีประสิทธิภาพที่สุด โดยอาศัยข้อมูลที่กำหนดไว้ก่อนแล้วของเราเตอร์ ซึ่งหากไม่พบข้อมูลที่ตรงกับโฮสต์หรือเน็ตเวิร์กเลยในเราต์ติ้งเทเบิ้ลแล้วดาต้าแกรมก็จะถูกส่งไปยังดีฟอลต์เราเตอร์เสมอ ดังนั้นหากเราเตอร์แต่ละตัวต่างก็มีตารางเส้นทางที่ถูกต้องแล้ว ดาต้าแกรมก็จะถูกส่งต่อไปเรื่อยๆ จนถึงปลายทางในที่สุด อาจจะล่าช้าหรือไม่มีประสิทธิภาพบ้างแต่ก็พอใช้งานได้

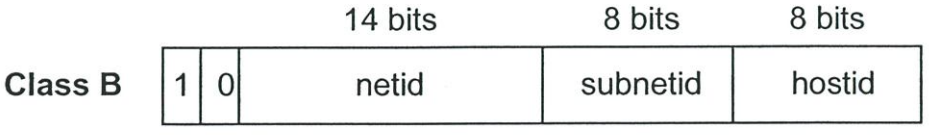
จะเห็นได้ว่าเราเตอร์จำเป็นต้องเก็บตารางเส้นทางของทุก ๆ เน็ตเวิร์คหรือทุกๆ โฮสต์ไว้ทั้งหมด แต่จะอาศัยการกระจายกันของข้อมูลในเราเตอร์ทุกๆ ตัวบนเน็ตเวิร์คและแต่ละตัวก็ส่งต่อข้อมูลให้ถูกต้อง ข้อมูลก็จะสามารถเดินทางถึงปลายทางได้ ด้วยเหตุนี้เองทำให้เน็ตเวิร์คสามารถขยายเพิ่มเติมออกไปได้เรื่อยๆ โดยไม่จำกัดและไม่ต้องทำการแก้ไขโครงสร้างของเน็ตเวิร์กเดิม อินเตอร์เน็ตจึงแผ่ขยายครอบคลุมโลกได้อย่างรวดเร็ว

อย่างไรก็ตาม IP Routing โดยการใช้ตารางเส้นทางเป็นกระบวนการพื้นฐานเท่านั้น เมื่อนำมาซ้อนจนเกินกว่าจะใช้การเราติ้งแบบธรรมดาได้ จึงจำเป็นต้องมีกระบวนการที่มีประสิทธิภาพกว่านี้และมีการพัฒนากระบวนการ IP Routing ที่สลับซับซ้อนออกมาหลายรูปแบบเช่น RIP, OSPF, BGP เป็นต้น

3.2.2 Subnet Addressing

ในตอนเริ่มต้นใช้โพรโตคอล TCP/IP นั้นการแบ่ง IP Address ออกเป็นแอดเดรสของเน็ตเวิร์ค (netid) และแอดเดรสของโฮสต์ (hostid) เป็นไปตามกติกาที่ระบุของแต่ละคลาส ต่อมามีผู้เสนอให้มีการแบ่งเน็ตเวิร์คย่อยภายในแต่ละ netid เพิ่มขึ้นอีกเพื่อจะได้ใช้งาน IP Address ได้อย่างมีประสิทธิภาพที่สุด เนื่องจากในคลาส A และคลาส B นั้นมีการจัดสรรส่วนที่เป็น hostid ในแต่ละเน็ตเวิร์คเป็นจำนวนมากคือในเน็ตเวิร์คคลาส A แต่ละเน็ตเวิร์คนั้นสามารถมีจำนวนโฮสต์ได้มากถึง = 16,777,214, โฮสต์ และสำหรับในแต่ละเน็ตเวิร์คคลาส C นั้นสามารถมีจำนวนโฮสต์ได้สูงที่สุดถึง = 65,534 โฮสต์ ซึ่งการที่จะนำ IP Address มาใช้อย่างทั่วถึงนั้นมีโอกาสเป็นไปได้ยากมาก ทั้งคลาส A และ คลาส B เพราะมีโอกาสน้อยมากที่จะมีเน็ตเวิร์คใดในโลกมีจำนวนโฮสต์มากมายขนาดนั้นอยู่ภายในเน็ตเวิร์คเดียว ดังนั้น IP Address ที่จัดสรรไปให้ในแต่ละเน็ตเวิร์คของคลาสเหล่านี้จึงถูกใช้ไม่หมดและไม่สามาถนำไปใช้ประโยชน์ที่อื่นได้

การทำ Subnet คือการแบ่งเน็ตเวิร์คย่อยภายในเน็ตเวิร์คหลักเพื่อให้แต่ละเน็ตเวิร์กมีขนาดที่เหมาะสมกับปริมาณโฮสต์ที่มีอยู่ โดยใช้หลักการเดียวกับการนำ IP Address มาแยกออกเป็น Host id และเป็น Network id คือแทนที่จะให้ค่า Host id เป็นค่าอิสระตั้งแต่ 1 จนถึงค่าสูงสุด ก็ทำการจัดกลุ่มของ Host id เหล่านั้นออกเป็นกลุ่มของเน็ตเวิร์คย่อย คือนำค่าในส่วนที่เป็น Host id เดิมมาแยกออกเป็นสองส่วนคือ Subnet id และ เป็น Host id ใหม่ ซึ่งจะทำให้สามารถจัดสรรการใช้งาน IP Addressได้อย่างเหมาะสมกับการมีอยู่จริงของโฮสต์ในแต่ละเน็ตเวิร์ค



รูปที่ 3.7 IP Address ในคลาส B เมื่อทำการ Subnet

รูปที่ 3.7 แสดงการจัดแบ่ง IP Address ของคลาส B ออกเป็นเน็ตเวิร์คย่อยด้วยวิธี Subnetting โดยแบ่งพื้นที่ส่วนที่เป็นของ host id เดิมออกเป็น 2 ส่วน โดยเป็นของ subnetid ขนาด 8 บิด และ hostid ใหม่ที่มีขนาดเล็กลงเหลือเพียง 8 บิท

ตารางที่ 3.3 ผลกระทบต่อจำนวนของขนาดของเน็ตเวิร์คเมื่อถูก Subnet

Class B	จำนวนเน็ตเวิร์กที่มีได้	จำนวนโฮสต์สูงสุดในแต่ละเน็ตเวิร์ก
เดิม	16,382	65,532
หลังการ Subnet	4,161,028	254

ผลที่ได้คือขนาดของเน็ตเวิร์คจะเล็กลงและมีจำนวนมากขึ้น จากเดิม 16,382 เน็ตเวิร์คก็เพิ่มเป็น 4,161,028 (16,382 * 254) และในขณะเดียวกันจำนวนโฮสต์ในแต่ละเน็ตเวิร์คจะลดลงจาก 65,532 เหลือเพียง 254 โฮสต์ อย่างไรก็ตามการ Subnet นั้นไม่จำเป็นต้องมีขนาดของ subnet id คงที่ตายตัวเสมอไป ผู้บริหารระบบสามารถปรับเปลี่ยนได้ตามความเหมาะสมของการใช้งาน เช่นอาจจะมีจำนวนเน็ตเวิร์คน้อยลง และจำนวนโฮสต์มากขึ้นก็สามารถกระทำได้โดยการแบ่งขนาดของ subnet id และ host id ใหม่ตามที่ต้องการ

นอกจากการที่สามารถใช้ IP Address ได้อย่างมีประสิทธิภาพแล้ว ข้อดีอีกอย่างหนึ่งของการ Subnet คือช่วยให้ประสิทธิภาพการสื่อสารดีขึ้นด้วย กล่าวคือ กระบวนการของ TCP/IP บางประการมีการใช้การสื่อสารแบบบรอดคาส (broadcast) เพื่อทำการสื่อสารกระจายไปทุกๆ โฮสต์ที่อยู่ในเน็ตเวิร์คเดียวกัน ดังนั้นหากเป็นเน็ตเวิร์คคลาส A ซึ่งมีโฮสต์ได้ถึง 16 ล้านโฮสต์แล้วการสื่อสารด้วยวิธีบรอดคาสท์แต่ละครั้งจะเป็นการกระจายข้อมูลไปยังเครื่องอื่นๆ จำนวนมาก และใช้แบนวิดธ์มากมายมหาศาลทั่วไปทั้งเน็ตเวิร์ค ส่งผลกระทบต่อการสื่อสารตามปกติอย่างยิ่ง และหากเน็ตเวิร์คประเภทนี้ถูกโจมตีโดยเทคนิคที่อาศัยการขยายสัญญาณเนื่องจากการบรอดคาสท์ เช่น Smurf แล้วก็มีโอกาสมากที่การสื่อสารข้อมูลภายในเน็ตเวิร์คจะเป็นอัมพาตได้อย่างรวดเร็วจากการถูกโจมตะเพียงแพ็กเก็ตเดียว ผู้ออกแบบเน็ตเวิร์คส่วนใหญ่จึงมักจะหลีกเลี่ยงการออกแบบให้เน็ตเวิร์คมีขนาดใหญ่เกินไป เนื่องจากควบคุมได้ยุ่งยากและมีประสิทธิภาพต่ำ วิธีการ Subnet จึงเป็นส่วนที่ถูกนำมาใช้ในการออกแบบเสมอ

โดยทั่วไปแล้วเรามักจะพบเห็นการ Subnet สำหรับ IP Address ในคลาส B เสียเป็นส่วนใหญ่ เนื่องจากคลาส B มีผู้ใช้งานกันแพร่หลาย ส่วนคลาส A จะพบได้ไม่บ่อยนักเพราะมีผู้ได้รับจัดสรรไม่มาก ส่วนคลาส C ก็อาจจะพอมีผู้ทำ Subnet อยู่บ้าง แต่เนื่องจากคลาส C มีขนาดของเน็ตเวิร์คไม่ใหญ่อยู่แล้ว จึงสามารถแบ่งย่อยออกไปได้อีกๆไม่มากนัก อย่างไรก็ตาม IP Address ทุกคลาสล้วนแต่สามารถถูกนำมา subnet ได้ทั้งสิ้น

3.2.3 Subnet Mask

หากกล่าวถึงการ Subnet Mask ด้วย การที่มีเฉพาะ IP Address เพียงอย่างเดียวนั้น กรณีที่เป็นการกำหนด netid และ hostid ตามที่ระบุในคลาสต่างๆ นั้นเราก็สามารถทราบว่าค่าทั้งสองได้ไม่ยากนัก โดยพิจารณาว่า IP Address อยู่ในช่วงใด อยู่ในคลาสใด หลังจากนั้นก็สามารถแยก netid และ hostid ได้จากการเปรียบเทียบกับมาตรฐานของคลาสเหล่านั้น

แต่เมื่อมีการแบ่งเน็ตเวิร์คย่อยโดยการ subnet แล้ว ย่อมไม่สามารถใช้วิธีการข้างต้นเพื่อหา netid และ hostid ได้อีกต่อไป เนื่องจาก subnet นั้นสามารถกำหนดได้โดยผู้ออกแบบเน็ตเวิร์กเองและมิได้มีข้อบังคับแต่อย่างใด ดังนั้นจึงจำเป็นต้องมีการระบุค่าใดค่าหนึ่งไว้เพื่อให้สามารถนำมาใช้ในการหาค่าจาก IP Address ได้ว่าเป็น hostid, netid และ subnet id และค่านั้นก็คือ Subnet Mask นั่นเอง

Subnet Mask เป็นตัวเลขขนาด 32 บิตเท่ากับ IP Address ทำหน้าที่ระบุหมายเลขของ host id และ net id + Subnet id ของ โฮสต์นั้น การกำหนดค่าของ Subnet Mask จะอยู่ในรูปแบบเดียวกับ IP Address คือทำการแบ่ง Subnet Mask ออกเป็นเลข 16 บิตจำนวน 4 ชุด และแยกแต่ละชุดออกจากกันด้วยจุด (.)

ตัวอย่าง Subnet Mask เช่น FF.FF.FF.00 (Hex) 255.255.255.0 (Dec)

ค่า Subnet Mask นี้จำเป็นต้องกำหนดไว้บนทุกโฮสต์คู่กับค่า IP Address เสมอ เนื่องจาก โพรโตคอล IP จำเป็นต้องใช้ค่านี้ไปคำนวณค่า net id ซึ่งจะเป็นอย่างยิ่งในกระบวนการ IP Routing อย่างไรก็ตามค่า Subnet Mask นี้จะไม่ถูกส่งไปกับ IP ดาต้าแกรมด้วย โฮสต์ทั้งหลายสามารถนำค่า Subnet Mask มาทำการทางคณิตศาสตร์กับ IP Address ก็จะสามารถหาค่า host id, subnet id, netid ออกมาโดยวิธีดังนี้

Net id + subnet id = (IP Address) AND (Subnet Mask)
Host id = (IP Address) AND (NOT ((Subnet Mask)))

ตัวอย่าง

IP Address = 192.168.15.20 Subnet Mask = 255.255.255.0
Net id = 192.168.15.20 AND 255.255.255.0 = 192.168.15.0
Host id = 192.168.15.20 AND (0.0.0.255) = 0.0.0.20

หรือพูดง่ายๆ ได้ว่า 'Net id' ก็คือ IP Address ส่วนที่ตรงกับบิตของ Subnet mask ที่มีค่าเป็น 1 ส่วน Host id คือ IP Address ส่วนที่ตรงกับ Subnet mask ที่มีค่าเป็น 0 นั่นเอง

ดังนั้นพึงระลึกเสมอว่านอกจากการกำหนด IP Address ที่ถูกต้องแล้ว การกำหนดค่า Subnet Mask ก็มีผลต่อ IP Routing เช่นเดียวกัน การกำหนดค่า Subnet Mask ผิดพลาดย่อมจะส่งผลให้การสื่อสารข้อมูลของ IP ไม่สามารถจะกระทำได้เช่นกัน

3.2.4 IP address ในกรณีพิเศษ

ถึงแม้ค่าของ IP Address มีขนาด 32 บิต ที่นำมาใช้งานได้จริง แต่มีกรณีพิเศษเป็นข้อยกเว้นที่ไม่อาจนำค่าเหล่านี้มากำหนดเป็นค่า IP Address ได้ ซึ่งค่าส่วนใหญ่จะเป็นค่าที่ IP เองนำไปใช้งานเพื่อวัตถุประสงค์อื่นแล้ว ผู้ใช้จึงมิอาจนำค่าเหล่านั้นมาใช้งานอีก ดังรายละเอียดต่อไปนี้

ตารางที่ 3.4 IP Address สำหรับกรณีพิเศษ

IP Address			แอดเดรสของ		รายละเอียด
Net ID	Subnet ID	Host ID	ต้นทาง	ปลายทาง	
0 ทุกบิต	ไม่มี	0 ทุกบิต	ได้	ไม่ได้	เป็นการระบุโฮสต์นี้ภายในเน็ตเวิร์กนี้
0 ทุกบิต	ไม่มี	Host ID	ได้	ไม่ได้	เป็นการระบุโฮสต์หมายเลขตาม Host ID ภายในเน็ตเวิร์กนี้
127 บิต	ไม่มี	อะไรก็ได้	ได้	ได้	แอดเดรสที่ภายในโฮสต์ตนเอง (loopback address)
ทุกบิต	ไม่มี	1 ทุกบิต	ไม่ได้	ได้	บรอดคาสต์เฉพาะภายในเท่านั้น แต่จะไม่ส่งต่อไปยังเน็ตเวิร์กอื่น
Net ID	ไม่มี	1 ทุกบิต	ไม่ได้	ได้	บรอดคาสต์โดยตรงไปยังเน็ตเวิร์กที่ระบุใน Net ID
Net ID	Subnet ID	1 ทุกบิต	ไม่ได้	ได้	บรอดคาสต์โดยตรงไปยังเน็ตเวิร์กย่อยที่ระบุใน Subnet ID
Net ID	1 ทุกบิต	1 ทุกบิต	ไม่ได้	ได้	บรอดคาสต์โดยตรงไปยังเน็ตเวิร์กย่อยทุกเน็ตเวิร์กภายในเน็ตเวิร์กที่ระบุใน Net ID

ตารางที่ 3.4 แสดง IP Address บางค่าที่ถูกโพรโตคอลนำไปใช้เพื่อวัตถุประสงค์อื่น และผู้ใช้ไม่สามารถนำมากำหนดเป็นแอดเดรสของโฮสต์ได้ โดยส่วนใหญ่ค่าที่มีปัญหาจะมีเพียง 3 ตัว คือ

127	หมายถึง Loopback Address คือส่งกลับเข้าหาตัวเอง
1 ทุกบิต	หมายถึง โฮสต์ทุกตัวในเน็ตเวิร์ค (คือการบรอดคาสนั่นเอง)
0 ทุกบิต	หมายถึง ตัวเน็ตเวิร์คเอง

ดังนั้นเพื่อป้องกันปัญหาของการกำหนดค่า IP Address จึงควรจะหลีกเลี่ยงการกำหนดค่า Net ID และ Host ID ด้วยเลขดังกล่าวเสีย

3.3 โพรโตคอล HSRP และการทำ Redundancy บน MSFC

3.3.1 คำนิยามของ HSRP

แนวทางอย่างหนึ่งเพื่อให้บรรลุเป้าหมายการใช้งานเครือข่ายได้ เข้าใกล้ 100 เปอร์เซ็นต์ คือการใช้ HSRP เพื่อให้เส้นทางสำรองในเครือข่ายแก่เครือข่าย IP ซึ่งรับรองการจราจรให้ผู้ใช้งานโดยทันทีและกลับสู่สภาพการใช้งานได้เหมือนเดิมเมื่อเกิดความเสียหายขึ้นตั้งแต่ฮอปแรกในเครือข่าย

Hot Standby Routing Protocol คือตัวจัดการ การสัญจรของเครือข่าย โดยที่ข้อมูลของผู้ใช้งานจะถูกส่งผ่านไปยัง ' first hop' ก่อนเสมอ โดยใช้ Active Router ทำงานร่วมกับ Standby Router ซึ่ง Standby Router จะทำงานก็ต่อเมื่อ Active Router ไม่สามารถทำงานได้

3.3.2 รูปแบบการทำงานของ HSRP

การปฏิบัติการของ HSRP ใช้เราเตอร์ 2 ตัวหรือมากกว่า โดยทำเป็น Virtual Router เดียวกัน ซึ่งใช้ IP address และ MAC address ร่วมกัน โดยสมาชิกของกลุ่ม Virtual Router ทำการแลกเปลี่ยนข้อมูลสถานภาพซึ่งกันและกันเป็นประจำ ในที่นี่เราเตอร์หนึ่ง ตัวสามารถสมมุติความรับผิดชอบในการรับ-ส่งของเราเตอร์อีกตัวหนึ่งได้และสามารถทำงานนอกแผนงานที่วางแผนไว้ได้ โฮสต์ดำเนินการส่งกลุ่ม IP ที่บรรจุ IP address และ MAC address อย่างต่อเนื่อง และเปลี่ยนรูปแบบการส่งของทุกอุปกรณ์เป็นแบบ transparent

กลไกการทำงานของเราเตอร์ ทำโดยไม่มีการหยุดนิ่ง กลไกจำนวนมากเหล่านี้ทำให้ไม่สามารถเกิดความยืดหยุ่นในเครือข่ายตามที่ผู้บริหารเครือข่ายต้องการได้ เพราะโพรโตคอล ไม่ได้ถูกออกแบบให้มีลักษณะยืดหยุ่นในเครือข่ายตั้งแต่แรก หรืออาจเพราะความไม่เหมาะสมที่โฮสต์ทุกตัวในเครือข่ายต้องถูกใช้งานในลักษณะนี้ ประกอบกับยังมีความสำคัญของการ set configuration ที่ต้องการให้มีเพียงโฮสต์เดียวเท่านั้นที่จะ ถูก set ให้เป็น default-gateway

จากการศึกษาพบว่า host implementations ไม่สามารถรองรับเราเตอร์แบบ dynamic ที่เป็นค่า default ของเราเตอร์ได้ หากทุกโฮสต์ running ตาม mechanism ของเราเตอร์ dynamic นั้นจะเกิดความไม่เหมาะสม เนื่องจากเหตุผลหลายประการ ซึ่งรวมถึง ค่า administrative overhead, processing overhead , หรือปัญหาความไม่มั่นคงหรือไม่เพียงพอ ดังนั้น HSRP จะทำหน้าที่ให้บริการแก่โฮสต์เหล่านี้ได้เมื่อเกิดเหตุการณ์ fail over

การใช้ HSRP บนเราเตอร์ทำโดยกำหนดให้มี หนึ่ง virtual router ที่โฮสต์บน LAN นั้น ซึ่งเรียกว่ากลุ่ม HSRP หรือ standby router และมี active router ซึ่งเป็นเราเตอร์ตัวที่ถูกเลือกจากกลุ่มให้มีความรับผิดชอบเกี่ยวกับการส่งต่อกลุ่มของแพ็กเก็ตข้อมูลไปยัง virtual router อีกตัวถูกเลือกให้ทำงานในฐานะ standby router ถ้า active router ไม่สามารถทำงานได้ (fail) standby

router ก็จะทำหน้าที่ส่งต่อแพ็กเก็ตแทน active router แม้ว่าจำนวนของเราเตอร์ ที่กำหนดการทำงาน HSRP มี เพียงกลุ่ม active router ให้ทำการส่งต่อแพ็กเก็ตไปยัง virtual router เท่านั้น

เพื่อทำให้เกิดการจราจรน้อยที่สุดในเครือข่ายทั้ง active และ standby เราเตอร์จะทำการส่งข้อความ HSRP เพียงข้อความเดียวก็ทำให้การประมวลผลการทำงานเสร็จสมบูรณ์ ถ้า active router ทำงานล้มเหลว standby router ก็จะทำหน้าที่เป็น active router แทน ในขณะที่ active router เดิมก็จะทำงานในฐานะ standby router เช่นกัน

3.3.3 HSRP Addressing

เมื่อทำการ configure routers เพื่อเป็นส่วนหนึ่งของกลุ่ม HSRP นั้น สิ่งที่ต้องการใช้คือ HSRP MAC address เพื่อให้กลุ่ม burned-in MAC address กันเอง โดยมีข้อยกเว้นคือเราเตอร์ที่ควบคุมอีเทอร์เน็ตสามารถจำ MAC address เดียวเท่านั้น ดังนั้นเราเตอร์เหล่านี้ใช้ HSRP MAC address เวลาที่เป็น active router และจะ burned-in address ในขณะที่เป็น standby router

Token Ring อินเตอร์เฟสใช้ functional addresses เพื่อใช้เป็น HSRP MAC address Functional addresses เป็นเพียงกลไกเดียวที่ใช้ multicast mechanism ได้ ซึ่งมีข้อจำกัดคือจำนวนของ Token Ring, functional addresses ที่ใช้งานได้และ addresses อื่นๆ ถูกจองสำหรับหน้าที่อื่น ดังนั้นสามารถใช้ address ข้างล่างทั้ง 3 address เพื่อใช้ทำ HSRP

```
c000.0001.0000  (group 0)
c000.0002.0000  (group 1)
c000.0004.0000  (group 2)
```

3.3.4 อินเตอร์เฟส Tracking

อินเตอร์เฟส tracking คือการยอมให้กำหนดอินเตอร์เฟสอีก port บนเราเตอร์ที่ทำการประมวลผล HSRP เพื่อ monitor สำดับความสำคัญของ HSRP ในกลุ่ม ถ้าอินเตอร์เฟสที่ถูกกำหนดเกิด line protocol down ความสำคัญของ HSRP บนอินเตอร์เฟสนี้ก็ลดลงและจะการอนุญาตให้ HSRP บนเราเตอร์อีกตัวมีความสำคัญที่สูงกว่าจนกลายเป็น active router

การ configure tracking อินเตอร์เฟส HSRPโดยใช้คำสั่ง

```
standby [group] track interface [priority]
```

ตัวอย่าง ของ configuration เมื่อค่าความสำคัญที่ลดลงมีค่าเป็น 10 โดย ไม่ได้กำหนดหมายเลข

กลุ่มของ HSRP group และ default group number คือ group 0

```
interface ethernet0
ip address 10.1.1.1 255.255.255.0
standby ip  10.1.1.3
standby priority 110
standby track serial0
standby track serial1
The HSRP behavior with this configuration is:
0 interfaces down = no decrease (priority is 110)
1 interface down = decrease by 10 (priority becomes100)
2 interfaces down = decrease by 10 (priority becomes 90)
```

ถึงแม้ว่าค่า HSRP ลดลงก็จะได้ค่า configured ดังแสดงข้างล่าง

```
interface ethernet0
ip address 10.1.1.1 255.255.255.0
standby ip  10.1.1.3
standby priority 110
standby track serial0 10
standby track serial1 10
```

3.3.5 การใช้ Burned-In Address

การใช้ลักษณะเฉพาะของ burned-in address(BIA) โดยกลุ่ม HSRP ยอมใช้ interfaces burned-in MAC address แทนการใช้ HSRP MAC address การ configure HSRP เพื่อใช้ BIA โดยใช้คำสั่ง

```
standby use-bia [scope interface]
```

คำสั่ง use-bia ถูกใช้เพื่อเอาชนะข้อจำกัดของการใช้ functional address สำหรับ HSRP MAC Address บนอินเตอร์เฟสของ Token Ring เนื่องจากเมื่อ HSRP ทำงานในสิ่งแวดล้อมที่

เป็น multiple-ring, source-routed และ HSRP routers อยู่ที่ rings ที่ต่างกันการใช้ functional addresses ทำให้เกิดความสับสนในการส่งข้อมูลของ Routing Information Field (RIF) และด้วยเหตุนี้นี้คำสั่ง use-bia จึงทำให้ต้องใช้ DECnet ที่เราเตอร์ที่เหมือนกับระบบการถ่ายเอกสาร (XNS) และ HSRP ยอมให้ DECnet MAC (BIA) ถูกใช้ในฐานะ HSRP MAC

อย่างไรก็ตามคำสั่ง use-bia เกิดความเสียเปรียบหลายๆ อย่าง เมื่อเราเตอร์กลายเป็น active router, virtual IP ถูกย้ายไปยัง MAC address ที่แตกต่างกัน active router ตัวใหม่ทำการตอบสนอง ARP ที่ไม่จำเป็น แต่ก็ยังไม่สามารถตอบสนอง ARP ที่ถูกต้องทั้งหมด Proxy ARP จะถูกทำลายเมื่อ configure เป็น use-bia เนื่องจาก standby router ไม่สามารถครอบคลุมข้อมูลทั้งหมดของ proxy ARP จากเราเตอร์ตัวเกิดความเสียหายได้

เมื่อทำการ configure use-bia ที่อินเตอร์เฟสย่อยก็จะปรากฏ use-bia ที่อินเตอร์เฟสหลักและถูกนำไปใช้ในทุกอินเตอร์เฟสย่อยทั้งหมด

3.3.6 Multiple HSRPP Groups

ลักษณะเฉพาะของกลุ่ม HSRP (MHSRP) ถูกเพิ่มใน Cisco IOS 10.3. ลักษณะเฉพาะอันนี้จะใช้ความซ้ำซ้อนและ load-sharing ภายในเครือข่าย นอกจากนี้ยังยอมให้มีเราเตอร์สำรองเพื่อใช้ประโยชน์สูงสุดให้เพียงพอกว่า ในขณะเดียวกันเราเตอร์ก็ทำหน้าที่ส่งสัญญาณเพื่อการจราจรในกลุ่มของ HSRP ซึ่งสามารถทำงานในโหมด standby หรือรับฟังเพื่อรองรับการทำงานของกลุ่มอื่นๆ ได้

โดยปกติจะใช้ HSRP เพื่อช่วยสถานีสุดท้ายที่มีการบรรจบกับฮอบ gateway แรกเพื่อส่ง IP routing สถานีสุดท้ายถูกตั้งค่าโดย default gateway อย่างไรก็ตาม HSRP สามารถให้มี redundancy ตั้งแต่ฮอบแรกแก่โพรโตคอลอื่นๆ ได้ บางโพรโตคอล เช่น Peer-to-Peer Networking (APPN) จะใช้ MAC address เพื่อกำหนดฮอบแรก ในเส้นทางจุดหมาย

ในกรณีนี้การสามารถกำหนด MAC address ที่อยู่บน virtual MAC address เพื่อเตรียมพร้อมในการใช้คำสั่ง MAC-address ที่จำเป็นบ่อยๆ ได้ virtual IP address ก็จะไม่มีความสำคัญเมื่อใช้โพรโตคอลนี้ รูปแบบคำสั่งนี้คือ

```
standby[group]mac-address mac-address
```

3.3.7 **การพิสูจน์ตัวจริง** (Authentication)

ลักษณะเฉพาะของการพิสูจน์ตัวจริง HSRP ประกอบด้วยกุญแจ clear-text ที่ถูกบรรจุภายในกลุ่ม HSRP ลักษณะเฉพาะอันนี้จะทำการยับยั้งเราเตอร์ที่มีความสำคัญต่ำกว่าจากการ learning standby IP address และเตรียมจับค่าเวลาจากเราเตอร์ที่มีค่าความสำคัญที่สูงกว่า

เพื่อตั้งค่า HSRP authentication string ทำได้โดยการใช้คำสั่ง

standby authentication string command

HSRP ให้บริการ stateless redundancy แก่ IP routing โดย HSRP จะจำกัดการรักษาสถานะของตัวมันเอง หมายความว่าเราเตอร์แต่ละตัวจะสร้างและรักษาตารางเส้นทางของตัวมันเองอย่างเป็นอิสระต่อกัน ลักษณะเฉพาะ ของ IP redundancy คือการยอมรับ HSRP ที่ให้การบริการต่อ client application เพื่อให้สามารถดำเนินการได้ในขณะที่เกิด statefull fail over

HSRP บน Multiprotocol Label Switching Virtual Private Networks (MPLS VPNs) อินเตอร์เฟส ถูกใช้โดยเมื่อทำการเชื่อมต่อ Ethernet ระหว่าง 2 (Pes) และมีขั้นตอนคือ set ตำแหน่ง customer edge(CE)ใน default route บน virtual IP address ของ HSRP host หนึ่งหรือมากกว่าให้เป็น virtual IP address ที่เป็น default gateway network diagram จะแสดง PE 2 ตัว ที่ running HSRP ระหว่าง VPN routing/forwarding (VRF) อินเตอร์เฟส โดยตั้งค่า CE กับ HSRP virtual IP address ให้เป็น default route และ configured ให้ HSRP track ตามอินเตอร์เฟสที่เชื่อมโยงไปถึง Pes เช่นถ้าอินเตอร์เฟส E1 ของ PE1 ทำงานล้มเหลว HSRP ก็จะจัดการให้ PE2 ทำหน้าที่ส่งต่อข้อมูลแทนโดยยึดตาม virtual IP/ MAC address ข้างล่างคือตัวอย่าง configurations

```
Router PE1
Router PE2
conf terminal
ip cef
ip vrf vrf1 rd 100:1
 route-target export 100:1
 route target import 100:1
 interface ethernet0
 no shutdown
 ip vrf forwarding vrf1
 ip address 10.2.0.1 255.255.0.0
 standby 1 ip 10.2.0.20
 standby 1 priority 105
```

```
standby 1 preempt delay minimum 10
standby 1 timers 3 10
standby 1 track ethernet1 10
standby 1 track ethernet2 10
conf terminal
ip cef
ip vrf vrf1 rd 100:1
route-target export 100:1
route-target import 100:1
interface ethernet0
no shutdown
ip vrf forwarding vrf1
ip address 10.2.0.2 255.255.0.0
standby 1 ip 10.2.0.20
standby 1 priority 100
standby 1 preempt delay minimum 10
standby 1 timers 3 10
standby 1 track ethernet1 10
standby 1 track ethernet2 10
```

สามารถใช้คำสั่งข้างล่างนี้ เพื่อ verify , HSRP virtual IP address ที่ถูกต้องใน VRF ARP

```
ed1-pe1#show ip arp vrf vrf1
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.2.0.1           -   00d0.bbd3.bc22  ARPA   Ethernet0/2
Internet  10.2.0.20          -   0000.0c07.ac01  ARPA   Ethernet0/2

ed1-pe1#show ip cef vrf vrf1
Prefix              Next Hop            Interface
0.0.0.0/0           10.3.0.4            Ethernet0/3
0.0.0.0/32          receive
```

10.1.0.0/16	10.2.0.1	Ethernet0/2
10.2.0.0/16	attached	Ethernet0/2
10.2.0.1/32	receive	
10.2.0.20/32	receive	
224.0.0.0/24	receive	
255.255.255.255/32	receive	

3.3.8 HSRP รองรับการทำงานของ ICMP redirect

HSRP ทำงานอยู่บนพื้นฐานแนวคิดที่ HSRP ทำการป้องกัน subnet โดยสามารถให้การเข้าถึง subnet ทั้งหมดที่อยู่ในเครือข่าย ดังนั้นเราเตอร์ตัวไหนๆ ก็กลายเป็น HSRP active router ได้ก็เพราะว่าเราเตอร์ทั้งหมดมีเส้นทางไปในทุกๆ subnet ได้นั่นเอง

โพรโตคอล ICMP ยอมให้เราเตอร์มีการชี้นำ endstation ตัวใหม่เพื่อให้ทำการส่งกลุ่มของข้อมูลไปยังปลายทางที่เจาะจงไปยังเราเตอร์อีกตัวที่ subnet เหมือนกัน โดยถ้าเราเตอร์ตัวแรกรู้จัก เราเตอร์ตัวอื่นๆว่ามีทางผ่านที่ดีกว่าเพื่อไปยังปลายทางนั้นก็จะทำการเปลี่ยนเส้นทาง ในกรณีที่เป็น default gateways ถ้าเราเตอร์ตัวที่ endstation ถูกชี้นำปลายทางใหม่เมื่อตัวปลายทางมีการทำงานที่ล้มเหลวและกลุ่มข้อมูลไม่สามารถถูกส่งไปยัง endstation ได้ ในมาตรฐานของ HSRP มาตรฐานเรื่องนี้ไม่ควรเกิดขึ้น สำหรับกรณีนี้เราความสามารถ disabling ICMP reddirects เพื่อใช้ HSRP แทนได้

ความแตกต่างระหว่าง ICMP redirect และ HSRP เพื่ออธิบายปัญหาที่เกิดขึ้นนี้ โดยคุณยังสามารถใช้ประโยชน์จากทั้งสองฟังก์ชั่น รายละเอียดการทำงานดังนี้ เมื่อมี HSRP 2 กลุ่มหรือมากกว่าทำงานในแต่ละ subnet HSRP ถูก configures ไว้ในเราเตอร์ที่ใช้งานร่วมกัน ลำดับความสำคัญทำได้โดยการ configure ให้มีแต่ละเราเตอร์หลักไว้อย่างน้อย 1 ตัวในแต่ละกลุ่มของ HSRP เมื่อเราเตอร์ตัวหนึ่งได้ตัดสินใจเลือก endstation ตัวใหม่ที่แตกต่างไปจากเดิมเพื่อส่งข้อมูลไปยังเราเตอร์ตัวปลายทางที่เจาะจงไว้ ในเวลานั้นแทนที่การชี้นำ endstation ไปยังเราเตอร์ที่ IP address มันกลับพบกลุ่ม HSRP ที่กำลังถูกทำให้เป็น Active router แทน และ การชี้นำ endstation ตัวใหม่อย่างถูกต้องทำโดยการชี้ที่ virtual IP address ถ้าเป้าหมายของมันคือเราเตอร์ตัวที่ทำงานผิดพลาดในเวลานั้น HSRP จะรับรองเราเตอร์ตัวอื่นเพื่อทำงานนั้นแทนและอาจจะกำลังอาจทำการชี้ endstation ตัวใหม่อีกครั้งบน virtual router

3.4 รูปแบบการทำงานของ MSFC redundancy

Multilayer Switch Feature Cards (MSFC) ทำหน้าที่จัดหาเส้นทางให้กับ multiplayer switching (MSL) ที่มีความเร็วในการสลับเส้นทางมากที่สุดถึง 15 Million packets per second (Mpps) เพื่อทำการอินเตอร์เฟสกับอีเทอร์เน็ตสวิตช์

โดยการทำงานของ MLS นั้นสามารถรองรับการใช้งานของโพรโตคอลต่างๆ เช่น IP ,IP multicast และ Inter Network Packet Exchange (IPX)

ขีดจำกัดของค่าที่ตั้งไว้บน MSFCs และความล้มเหลวที่สามารถเกิดขึ้นถ้าขีดจำกัดเหล่านั้นไม่ถูกทำตาม และ ข้อได้เปรียบ/ข้อเสียเปรียบของ MSFC redundancy 3 รูปแบบคือ

3.4.1 ทางเลือกที่ 1: การทำงานด้วย MSFCs คู่ที่ทำงานโดยการแยกเราเตอร์คนละตัว

ข้อกำหนดนี้คือวิธีที่เป็นต้นฉบับของภายใน MSFC redundancy เมื่อการใช้วิธีนี้ MSFCs 2 card ทำงานที่เราเตอร์คนคนละตัว เราเตอร์ต้อง configured ในแนวทาง และเหตุผลสำหรับการนำไปสู่ความคิดของการออกแบบ MSFC

- การออกแบบ MSFC

ในการ configuration ภายใน redundant MSFC (ทำการติดตั้งcard MSFCs เหมือนกัน 2 chassis) ในการออกแบบ MSFC คือ MSFC ต้องทำงานขึ้นมาก่อนหรือใช้งานยาวนานที่สุด โดยสามารถวาง MSFC ในช่อง 1 หรือ ในช่อง 2 ก็ได้ จะเห็นว่าไม่มีกลไกใดที่มีอิทธิพลต่อการออกแบบ MSFC แบบนี้ได้ สิ่งแรกที่ต้องคำนึงถึงในการออกแบบ MSFC คือเรื่องของการ on-line ถ้าการออกแบบ MSFC ถูก reload ด้วยมือหรือประสบการณ์การ reload ที่ไม่ชำนาญ MSFC อื่นๆ จะกลายเป็น MSFC ที่ถูกออกแบบ คุณสามารถพิสูจน์ MSFC ด้วยการออกแบบ MSFCในช่องที่ 2 ดัง ตัวอย่าง output ด้านล่าง โดยการใช้คำสั่ง show fm feature หรือ sh redundancy บน MSFC

ตัวอย่าง เช่น, คำสั่ง execute บน MSFC ในช่องที่ 1 แสดงว่า MSFC นี้ ไม่ได้ถูกออกแบบให้เป็น MSFC และ MSFC ในช่องที่ 2 ถูกออกแบบให้เป็น MSFC

```
Cat6k-MSFC-slot1#show fm feature
Redundancy Status: Non-designated
    Designated MSFC: 2
    Non-designated MSFC:1
```

คำสั่งเดียวกันออกบน MSFC ในช่อง 2 จะแสดงดังต่อไปนี้:

```
Cat6k-MSFC-slot2#show fm feature
Redundancy Status: designated
    Designated MSFC: 2
    Non-designated MSFC:1
```

คำสั่ง sh redundancy จะแสดงสถานะขอ MSFC

```
Cat6k-MSFC-slot1# sh redundancy
Designated Router: 2 Non-designated Router: 1
Redundancy Status: designated
```

- การ Configuring HSRP บน MSFC

การ redundancy ระหว่าง MSFC 2 อันที่ใช้ฟังก์ชั่น HSRP (โดยการ configure ให้ลำดับความสำคัญ ของการ standby ในแต่ละ MSFC ที่แตกต่าง) สำหรับเลเยอร์สาม redundancy การ configuration บน MSFCs ทั้ง 2 อันจะเหมือนกันยกเว้นพารามิเตอร์ข้างล่างคือ:

```
HSRP standby priority
IP address commands
```

ข้อได้เปรียบและเสียเปรียบของทางเลือกที่ 1

ข้อได้เปรียบ

1. MSFCs ทั้งสองทำงานบน routing protocol และตารางเส้นทางเดียวกัน ดังนั้นเวลาที่เกิดผิดพลาดใน MSFC ตัวที่ 1 MSFC ตัวที่ 2 ไม่ต้องใช้เวลาเพื่อรอการรวมของข้อมูลที่ต้องส่งต่อ
2. HSRP สามารถทำให้ failover ที่เกิดจากอุปกรณ์ active ไปยัง standby เกิดขึ้นอย่างรวดเร็วเมื่อเป็น gateway redundancy

เป็นการรวมสภาพที่เป็นประโยชน์ที่สูงสำหรับระดับชั้นที่สองเกิดการ fail over และใช้เวลาในการฟื้นตัวภายในอย่างรวดเร็วภายในไม่กี่วินาที ถ้าผิดพลาดเกิดขึ้นบนหนึ่ง MSFC/SUP

ข้อเสียเปรียบ

1. ต้องใช้ IP address ถึง 2 IP ต่อ VLAN ต่อ chassis
2. มีความจำเป็นในการเพิ่ม routing protocol
3. Non-Reverse Path Forwarding (RPF) จะทำการ drop IP multicast โดยซอฟต์แวร์ เมื่อใช้รูปแบบ SUP IA
4. มีความซับซ้อนในทางปฏิบัติ ก็คือการ configurations

3.4.2 ทางเลือกที่ 2: โดยการใช้ Router ตัวเดียว Single Router Mode (SRM)

การใช้เราเตอร์ตัวเดียว คือลักษณะเฉพาะแบบใหม่ที่กล่าวถึงจุดบกพร่องของ MSFC redundancy บนพื้นฐานการใช้งาน HSRP ก่อนหน้านี้คือ

- MSFCs ทั้งสองมี configuration ที่เหมือนกัน
- MSFC ที่ถูกชี้ชัดเท่านั้นที่จะถูกมองเห็นในเครือข่าย
- MSFC ที่ไม่ได้ถูกชี้ชัด จะอยู่ที่อินเตอร์เฟสของ VLAN ทั้งหมด (มีการถูก boot อย่างสมบูรณ์)
- การ configuration อนุญาตให้ทำบน MSFC ที่ถูกชี้ชัดเท่านั้น

เมื่อ SRM ถูก enable non-DR กำลังออนไลน์แต่อินเตอร์เฟสทั้งหมด down ดังนั้นมันจะไม่เก็บข้อมูลตารางเส้นทางใดๆ เลย วิธีการทำงานนี้ เมื่อ DR ทำงานล้มเหลวจะมีล่าช้าก่อนที่ non-DR จะ online ต้องมีตารางเส้นทางสมบูรณ์เสียก่อน ข้อมูลที่ใช้ เพื่อจัดลำดับของความเสียหายโดย SUP ที่ระดับชั้นที่สามเพื่อทำการส่งต่อข้อมูลเหล่านี้และทำการปรับปรุงข้อมูลใหม่จาก DR ตัว ใหม่

ข้อได้เปรียบและข้อเสียเปรียบของ SRM

ข้อได้เปรียบ

1. มีการแปลง IP address
2. ทำให้ routing protocol ที่ peering น้อยลง
3. การ configuration ทำแบบธรรมดามาก ไม่ทำให้เกิดการ configuration ที่ไม่เหมาะสม

ข้อเสียเปรียบ

1. เรายังคงใช้ FIB image เก่าถึงแม้ว่าตารางเส้นทางที่สร้างจะไม่ออนไลน์อีกต่อไปแล้ว เกิดปัญหาระหว่างการ ทำ table-update เนื่องจากมี delay time เพื่อส่งกลุ่มข้อมูลไปยังเส้นทางที่ยังใช้งานไม่ได้
2. น่าจะมีจุดบกพร่องกว่าทางเลือก 1 สำหรับเครือข่ายเพราะว่า ตารางเส้นทาง จำเป็นที่จะจงใจ configuration ที่ DR ตัวใหม่

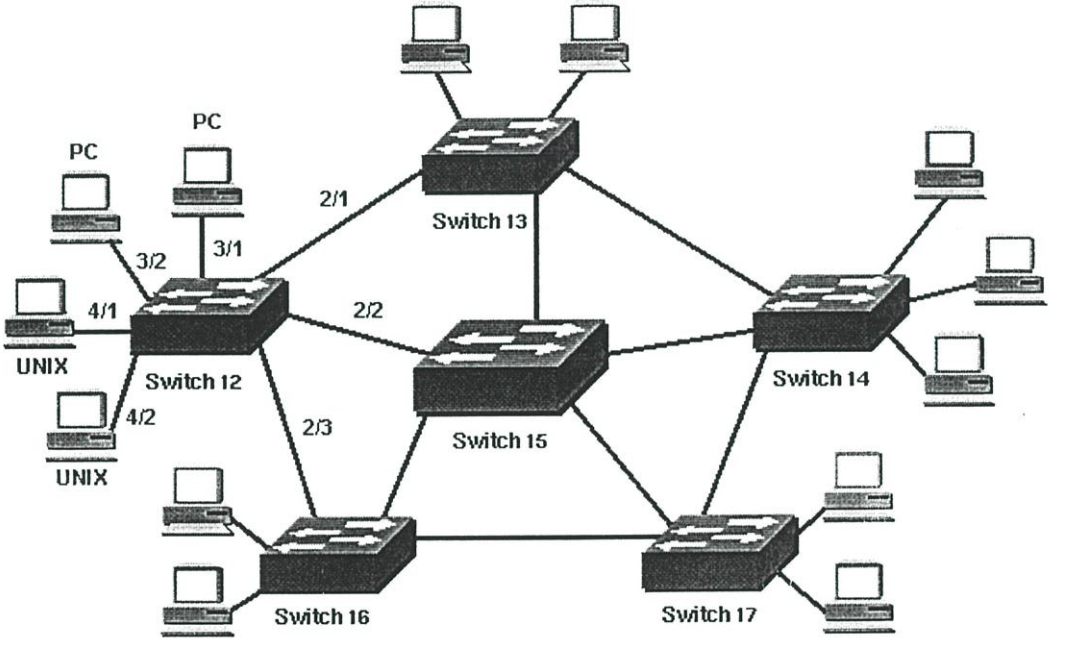
3.4.3 **ทางเลือกที่** 3: Manual Mode Redundancy

ทางเลือกสุดท้ายจำเป็นต้องมี SUP คู่โดยมี MSFCs คู่และใช้ MSFCในช่องที่ 1 เท่านั้น MSFCในช่องที่ 2 จะอยู่ใน ROM Monitor Mode โดยการไม่มีเลเยอร์สาม redundancy ที่ MSFC ในช่องที่ 1 เลย แต่ในการออกแบบนี้จะให้มีการทำเลเยอร์สาม redundancy ที่ chassis ที่ 2 แทน

บทที่ 4

โพรโตคอล Spanning- Tree Protocol (STP)

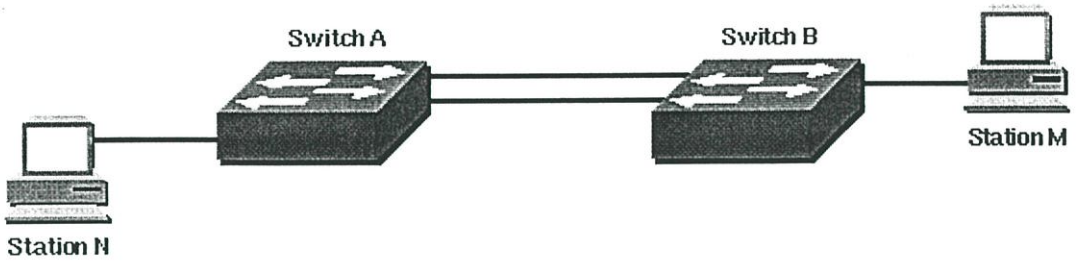
STP คือโพรโตคอลในเลเยอร์ 2 ที่ถูกออกแบบให้ทำงานบนอุปกรณ์บริดจ์และสวิตช์ จุดมุ่งหมายที่สำคัญของ STP คือทำให้มั่นใจว่าไม่เกิดการลูปขึ้นในเครือข่าย เมื่อมีการทำเส้นทางสำรอง เนื่องจากการลูปเป็นปัญหาที่ทำให้เครือข่ายไม่สามารถใช้งานได้



รูปที่ 4.1 แสดงเน็ตเวิร์คไดอะแกรมของเครือข่าย

แนวคิด

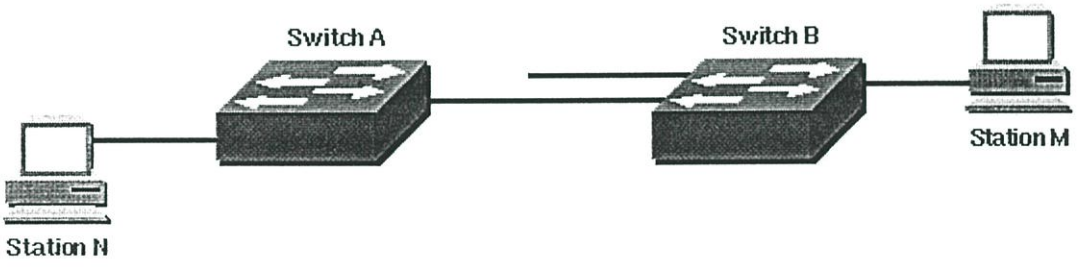
STP ทำหน้าที่ป้องกันการลูปในโครงข่ายเมื่อต้องการเส้นทางสำรอง เส้นทางสำรองมีความสำคัญซึ่งจะเป็นแบ็คอัพ ในกรณีการ fail over ขึ้นในเครือข่าย ถ้าเส้นทางหลักไม่สามารถใช้งานได้เส้นทางสำรองก็จะถูก active ขึ้นทำให้เครือข่ายมีการใช้งานได้อย่างต่อเนื่อง ถ้าปราศจาก STP บนอุปกรณ์บริดจ์หรือสวิตช์แล้ว ผลก็คือทำให้เครือข่ายไม่สามารถใช้งานได้เนื่องจากผลของการลูป ดังรูปเครือข่ายข้างล่าง



รูปที่ 4.2 แสดงการเกิดลูปในเครือข่ายที่ปราศจาก STP

ในรูปเน็ตเวิร์คไดอะแกรมข้างบน เส้นทางสำรองถูกสร้างขึ้นระหว่างสวิตช์ A และ สวิตช์ B แต่ก็ยังมีความเป็นไปได้ที่จะเกิดสะพานลูป เนื่องจาก เช่น หากมีแพ็กเก็ต broadcast หรือ multicast ผ่านจากสถานี M ไปยัง สถานี N มีความเป็นไปได้สูงที่จะเกิดการส่งต่อของข้อมูลระหว่างสวิตช์ ทั้งสองครั้งแล้วครั้งเล่าจนสวิตช์ทั้งสองตัวไม่สามารถใช้งานได้

อย่างไรก็ตาม ถ้ามีการใช้งาน STP บนสวิตช์ทั้งสองตัว ตรรกของเครือข่ายก็จะได้ตามรูปข้างล่าง



รูปที่ 4.3 แสดงการทำงานของเครือข่ายเมื่อใช้งาน STP

เพื่อหลีกเลี่ยงการลูปบนเส้นทางสำรอง STP จะทำการ block เส้นทางสำรอง และผลักดันข้อมูลให้ผ่านเส้นทางหลัก เมื่อไหร่ก็ตามที่เส้นทางหลักไม่สามารถใช้งานได้ STP ก็จะทำการ reconfigure เครือข่าย และทำการย้ายเส้นทางของข้อมูลสู่เส้นทางสำรองซึ่งขณะนั้นได้กลายเป็นเส้นทางหลักไปแล้ว

กุญแจที่สำคัญของ STP ก็คือสวิตช์ในเครือข่ายที่ถูกเลือกให้เป็น root bridge รวมกันกลายเป็นจุดรวมในเครือข่าย การตัดสินใจอื่นๆ ในเครือข่าย เช่นการ block port และ การวาง port ใน forwarding mode ถูกทำโดย root bridge นี้ สภาพแวดล้อมของสวิตช์ A จะแตกต่างจาก

บริดจ์เนื่องจากประกอบด้วย VLANs จำนวนมาก เมื่อทำการติดตั้งสวิตช์ ในเครือข่าย root bridge มักจะอ้างอิง root switch โดยแต่ละ VLAN จะต้องมี root bridge ของมันเอง

4.1 การทำงานของ STP

4.1.1 หน้าที่ของ STP

เงื่อนไขจำเป็นก่อนที่จะทำการ Configuring STP ต้องเลือกสวิตช์ขึ้นมาหนึ่งตัวเพื่อเป็น root ของ Spanning-tree โดยไม่จำเป็นว่าต้องเป็นสวิตช์ตัวที่ใช้งานได้ประสิทธิภาพสูงสุด แต่เป็นสวิตช์ตัวที่เป็นศูนย์รวมให้กับเครือข่าย การไหลของข้อมูลทั้งหมดในเครือข่ายจะทำโดยการตัดสินใจของสวิตช์ตัวนี้ นอกจากนี้ยังมีความสำคัญคือสวิตช์ตัวนี้ต้องทำการการะจายข้อมูลน้อยที่สุดในเครือข่าย ซึ่งส่วนใหญ่จะให้แบ็คโบนสวิตช์ทำหน้าที่นี้ เพราะว่าจะไม่มีเครื่องลูกข่าย (end stations) ตัวใดต่อโดยตรงกับแบ็คโบนสวิตช์ ดังนั้นจะไม่ส่งผลกระทบการใช้งานเมื่อมีการเปลี่ยนแปลงเส้นทางในเครือข่าย

หลังจากตัดสินใจเลือก Root สวิตช์แล้ว ต่อไปคือการ set ค่าในตัว root switch ซึ่งค่าเดียวที่ต้อง set คือ bridge priority หากในเครือข่ายนี้มี bridge priority จะ set ค่าให้ต่ำกว่าสวิตช์ตัว อื่นๆ เสมอ ซึ่งในการเลือกนี้สามารถทำโดยอัตโนมัติที่ตัว root switch อยู่แล้ว

เครื่องลูกข่าย (End stations) บนพอร์ตสวิตช์ ทำได้โดยการ set คำสั่ง spantree portfast ซึ่งทำได้บนพอร์ตพื้นฐาน portfast นี้สามารถเปลี่ยนแปลงได้ ซึ่งเมื่อ enable บน port แล้ว port จะเปลี่ยนแปลงสถานะจาก blocking mode เป็น forwarding mode อย่างไรก็ตามคำสั่งนี้ใช้ได้ก็ต่อเมื่อได้ทำการเชื่อมต่อระหว่างสวิตช์กับสวิตช์เท่านั้น ในการเปลี่ยนสถานะจาก blocking เป็น forwarding จะใช้เวลาประมาณ 30 – 60 วินาที ทำให้สามารถป้องกันการเกิดลูปในเครือข่ายเมื่อทำการต่อสวิตช์กับสวิตช์ได้

4.1.2 กฎของการทำงาน

เมื่อสวิตช์ตัวแรกเริ่มทำงาน Root switch ก็จะเริ่มกระบวนการเลือก โดยสวิตช์แต่ละตัวจะส่ง BPDU ไปยังสวิตช์ที่ต่อโดยตรงกับมันบน VLAN

เมื่อ BPDU ถูกส่งออกไปนอกเครือข่าย สวิตช์แต่ละตัวจะทำการเปรียบเทียบ BPDU ที่รับมาจากตัวเพื่อนบ้าน ในการเปรียบเทียบนี้ สวิตช์จะทำเพื่อทราบว่าสวิตช์ตัวไหนเป็น root switch ซึ่งหากสวิตช์ตัวไหนมีค่า priority ต่ำสุดในเครือข่ายก็จะชนะและถูกเลือกให้เป็น root switch ข้อควรจำ : กำหนด root switch ได้ตัวเดียวต่อ VLAN ซึ่งหลังจากกำหนดแล้วสวิตช์จะทำงานตามกฎข้างล่างนี้

- กฎข้อที่หนึ่ง ทุกพอร์ตของ Root switch ต้องทำงานใน forwarding mode หลังจากนั้นสวิตช์แต่ละตัวจะเลือกเส้นทางที่ดีที่สุด โดยการเปรียบเทียบข้อมูล BPDUs ที่รับเข้ามา

จากทุกพอร์ต พอร์ตที่บรรจุข้อมูลน้อยที่สุดก็จะถูกใช้เป็น root switch ซึ่งพอร์ตนี้จะถูกเรียกว่า root port หลังจากสวิตช์ได้ root port แล้วก็จะทำตามกฎข้อที่ 2

- กฎข้อที่สอง เมื่อสวิตช์ตัวหนึ่งถูกกำหนดให้เป็น Root switch แล้วต้องทำงานใน forwarding mode เท่านั้น แต่ละส่วนของ LAN การสื่อสารระหว่างสวิตช์ตัวอื่นๆ จะใช้เพื่อการเคลื่อนย้ายข้อมูลไปยัง root bridge ซึ่งสวิตช์เหล่านี้เรียกว่า designated switch
- กฎข้อที่สาม ในส่วนพอร์ท LAN ของ designated switch ที่ทำการเชื่อมต่อกับ LAN ต้องทำงานใน forwarding mode ด้วย
- กฎข้อที่สี่ พอร์ตอื่นๆ ที่เหลือในสวิตช์ทุกตัวต้องทำงานใน Blocking mode ซึ่งหมายถึงพอร์ตที่ทำการเชื่อมต่อกับ bridges หรือ switches ตัวอื่น สำหรับพอร์ตที่ทำการเชื่อมต่อกับ workstation หรือเครื่องคอมพิวเตอร์จะไม่มีผลต่อการทำงานของ STP อยู่แล้ว

4.2 พารามิเตอร์ และ การแสดงสถานะของ STP

ในการใช้งาน STP ต้องมีการตั้งค่าพารามิเตอร์และการแสดงสถานะต่างๆ ของ STP ซึ่งจะรวมกันอยู่ในการใช้งานจริง ต่างๆ ดังต่อไปนี้

ขั้นตอนการใช้งาน

1. ใช้คำสั่ง **show version** เพื่อแสดง software version ที่สวิตช์ใช้งานอยู่ดังแสดงด้านล่าง

Switch-15> (enable) **sh version** WS-C5505 Software, Version McpSW: 4.2(1) NmpSW: 4.2(1)
Copyright (c) 1995-1998 by Cisco Systems
NMP S/W compiled on Sep 8 1998, 10:30:21 MCP S/W compiled on Sep 08 1998, 10:26:29 System Bootstrap Version: 5.1(2)
Hardware Version: 1.0 Model: WS-C5505 Serial #: 066509927 Mod Port Model Serial # Versions --- ---- ---------- --------- ---------- 1 0 WS-X5530 008676033 Hw : 2.3 Fw : 5.1(2)

```
Fw1: 4.4(1)
Sw : 4.2(1)
```

2. สมมุติว่า Switch-15 เป็นตัวเลือกที่ดีที่สุดสำหรับ root switch ในเครือข่าย VLANs เนื่องจากมันเป็น backbone switch การ set คำสั่ง spantree root *{vlan_id}* ทำโดยการ sets priority ของสวิตช์ให้มีค่าเป็น 8192

   หมายเหตุ : เนื่องจากค่า default priority ของสวิตช์คือ 32768 ดังนั้นคำสั่งนี้จะทำให้ Switch-15 ถูกเลือกให้เป็น root switch เพราะมีค่า priority ต่ำสุด

```
Switch-15> (enable) set spantree root 1
VLAN 1 bridge priority set to 8192.
VLAN 1 bridge max aging time set to 20.
VLAN 1 bridge hello time set to 2.
VLAN 1 bridge forward delay set to 15.
Switch is now the root switch for active VLAN 1.
Switch-15> (enable)

Switch-15> (enable) set spantree root 200
VLAN 200 bridge priority set to 8192.
VLAN 200 bridge max aging time set to 20.
VLAN 200 bridge hello time set to 2.
VLAN 200 bridge forward delay set to 15.
Switch is now the root switch for active VLAN 200.
Switch-15> (enable)

Switch-15> (enable) set spantree root 201
VLAN 201 bridge priority set to 8192.
VLAN 201 bridge max aging time set to 20.
VLAN 201 bridge hello time set to 2.
VLAN 201 bridge forward delay set to 15.
Switch is now the root switch for active VLAN 201.
```

```
Switch-15> (enable)

Switch-15> (enable) set spantree root 202
VLAN 202 bridge priority set to 8192.
VLAN 202 bridge max aging time set to 20.
VLAN 202 bridge hello time set to 2.
VLAN 202 bridge forward delay set to 15.
Switch is now the root switch for active VLAN 202.
Switch-15>

Switch-15> (enable) set spantree root 203
VLAN 203 bridge priority set to 8192.
VLAN 203 bridge max aging time set to 20.
VLAN 203 bridge hello time set to 2.
VLAN 203 bridge forward delay set to 15.
Switch is now the root switch for active VLAN 203.
Switch-15>

Switch-15> (enable) set spantree root 204
VLAN 204 bridge priority set to 8192.
VLAN 204 bridge max aging time set to 20.
VLAN 204 bridge hello time set to 2.
VLAN 204 bridge forward delay set to 15.
Switch is now the root switch for active VLAN 204.
Switch-15> (enable)
```

คำสั่งที่สั้นกว่าและใช้งานได้เช่นเดียวกันได้แสดงอยู่ด้านล่างคือ

```
Switch-15> (enable) set spantree root 1,200-204
VLANs 1,200-204 bridge priority set to 8189.
VLANs 1,200-204 bridge max aging time set to 20.
VLANs 1,200-204 bridge hello time set to 2.
```

```
VLANs 1,200-204 bridge forward delay set to 15.
Switch is now the root switch for active VLANs 1,200-204.
Switch-15> (enable)
```

คำสั่งที่สามของการกำหนด Root switch คือ

```
Switch-15> (enable) set spantree priority 8192 1
Spantree 1 bridge priority set to 8192.
Switch-15> (enable)
```

หมายเหตุ : ในกรณีนี้สวิตช์ทุกตัวจะถูกล้าง configurations หมายความว่าสวิตช์ทุกตัวจะเริ่มต้นที่มี Bridge Priority เป็น 32768

3. ขั้นตอนต่อไปคือการ Configure portfast บนสวิตช์ 12, 13, 14, 16, และ 17 โดยใช้คำสั่ง by set **spantree portfast mod_num/port_num enable**

หมายเหตุ: การ set configured จะทำบน ports ที่เชื่อมต่ออยู่กับ workstations หรือเครื่องคอมพิวเตอร์เท่านั้น เราจะไม่ enable portfast บนทุกพอร์ตที่ทำการเชื่อมต่ออยู่กับสวิตช์

ตัวอย่าง เฉพาะ Switch-12 เท่านั้นที่ถูก configure โดยมีขั้นตอนดังนี้

```
port 2/1 connects to Switch-13
port 2/2 connects to Switch-15
port 2/3 connects to Switch-16
port 3/1 through 3/24 connects to PCs
port 4/1 through 4/24 connects to UNIX workstations
```

จากข้อมูลดังกล่าวทำให้เราทราบว่า portfast คือ ports 3/1 - 3/24, และ ports 4/1 - 4/24 นั่นเอง

```
Switch-12> (enable) set spantree portfast 3/1-24 enable
```

ข้อควรระวัง : Spantree port fast จะเริ่มต้นทำงานเฉพาะพอร์ตที่มีโฮสต์เดียว การเชื่อมโยงสู่ hubs จุดศูนย์รวมสัญญาณ, สวิตช์,บริดจ์ และอื่นๆ เพื่อให้ fast port สามารถทำงานเป็น spanning-tree loopsชั่วคราวได้ โดยการใช้ข้อความเพื่อเตือนดังนี้

```
Spantree ports 3/1-24 fast start enabled.
Switch-12> (enable)
Switch-12> (enable) set spantree portfast 4/1-24 enable
```

4. ขั้นตอนของการตรวจสอบ Switch-15 ว่าเป็น root ของ VLANs หรือไม่ โดยใช้คำสั่ง

```
show spantree {vlan_id} .
```

โดยใช้ผลของคำสั่งนี้เปรียบเทียบกับ MAC address ของสวิตช์ที่ถูกกำหนดให้เป็น root ถ้าผลที่ได้เท่ากัน สวิตช์ตัวดังกล่าวก็จะเป็น root switch ของ VLAN เช่นเดียวกันถ้า root port คือ 1/0 ก็มีความหมายเช่นเดียวกันคือเป็น root switch ตัวอย่างของคำสั่งได้แสดงอยู่ข้างล่างดังนี้

```
Switch-15> (enable) sh spantree 1
VLAN 1
spanning-tree enabled
spanning-tree type          ieee

Designated Root             00-10-0d-b1-78-00

!-- MAC address of the root switch for VLAN 1.

Designated Root Priority    8192
Designated Root Cost        0
Designated Root Port        1/0
Root Max Age   20 sec    Hello Time 2  sec   Forward Delay 15
sec
```

```
Bridge ID MAC ADDR          00-10-0d-b1-78-00
Bridge ID Priority          8192
Bridge Max Age 20 sec    Hello Time 2  sec    Forward Delay 15
sec
```

ค่าที่แสดงข้างบนชี้ชัดว่า Switch-15 เป็น Designated Root บน spanning-tree สำหรับ VLAN 1 MAC address ของ designated root switch (00-10-0d-b1-78-00) มีค่าเช่นเดียวกัน Switch-15 เมื่อเป็นบริดจ์ ID Mac Address (00-10-0d-b1-78-00) ค่าแสดงอื่นๆ ที่จะชี้ว่าเป็น Designated Root หรือไม่ก็คือค่า Designated Root Port เป็น 1/0

ผลที่ได้ข้างล่างจาก Switch-12 แสดงว่ามันยอมรับให้ Switch-15 เป็น Designated Root ใน VLAN 1

```
Switch-12> (enable) sh spant 1
VLAN 1
spanning-tree enabled
spanning-tree type  IEEEDesignated Root    00-10-0d-b1-78-00

!-- MAC address of the root switch for VLAN 1.

Designated Root Priority    8192
Designated Root Cost        19
Designated Root Port        2/3
Root Max Age   20 sec    Hello Time 2  sec    Forward Delay 15
sec

Bridge ID MAC ADDR          00-10-0d-b2-8c-00
Bridge ID Priority          32768
Bridge Max Age 20 sec    Hello Time 2  sec    Forward Delay 15
sec
```

หมายเหตุ : ผลของการใช้คำสั่ง show spantree *{vlan_id}* เพื่อแสดงสวิตช์ตัวที่เหลืออยู่และ ทำให้ทราบว่า Switch-15 เป็น Designated Root สำหรับ VLANs นี้

การพิสูจน์ ทำได้โดยการใช้คำสั่ง

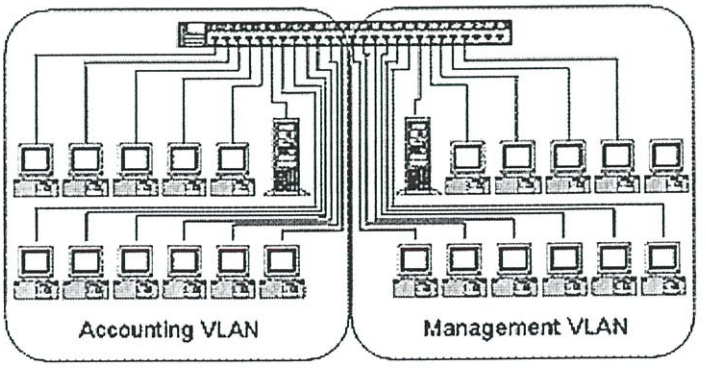
- show spantree vlan_id: เพื่อแสดงสถานะปัจจุบันของ spanning-tree ที่ vlan_id ที่เป็นสมาชิกในตัวสวิตช์
- show spantree summary: แสดงผลรวมของ spanning-tree ports ที่เชื่อมต่อใน VLAN

บทที่ 5
โพรโตคอล VLAN Trunk Protocol และ VLAN Routing

5.1 คำนิยามของ VLAN

VLAN (Virtual Area Network) เป็นการจัดแยกการเชื่อมต่อเครือข่ายในรูปแบบที่เรียกว่าโดเมนส์ ซึ่งจุดประสงค์ของการแยกออกเป็นโดเมนส์นี้ ก็เพื่อให้เครื่องคอมพิวเตอร์ที่อยู่ต่างโดเมนส์ไม่สามารถสื่อสารกันได้ ทั้งนี้เพื่อความปลอดภัยของเครือข่าย รวมทั้งสามารถเพิ่มประสิทธิภาพการทำงานของเครือข่ายอีกด้วย

ในหนึ่งเครือข่ายอาจประกอบด้วย Switching Hub หลาย ๆ ตัว และใน Switching Hub หนึ่งตัวอาจประกอบด้วย VLAN หลาย ๆ โดเมนส์ หรือหลาย VLAN ก็เป็นได้ การแบ่ง VLAN จะทำให้เครื่องคอมพิวเตอร์แม้จะเชื่อมต่อกันใน Switches Hub เดียวกัน แต่อยู่ต่าง VLAN กัน ไม่สามารถสื่อสารกันได้ รวมทั้งไม่สามารถมองเห็นกันได้ด้วยซ้ำไป (รูปที่ 5.1) และที่แน่นอน หนึ่ง VLAN สามารถกระจายไปตาม Switches Hub ต่าง ๆ ได้ เช่นกัน ทุกๆ switch port สามารถเป็นส่วนหนึ่งของ VLAN โดยสามารถทำ unicast, broadcast packet เฉพาะเครือข่ายที่อยู่ใน VLAN เดียวกัน VLAN ประกอบด้วย logical network และ packet ปลายทางสำหรับสถานีที่ไม่ได้อยู่ใน VLAN จะถูกส่งต่อไปยัง router หรือ bridge เนื่องจาก VLAN ถูกมองเป็น logical network ที่แยกออกมาซึ่งจะจำกัดข้อมูล MIB bridge ของมันเอง และสามารถทำ STP ด้วยตัวมันเองภายใต้ Switches Hub ของ Cisco 1 ตัว สามารถติดตั้ง VLAN ได้มากถึง 64 VLAN และทั้งระบบสามารถมี VLAN ได้มากถึง 1024 VLAN จำนวนของ VLANs , VLANs ถูกกำหนดให้มีจำนวนระหว่าง 1-1001



รูปที่ 5.1 แสดงการแบ่ง VLAN ออกเป็น 2 ชุด ภายใน Switch เดียว

5.2 ทำไมต้องใช้ VLAN

1. เพิ่มประสิทธิภาพของเครือข่าย

ในระบบเครือข่ายทั่วไปจะมีการส่งข้อมูล Broadcast จำนวนมาก ทำให้เกิดความคับคั่ง (Congestion) และ VLAN มีความสามารถช่วยเพิ่มประสิทธิภาพของเครือข่ายได้เนื่องจาก VLAN จะจำกัดให้ส่งข้อมูล Broadcast ไปยังผู้ที่อยู่ใน VLAN เดียวกันเท่านั้น

2. ง่ายต่อการบริหารการใช้งาน

VLAN อำนวยความสะดวกในการบริหารจัดการโครงสร้างของระบบเครือข่ายให้ง่าย มีความยืดหยุ่น และเสียค่าใช้จ่ายน้อย โดยเพียงเปลี่ยน โครงสร้างทางตรรกะ (Logical) เท่านั้น ไม่จำเป็นต้องเปลี่ยนโครงสร้างทางกายภาพ กล่าวคือ ถ้าต้องการเปลี่ยนโครงสร้างของ VLAN ก็ทำโดยการคอนฟิกที่อุปกรณ์เครือข่ายใหม่ ไม่จำเป็นเปลี่ยนรูปแบบทางกายภาพของการเชื่อมต่อเครือข่ายที่มีอยู่เดิม

3. เพิ่มการรักษาความปลอดภัยมากขึ้น

เนื่องจากการติดต่อระหว่างอุปกรณ์เครือข่ายจะสามารถทำได้ภายใน VLAN เดียวกันเท่านั้น ถ้าต้องการที่จะติดต่อข้าม VLAN ต้องติดต่อผ่านอุปกรณ์ค้นหาเส้นทางหรือสวิตช์เลเยอร์สาม

ความแตกต่างระหว่าง Switched LAN กับ VLAN

- VLAN ทำงานบน Layer 2 และ 3 ของ OSI Model
- การเชื่อมต่อกันระหว่าง VLAN สามารถทำได้โดยการใช้เราเตอร์
- VLAN สามารถควบคุมการเกิด Broadcast บนเครือข่าย ขณะที่ Switches Hub แบบ Layer 2 ไม่สามารถทำได้
- ผู้ดูแลเครือข่ายเท่านั้น ที่จะเป็นผู้กำหนด การทำงานของ VLAN
- VLAN สามารถป้องกันความปลอดภัยของข้อมูลได้ดีกว่าสวิตช์ทั่วไป

5.3 ชนิดของ VLAN

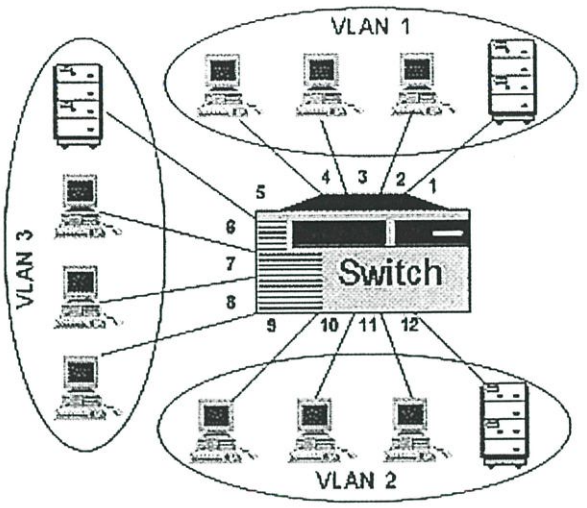
5.3.1 แบ่งตามประเภทของสวิตช์และลักษณะของการใช้งาน

โดยสามารถแบ่งออกเป็นแบบต่าง ๆ ดังนี้

1. Port-Based VLAN

Port-Based VLAN เป็น การจัดแบ่ง VLAN โดยอาศัยพอร์ตและหมายเลขพอร์ตเป็น

หลัก โดยเพียงแต่กำหนดว่า ในหนึ่ง Switches Hub มีกี่ VLAN มีชื่ออะไรบ้าง และต้องการให้พอร์ตใด หมายเลขใด เป็นสมาชิกของ VLAN ใดบ้าง



รูปที่ 5.2 แสดงลักษณะการแบ่ง VLAN โดยอาศัยหมายเลขพอร์ตเป็นหลัก

จากพอร์ตที่ 3 แสดงให้เห็นว่า VLAN 1 ประกอบด้วย เครื่องคอมพิวเตอร์รวมทั้งเครื่องเซิร์ฟเวอร์ที่เชื่อมต่อกับพอร์ตหมายเลข 1-4 และ VLAN 2 ประกอบด้วย คอมพิวเตอร์ ที่เชื่อมต่อกับพอร์ตหมายเลข 9-12 ส่วน VLAN 3 ประกอบด้วยคอมพิวเตอร์ที่เชื่อมต่อกับพอร์ตหมายเลข 5-8 เป็นต้น ขั้นตอนในการจัดตั้ง Port-Based VLAN สามารถกระทำได้โดยง่ายโดยมีขั้นตอนคร่าว ๆ ดังนี้

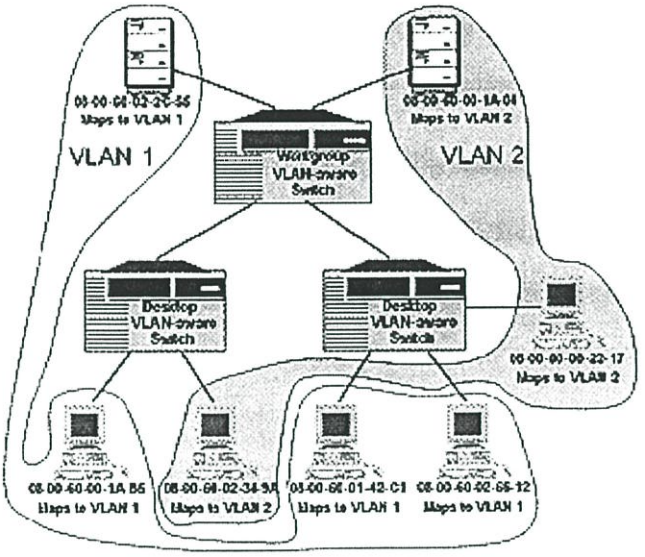
- กำหนด VTP Domain ให้เรียบร้อย (สำหรับสวิตช์ของ Cisco)
- กำหนดชื่อของ VLAN รวมทั้งเลขหมายของ VLAN
- กำหนดหมายเลขพอร์ตให้กับ VLAN แต่ละชุดที่ถูกสร้างขึ้น

ข้อเสียของ Port-Based VLAN ได้แก่การที่ สามารถเปลี่ยนแปลงได้ง่าย เนื่องจากผู้ใช้งานสามารถเปลี่ยนแปลงคอนฟิกของ VLAN ได้ ก็เพียงแต่ย้ายสายแลนจากหมายเลขพอร์ตหนึ่งไปยังพอร์ตอื่น ๆ ได้ง่าย ดังนั้นการโยกย้าย VLAN ก็เพียงแต่ย้ายสายแลนเท่านั้น

2. MAC Address-Based VLAN

MAC Address-Based VLAN เป็นการจัดตั้ง VLAN ที่อาศัย MAC Address เป็นหลัก ซึ่งแอดเดรสนี้เป็น แอดเดรสที่มาจากการ์ดแลนของเครื่องคอมพิวเตอร์แต่ละเครื่อง การแบ่ง VLAN

ด้วยการอาศัย MAC Address นี้ง่ายต่อการจัดคอนฟิกมาก เนื่องจากท่านไม่ต้องกำหนดเลขหมายของพอร์ต ไม่ต้องสนใจว่า เครื่องคอมพิวเตอร์ของท่านติดตั้งอยู่บนพอร์ตหมายเลขใด และไม่ต้องกลัวว่า จะมีใครย้ายเพื่อเปลี่ยน VLAN เนื่องจาก ไม่ว่าท่านจะย้ายไปอยู่ที่ใด บนสวิตช์ ตัวใด ตราบใดที่กำหนด MAC Address ประจำ VLAN แล้ว ท่านจะเปลี่ยนแปลง VLAN เองได้ก็ต่อเมื่อเปลี่ยนการ์ดแลนเท่านั้น (รูปที่ 5.3)



รูปที่ 5.3 แสดงลักษณะการเชื่อมต่อ VLAN กับ AC-Based VLAN

ข้อจำกัดของ MAC-Based VLAN

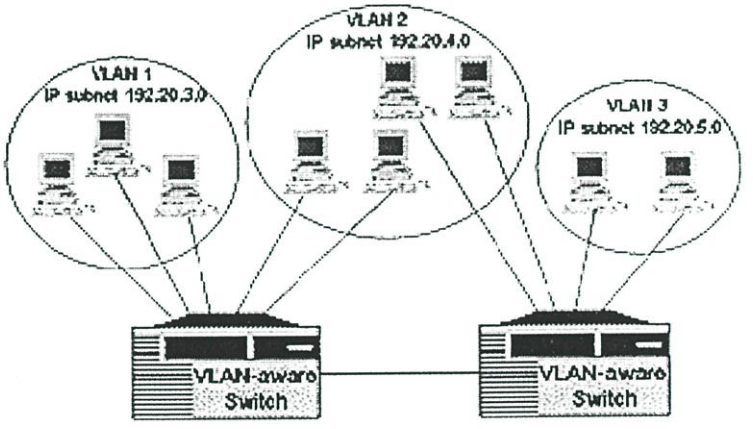
- พอร์ตที่จะเข้าร่วมใช้งานเป็น MAC-Based VLAN นั้นจะต้องไม่เป็น Static VLAN หมายความว่า จะต้องไม่มีการกำหนดหมายเลขพอร์ตที่ตายตัวให้กับ VLAN ต่างๆ
- MAC Based VLAN ถูกออกแบบมาให้สามารถสนับสนุน 1 ไคลเอนต์ต่อหนึ่งพอร์ต (ทางกายภาพสวิตช์บางรุ่น) ขณะที่บางสวิตช์สามารถสนับสนุนได้หลายยูสเซอร์ต่อ 1 พอร์ต

3. IP หรือ Subnet-Based VLAN

IP หรือ Subnet-Based VLAN บางครั้งถูกเรียกว่า Layer-3 Based VLAN เป็น VLAN ที่ถูกสร้างขึ้นโดยอาศัยข้อมูลข่าวสารในระดับ Network Layer โดยสวิตช์จะตรวจสอบข้อมูล IPที่ Header ของแพ็กเก็ต ปกติ IP หรือ Subnet-based VLAN จะถูกติดตั้งบนสวิตช์แบบ Layer 3

เท่านั้น ขณะที่ชนิดของ VLAN ที่ได้กล่าวมาก่อนหน้านี้ทำงานบน Layer-2 Switches รูปที่ 5.3 แสดงการใช้ Layer 3 Switches เพื่อสร้าง VLAN จำนวน 3 ชุดขึ้น จะเห็นว่ามีการแบ่ง VLAN ออกเป็นส่วน ๆ โดยใช้ เลขหมายไอพีที่อยู่ต่างเครือข่ายกัน มากำหนด VLAN ที่ต่างกันขึ้น ข้อดีของการจัด VLAN แบบนี้ มีอยู่ 3 แบบ ได้แก่

- ความยืดหยุ่น เนื่องจากท่านสามารถเปลี่ยนแปลง VLAN โดยการเปลี่ยน IP เท่านั้น ผู้ใช้งานสามารถโยกย้ายเครื่องออกจากพอร์ต ได้โดยไม่ต้องจัดคอนฟิกแอดเดรสของเครือข่ายกันใหม่ให้กับคอมพิวเตอร์แต่ละเครื่อง เหมาะสำหรับเครือข่ายที่ใช้โพรโตคอล TCP/IP เป็นหลัก
- ให้การสนับสนุนเราติ้ง โดยสนับสนุนการเชื่อมต่อระหว่าง VLAN ที่ต่างกันได้
- การจัด คอนฟิกของ VLAN แบบนี้ สามารถเกิดขึ้นได้โดยอัตโนมัติ ดังนั้นค่าใช้จ่ายในการที่จะดูแลการทำงานของ VLAN ประเภทนี้ จะถูกกว่า MAC Address-Based มาก



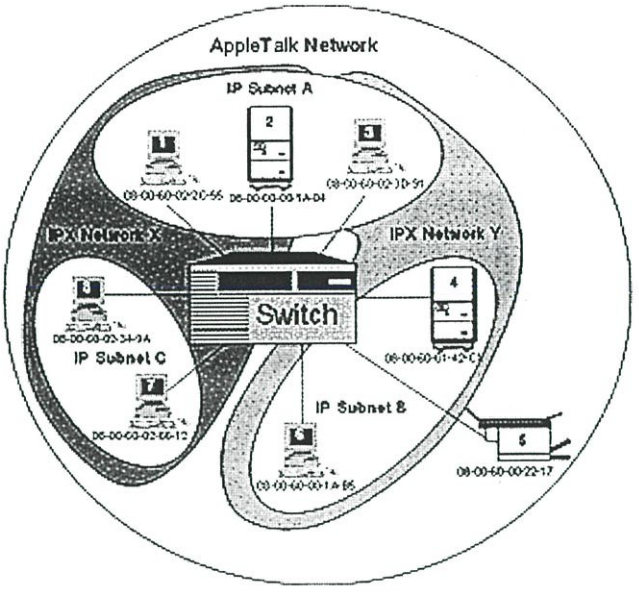
รูปที่ 5.4 แสดงการจัดตั้ง VLAN แบบ IP หรือ Subnet-Based VLAN

ข้อเสียของ IP หรือ Subnet-Based VLAN

ข้อเสียมีเพียงประการเดียว ได้แก่ การจัดตั้ง IP Address ที่อาจเกิดความสับสน รวมทั้งปัญหาของสวิตซ์บางรุ่นที่อาจสนับสนุนหลายไอพีแอดเดรสบนพอร์ตเดียวกัน

4. Protocol-Based VLAN

แบบของ VLAN แบบนี้ จะช่วยให้ท่านสามารถจัดสร้าง VLAN ได้อย่างง่ายดาย อย่างชนิดที่ไม่มีมาก่อน เนื่องจากว่า การกำหนด VLAN อาศัยโพรโตคอลการทำงานในระดับเน็ตเวิร์ค ซึ่งได้แก่ IP IPX หรือ AppleTalk (รูปที่ 5.5)



รูปที่ 5.5 แสดงลักษณะการจัดแบ่ง VLAN แบบ Protocol-Based

Protocol-Based VLAN ถูกนำมาใช้บ่อยในสถานการณ์ที่เครือข่ายประกอบด้วยหลาย Segment หรือติดตั้งสวิตช์หลาย ๆ ตัว รวมทั้งเครื่องคอมพิวเตอร์ต่างๆ มีการใช้โพรโตคอลที่แตกต่างกัน รวมทั้งเครื่องคอมพิวเตอร์เครื่องหนึ่งอาจติดตั้งใช้งานหลายโพรโตคอล เช่น มีการใช้งาน IP กับ NetBIOS ในเครื่องเดียวกัน

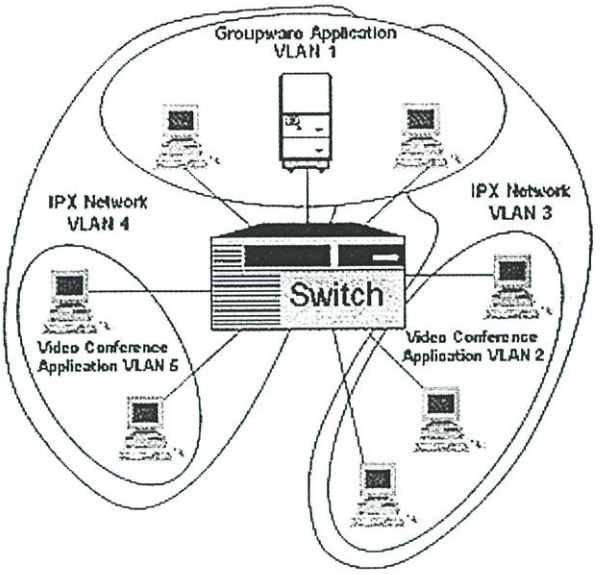
ข้อดีของการใช้ Protocol-Based VLAN

ได้แก่ความยืดหยุ่น เนื่องจากว่าท่านสามารถกำหนดว่า จะให้ใครเป็นสมาชิกของ VLAN ใด ก็แล้วแต่ว่าใครใช้โพรโตคอลอะไร การใช้ VLAN แบบนี้มีประโยชน์มาก เนื่องจากเครื่องคอมพิวเตอร์ หรือเครื่องเซิร์ฟเวอร์สามารถติดตั้งไว้ที่ใด หรือสวิตช์ตัวใดก็ได้ ตราบใดที่ยังเชื่อมต่อกันอยู่ ผู้ที่ใช้โพรโตคอลเดียวกัน จะสามารถสื่อสารถึงกันได้

5. Application-Based VLAN

สามารถติดตั้ง VLAN โดยอาศัยลักษณะหรือชนิดของแอพพลิเคชันได้ แต่สวิตช์ที่ให้การสนับสนุน การทำงานในลักษณะนี้ไม่ค่อยจะได้เห็นกันบ่อยนัก อีกทั้งมีราคาแพงมาก

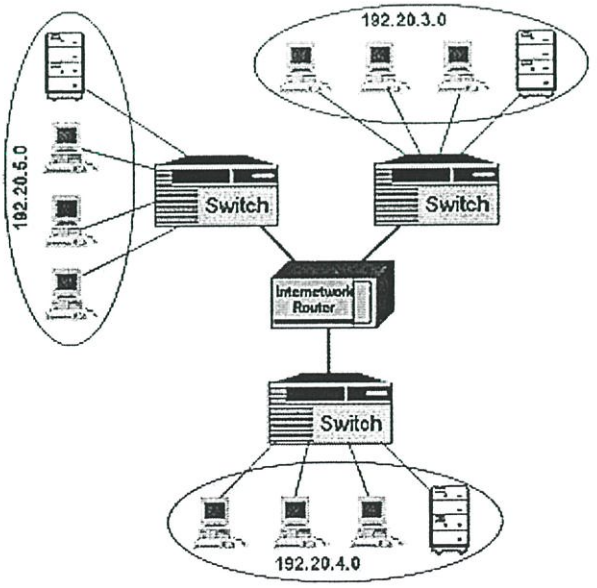
จุดประสงค์ของการแยก VLAN โดยอาศัยแอพพลิเคชันนี้ เป็นการเอื้อประโยชน์ให้กับแอพพลิเคชันแต่ละตัวที่สามารถใช้แบนด์วิดธ์ได้อย่างเต็มประสิทธิภาพ อีกทั้งสามารถแยกประเภทของงานออกได้อย่างชัดเจน Application-Based VLAN จึงมีประโยชน์สำหรับหน่วยงานที่ต้องใช้งานที่จำเพาะเจาะจงเฉพาะผู้ใช้กลุ่มต่าง ๆ



รูปที่ 5.6 แสดงลักษณะของ VLAN ที่อาศัยแอพเคชั่นที่ต่างกันเป็นหลัก

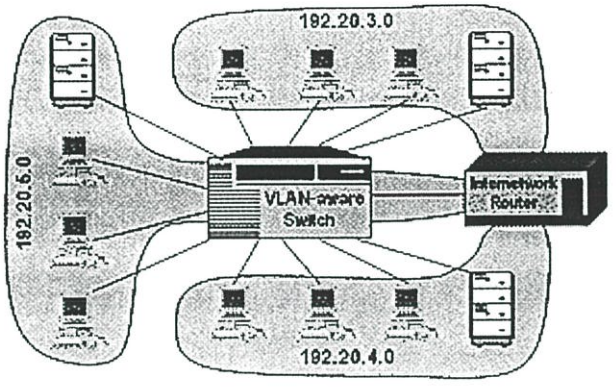
การเชื่อมต่อ VLAN เข้าด้วยกัน

ไม่เพียงจะสามารถติดตั้ง VLAN ได้ในสวิตช์ตัวเดียวเท่านั้น แต่ยังสามารถติดตั้ง VLAN ไว้ตามสวิตช์ต่าง ๆ ได้ และสามารถเชื่อมโยงสวิตช์ต่าง ๆ เข้าด้วยกัน (รูปที่ 5.7)



รูปที่ 5.7 แสดงลักษณะการเชื่อมต่อ VLAN ประเภท IP หรือ Subnet-based ด้วย เราเตอร์

นอกจากนี้ หากต้องการเชื่อมต่อ VLAN ต่าง ๆ เข้าด้วยกัน ให้สามารถมองเห็นกันและสื่อสารกันได้ มีเพียงวิธีเดียวคือการติดตั้งเราเตอร์ เพื่อเชื่อมต่อระหว่าง VLAN เข้าด้วยกัน รูปแบบการเชื่อมต่อ เป็นไปตามรูปที่ 8 ซึ่งเหมาะสำหรับการเชื่อมต่อ VLAN ที่อยู่ต่างสวิตช์เข้าด้วยกัน แต่ถ้าหากเป็นการเชื่อมต่อ VLAN ต่าง ๆ ที่ติดตั้งอยู่ในสวิตช์เดียวกัน ท่านสามารถใช้สวิตช์ตัวเดียว และเชื่อมต่อแบบ Single Edge หรือ One-arm Router ดูรูปที่ 5.8



รูปที่ 5.8 แสดงการเชื่อมต่อ VLAN แบบ One-arm หรือ Single Edge Router

5.3.2 เมื่อมีการติดตั้ง VLAN บนสวิตช์ในระดับ Access

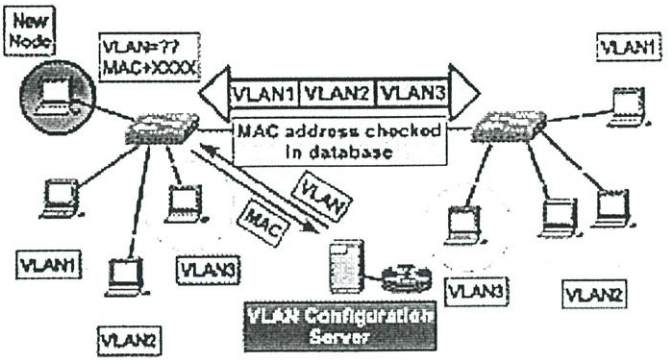
ต้องกำหนดว่าจะให้คอมพิวเตอร์ เครื่องใดเป็นสมาชิกของ VLAN วงใดบ้าง สำหรับเครือข่าย Cisco ได้กำหนดความเป็นสมาชิกภาพของ VLAN อยู่ 2 ชนิด ได้แก่ Static VLAN และ Dynamic VLAN

1. Static VLAN

Static VLANs เป็น VLAN ที่อาศัยการกำหนดหมายเลขของพอร์ตเป็นหลักในการกำหนดว่า จะให้เป็นสมาชิกของ VLAN วงใดบ้าง การกำหนดเช่นนี้ เป็นแบบตายตัว หมายความว่า ท่านจะต้องเป็นสมาชิกของ VLAN วงใดวงหนึ่งที่แน่นอน ตราบใดที่ท่านไม่ได้โยกย้ายสายแลนจากพอร์ตเดิมที่เครื่องคอมพิวเตอร์ของท่านติดตั้งอยู่ ให้ไปอยู่ที่พอร์ตอื่น ๆ ที่ได้กำหนดให้เป็น VLAN วงอื่นๆ หรือพูดง่ายๆ ก็คือ Static VLAN ก็คือ Port-Based VLAN ก็ไม่ผิดไปจากความจริงแต่อย่างใด

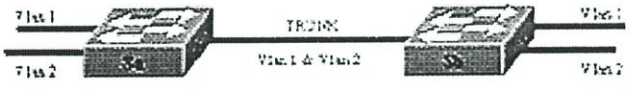
2. Dynamic VLAN

การกำหนดความเป็นสมาชิกภาพของ Dynamic VLAN นั้น อาศัย MAC Address ของ



รูปที่ 5.9 แสดงลักษณะการทำงานของ Dynamic VLAN ที่แสดงการใช้ MAC-Address เป็นหลัก

การ์ดแลนบนเครื่องคอมพิวเตอร์เป็นหลัก ไม่ว่าท่านจะย้าย เครื่องคอมพิวเตอร์ของท่านจากพอร์ตหนึ่งไปสู่พอร์ตใด ๆ ก็ตาม ท่านก็ยังไม่สามารถย้ายความเป็นสมาชิกภาพ ไปจาก VLAN เดิมที่ท่านสังกัดอยู่ ดังนั้น เราอาจกล่าวได้ว่า Dynamic VLAN ก็คือ MAC-Address-Based VLAN นั่นเอง (รูปที่ 5.9)



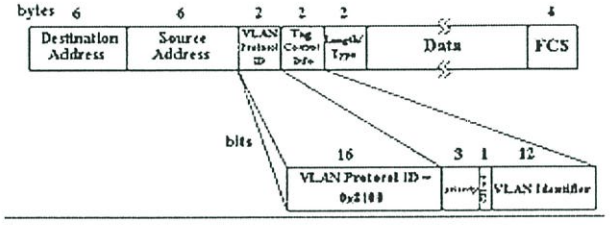
รูปที่ 5.10 จะเห็นว่า มีการเชื่อมต่อ VLAN 1 กับ VLAN 2 ระหว่างสวิตช์ทั้งสอง

หากมีเครื่องคอมพิวเตอร์เครื่องหนึ่ง ที่เป็นสมาชิก VLAN 1 ซึ่งอยู่ในสวิตช์ ชื่อ Sa ต้องการติดต่อกับคอมพิวเตอร์อีกเครื่องหนึ่งที่อยู่ใน VLAN 1 เช่นกัน แต่ติดตั้งอยู่ที่ Switches Hub ชื่อ Sb คำถามมีอยู่ว่า คอมพิวเตอร์ที่อยู่ใน VLAN 1 ของ Sa สามารถติดต่อกับคอมพิวเตอร์ ที่อยู่ใน VLAN 1 ของ Sb ได้อย่างไร? คำตอบคือ การใช้ วิธีการผสมผสานกันระหว่าง การใช้ VLAN Trunking กับการใช้ VLAN Tagging

การที่จะให้ Sb ทราบว่า เฟรมข้อมูลที่มาจาก Sa นั้น มาจาก VLAN หมายเลขใด และมีจุดประสงค์ปลายทาง ที่ Sb บน VLAN หมายเลขใดนั้น ต้องอาศัย กรรมวิธีที่เรียกว่า Tagged VLAN โดยกรรมวิธีนี้ เป็นมาตรฐาน ของการสอดแทรก ข้อมูลข่าวสารเพิ่มเติมลงไปที่ เฟรมข้อ

มูล ข้อมูลข่าวสารนี้ ประกอบไปด้วย เลขหมายหรือข้อมูลที่แสดงความเป็นสมาชิกภาพของ VLAN ต่างๆ และต้องการติดต่อกับ VLAN เลขหมายเดียวกัน กระบวนการสอดแทรกข้อมูลนี้ เราเรียกว่า Frame Tagging (รูปที่ 12)

การทำ Frame Tagging นี้เป็นมาตรฐาน ที่เรียกว่า 802.1q ซึ่งเป็นมาตรฐานที่ใช้งานทั่วไป กับ Switches Hub ประโยชน์ของการใช้ Frame Tagging นี้ ก็เพื่อให้สามารถสื่อสารกันระหว่าง VLAN หมายเลขเดียวกัน แต่อยู่ต่าง Switches Hub กัน



รูปที่ 5.11 แสดงลักษณะของการสอดแทรกข่าวลงไปบน เฟรมข้อมูลที่เรียกว่า Tagged Frame

5.4 Virtual Local Area Network (VLAN) Trunk Protocol (VTP)

VTP เป็นโพรโตคอลของ ที่มีไว้เพื่อการแพร่ข่าวสารเกี่ยวกับ VLAN จาก Switches Hub หนึ่ง ไปยัง Switches Hub อื่นๆ อย่างต่อเนื่อง

VTP จะทำให้ Switches Hub ที่ติดตั้ง VLAN ต่าง ๆ ไม่ว่าจะมีกี่ VLAN ก็ตาม จะต้องแพร่ข้อมูลข่าวสารเกี่ยวกับ VLAN จาก Switches Hub นั้น ออกมา ยัง Switches Hub อื่นๆ ที่เชื่อมต่อกัน ด้วยสายแลน การแพร่ข้อมูลข่าวสารนี้ จะเกิดขึ้น เป็นระยะ ๆ เป็นห้วงเวลาที่แน่นอน เมื่อ Switches Hub ผู้รับ ได้รับข้อมูลข่าวสารเกี่ยวกับ VLAN แล้ว ก็จะทำการ Update ข้อมูลเกี่ยวกับ VLAN ของ Switches Hub ต้นทาง การทำเช่นนี้ จะช่วยให้ ผู้ดูแลเครือข่ายได้รับความสะดวก เนื่องจาก หากมีการเปลี่ยนในการจัดคอนฟิกของ VLAN ที่ Switches Hub หนึ่ง ก็จะมีการ Update ข้อมูลของ VLAN ที่เปลี่ยนแปลงไปนี้ ให้กับ Switches Hub อื่นๆ ทุกตัวบนเครือข่าย ทำให้ผู้ดูแลเครือข่าย ได้รับความสะดวก คือไม่ต้องไม่ไล่จัดคอนฟิกของ VLAN ให้กับ Switches อื่นๆอีก

VTP เป็น Protocol ที่ใช้เพื่อการแพร่ข้อมูลและจัดให้มีการประสานการทำงาน เกี่ยวกับ Configuration ของ VLAN ให้สามารถแพร่กระจายจาก Switches Hub ตัวหนึ่งไปตาม Switches Hub ต่าง ๆ ที่ต้องเชื่อมกันบนเครือข่ายเดียวกัน แต่การที่จะทำเช่นนี้ ได้ ท่านจะต้อง

จัดคอนฟิกให้ Switches ตัวนั้น เรียก VTP ออกมาใช้ วิธีการเรียก VTP ออกมาใช้ ท่านจะต้องสร้างชื่อ VTP Domain ด้วยคำสั่ง ที่สามารถจัด คอนฟิกได้บน Switches Hub

VTP จัดเป็น Layer 2 Messaging Protocol ที่ใช้เพื่อดูแลและรักษา VLAN Configuration บน Switch ต่าง ๆ ไม่ว่าจะมีการปรับเพิ่ม/ลดหรือการเปลี่ยนแปลงชื่อใด ๆ ของ VLAN เกิดขึ้นก็ตาม นอกจากนี้ VTP จะช่วยลดความผิดพลาดของ Configuration ให้น้อยลงมากที่สุดได้ และสามารถป้องกันการมีชื่อ VLAN ซ้ำ หรือชนิดของ VLAN ที่ผิดข้อกำหนดในการทำงาน

VTP Management

สวิตซ์ที่อยู่ภายใต้ VTP Management Domain จะสามารถจัดแบ่งข่าวสารเกี่ยวกับ VLAN ได้โดยการใช้ วิธีการที่เรียกว่า VTP Advertisement ซึ่งมีอยู่ 3 แบบ ดังนี้

1. Advertisement Request: เกิดขึ้นเมื่อ Client (ในที่นี้หมายถึง Switches Hub ที่ถูกกำหนดให้เป็น Client) ได้ร้องขอ ข่าวสารเกี่ยวกับ VLAN สำหรับเครือข่ายขณะในขณะนั้นออกมา และ Switches Hub ที่ถูกกำหนดให้เป็น Server จะใช้ VTP เพื่อจัดส่ง Advertisement อันเป็นข่าวสารเกี่ยวกับ VLAN นี้กลับมาที่ Client พร้อมด้วยข้อมูล เช่น Version Field , Code Field , reserved Field, Management Domain Field (ขนาด 32 ไบต์) รวมทั้ง Start value field

2. Summary Advertisement : จะมีการส่ง Advertisement นี้ออกมาทุก 5 นาที (300 วินาที) ไปยัง สวิตซ์ต่าง ๆ ทั้งหมดบนเครือข่าย Summary Advertisement อาจถูกส่งออกมาทันที หาก Topology มีการเปลี่ยนแปลง เช่น สวิตซ์บางตัวหยุดทำงานหรือเพิ่มสวิตซ์เข้าไปที่เครือข่าย Summary Advertisement frame ประกอบด้วย Version Field , Code Field , Follower Field , Management Domain Name Field , Configuration version Number Field ข่าวสารที่ใช้แสดงตน ของผู้ Update , การประทับเวลา ของผู้ update และข้อมูลที่เข้ารหัสลับแบบ MD5

3. Sub-set Advertisement: ประกอบด้วยข้อมูลข่าวสารที่เป็นรายละเอียดเกี่ยวกับเครือข่าย รวมทั้ง version,Code,เลขหมายที่แสดงลำดับการทำงาน Management Domain Name Configuration version No. และ VLAN Information Field

VTP ADVERTISEMENT สามารถประกอบด้วยข้อมูลข่าวสาร ดังนี้

1. 802.10 SAID Values - สำหรับ FDDI Physical Media

2. Configuration Revision number ตัวเลขยิ่งสูง ข้อมูลก็ยิ่งได้รับการ Update มากขึ้น

3. Emulated LAN names - ใช้สำหรับ ATM LANE

4. Frame Format - ข้อมูลข่าวสารเกี่ยวกับ Format และ Content ของ Frame

5. Management Domain Name - ชื่อของ VTP Management Domain ถ้าหาก Switch ถูกจัด Configuration ให้มี 1 ชื่อและรับ Frame ที่มีชื่ออื่นเข้ามา ข้อมูลข่าวสารจะถูก ignored

6. MD5 Digest - ใช้เมื่อมีการใช้ Password ไปทั่วตลอดทั้ง Domain กุญแจที่ใช้จะต้อง Match กับกุญแจที่ให้ไว้กับเครื่องปลายทาง

7. Update Identity - ค่าที่แสดงความเป็นตัวตนของ Switch ที่ Forward ค่า Summery ไปที่ Switches อื่นๆ

8. VLAN Configuration - รวมทั้งข้อมูลข่าวสารของ VLAN ซึ่งเป็นที่รู้กันแล้วบนเครือข่าย รวมทั้ง Parameter เฉพาะเจาะจงและค่า MTU ของแต่ละ VLAN ใน VTP Management Domain

9. VLAN Identification - ข้อมูลข่าวสารเกี่ยวกับ ISL หรือ 802.1Q

- Advertisement Frame ถูกส่งออกไปที่ Multicast Address ดังนั้นอุปกรณ์ VTP ทุกตัวใน Management DOMAIN เดียวกันสามารถได้รับ Frame และ Frame จะไม่ได้รับการ Forward ภายใต้การควบคุมของ Bridge ตามปกติ
- VTP Management Domain มีอยู่ 2 แบบ ได้แก่
- Server Originating Advertisement
- Request advertisement จาก client ที่ต้องการข้อมูลข่าวสารของ VLAN เมื่อตอนที่ Client Boot up ระบบขึ้นมา
- แต่ละ Advertisement จะมี Revision No. เป็นส่วนสำคัญที่สุด เมื่อใดที่ VTP Database ถูก Modified ก็จะมีการเพิ่มค่า Revision No. เป็น 1 จากนั้น VTP Server จะ Advertise ข่าวสารนั้นจากฐานข้อมูลไปสู่ Switch ตัวอื่น ๆ

เมื่อ VTP Switch ได้รับ Advertisement ที่มี Revision No. สูงค่ากว่าในปัจจุบันก็จะมีการนำมา Update ที่ฐานข้อมูลปัจจุบัน ซึ่งอยู่ใน NVRAM

- ทุกครั้งที่ Server ส่ง Update Advertisement ออกมา มันจะเพิ่มค่า Revision No. 1 เลขหมาย หาก Client Switch ได้รับ 2 Advertisement พร้อมกัน มันรู้ว่าจะเลือกอันใด โดยดูจาก Revision No. ที่สูงกว่า

5.5 การทำงานของ VTP

การประกาศตัวของ VTP เป็นการส่งสถานะของ VTP ออกมานอกบนเครือข่ายในทุก ๆ 5 นาที หรือเมื่อมีการเปลี่ยนแปลง Configuration ของ VLAN ขึ้น

VTP ที่ประกาศออกมาจะถูกส่งออกมาบน default VLAN1 (จากผู้ผลิต) โดยการใช้ Multicast Frameโดยข้อความดังกล่าวจะครอบคลุมถึง Configuration Revision No. ซึ่งหมายถึง เป็น VLAN Information ที่ Update กว่าข้อมูลในปัจจุบัน

หากใช้คำสั่งเรียกดู ข้อมูลเกี่ยวกับ VTP บน Switches ท่านจะเห็นได้โดยใช้คำสั่งดังนี้

```
คำสั่ง Switch# sh vtp
VTP Version : 1
Configuration revision : 53
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
VTP domain name : Wildcats
VTP password :
VTP operating mode : server
VTP pruning mode : Disabled
VTP traps generation : Enabled
Configuration last modified by : 172.16.100.8 at 00-00-0000
00:00:00
```

Cisco มี 3 Switch Mode ที่ใช้เพื่อการจัด Configured ให้กับสวิตซ์เพื่อให้มีส่วนร่วมในการทำงานบน VTP DOMAIN ได้แก่

- Client Mode

- Server Mode
- Transparent Mode

5.5.1 Client Mode

Client Mode จะทำให้สวิตช์สามารถมีฟังก์ชันเดียวกับ Server Mode ยกเว้น แต่ว่ามันไม่สามารถเปลี่ยนแปลง VLAN INFORMATION ใด ๆ

Switch ที่ทำงานเป็น Client Mode ไม่สามารถเปลี่ยนแปลง VLAN Information ใด ๆ ไม่สามารถ Modify,Create, Delete VLAN บน Client Switch ใด ๆ แต่เมื่อใดที่มันได้รับประกาศจากสวิตช์ที่ทำงานใน Server Mode สามารถประกาศสถานะVLAN Configuration ของมัน รวมทั้งการทำ Synchronize VALN Information ไปที่ Switch อื่น ๆ บนเครือข่าย เมื่อใดที่ Restart แล้วค่า Global VLAN Info. จะหายไป

5.5.2 Server Mode

Server Mode จะถูกจัด Configured โดย Default สามารถให้ Create , Modify และ Delete VLAN เพื่อที่จะบริหารจัดการ Domain เมื่อมีการเปลี่ยนแปลง Configuration ก็จะมีการส่งไปที่สมาชิกอื่น ๆ ใน VTP Domain ใน 1 เครือข่ายอาจมีสวิตช์มากกว่า 1 ตัว ที่สามารถถูกจัด Configured ให้เป็น Server Mode เพื่อผลแห่ง Redundant

เมื่อใดที่ Restart Server แล้วค่า Configuration อันเป็น Global VLAN Information จะยังคงถูกรักษาไว้

5.5.3 Transparent Mode

Transparent Mode ทำให้ VTP Switch ที่ถูก Configured เป็น Mode นี้ ไม่ต้องรับ VTP Information ที่เข้ามาเพื่อ Update แต่จะส่งผ่านต่อไปยังสวิตช์ตัวอื่น ๆ ภายใน VTP Domain แม้ว่า Switch ใน Transparent Mode จะสามารถวิ่ง VTP Information รวมทั้งประกาศไปยัง Switch อื่น ๆ แต่มันจะไม่สามารถ Update ฐานข้อมูลตัวมันเอง รวมทั้งส่งออกข่าวสารเกี่ยวกับ Topology ที่เปลี่ยนไป

Mode นี้สวิตช์ทำหน้าที่ส่งผ่าน Information เฉย ๆ ไม่มี VTP Function ไม่มีการส่ง คำประกาศไม่มี Synchronization

แต่ VTP Version 2 อนุญาตให้ Transparent Mode สามารถ Forward คำประกาศที่ได้รับไปยัง Switch ที่ได้ถูกจัด Configured Trunk Port

Cisco ได้กำหนดไว้เป็นค่า Default ว่า ตัว Switches Hub ตัวแรกที่ติดตั้ง VLAN จะต้องทำงานในฐานะของ Server Mode ซึ่งหาก Switches Hub ใดทำงานเป็น Server Mode ตัว Switches Hub นั้น จะต้องรับผิดชอบในการแพร่ข่าวสารเกี่ยวกับ คอนฟิกของ VLAN ออกมา

ตารางที่ 5.1 แสดงขีดความสามารถของ Mode ต่างๆของ VTP Modes

Server Mode	Client Mode	Transparent Mode
Sends/forward VTP advertisements.	Sends/forwards VTP Advertisements.	ส่งผ่าน VTP advertisements.
ประสานการทำงานกับ VLAN	ประสานการทำงานกับ VLAN	ไม่ประสานการทำงานกับ VLAN
ค่าคอนฟิกของ VLAN เก็บไว้ใน NVRAM.	ค่า คอนฟิกของ VLAN ไม่ถูกเก็บไว้ใน NVRAM.	ค่าคอนฟิกของ VLAN จะถูกเก็บไว้ใน NVRAM
Catalyst switch สามารถสร้าง VLANs.	Catalyst switch ไม่สามารถสร้าง VLANs.	Catalyst switch สามารถสร้าง VLANs.
Catalyst switch สามารถแก้ไขข้อมูล VLANs.	Catalyst switch ไม่สามารถแก้ไขข้อมูล VLANs.	Catalyst switch แก้ไขข้อมูล VLAN
Catalyst switch สามารถลบVLANs.	Catalyst switch ไม่สามารถลบVLANs.	Catalyst switch สามารถลบ VLANs.

เมื่อใดที่มีการจัดตั้ง VTP บนสวิตซ์ท่านควรเลือก Mode ที่เหมาะสม เนื่องจาก VTP สามารถเขียนทับ VLAN Configuration ลงบนสวิตซ์บางตัวและสร้างปัญหาให้กับเครือข่ายได้

แนวทางการเลือก Mode

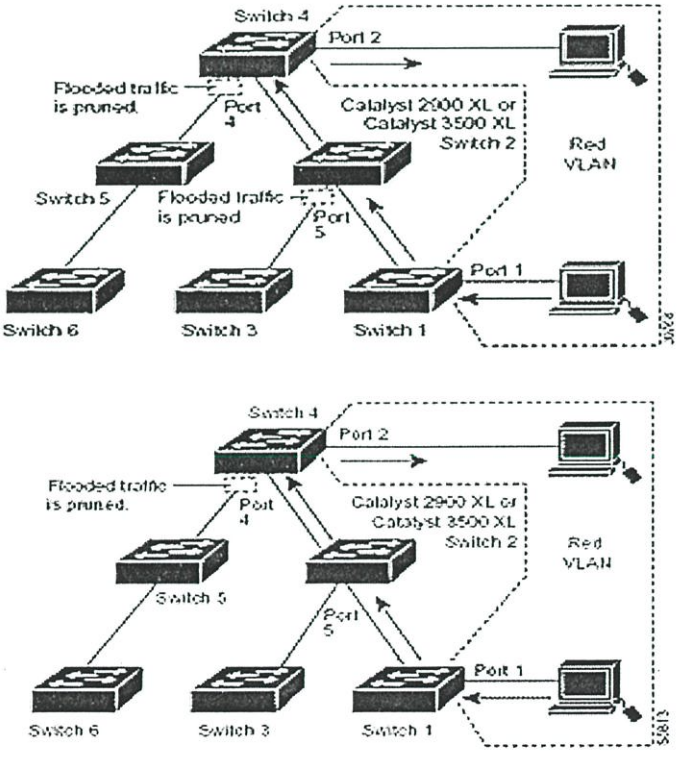
- Server Mode: ควรใช้กับสวิตซ์ที่ท่านจะใช้สร้าง, เปลี่ยนหรือลบ VLAN โดยเครื่องเซิร์ฟเวอร์จะส่งผ่านข่าวสารนี้ไปยังเครื่องเซิร์ฟเวอร์ตัวอื่น ๆ ที่ถูกจัด Configured เป็นเครื่องเซิร์ฟเวอร์หรือ เครื่องไคลเอนต์
- Client Mode: ควรใช้กับสวิตซ์ที่จะถูกนำมาเพิ่มเข้ามาเป็นเครือข่ายหรือเข้ามาเป็น VTP Domain ด้วยกันเพื่อป้องกันการถูกเขียนทับ

Transparent Mode: ใช้กับสวิตช์ที่เราต้องการจะส่งผ่าน Advertisement (VTP) ไปยังสวิตช์อื่นๆ แต่ก็ยังต้องการคงไว้ซึ่งขีดความสามารถที่จะบริหารจัดการ VLAN ได้อย่างอิสระ

5.5.4 VTP Pruning

VLAN VTP PRUNING ถูกใช้เพื่อการเพิ่มแบนด์วิดธ์ให้กับเครือข่าย โดยการลด LAN Traffic ที่วิ่ง ผ่าน Switch Trunk Link ซึ่ง LAN Traffic ในที่นี้หมายถึง ข้อมูลข่าวสารเกี่ยวกับ VLAN (รูปที่ 5.12)

VTP PRUNING จะทำหน้าที่ Filter Network Traffic เช่น Broadcast, Multicast และ Unicast บน Trunk Link ที่เชื่อมต่อที่ประกอบด้วย พอร์ตที่ไม่มี VLAN หมายความว่า VTP Pruning จะช่วยป้องกันมิให้ข้อมูลข่าวสารเกี่ยวกับ VLAN วิ่งไปยัง Switches Hub ใดที่ไม่ได้ติดตั้ง VLAN นั้นอยู่



รูปที่ 5.12 แสดงการใช้ VTP Pruning (บน) และไม่ได้ใช้ VTP Pruning(]ล่าง)

เมื่อ VTP Pruning ถูก Enable บนเครื่องเซิร์ฟเวอร์ข่าวสารจะถูกแพร่กระจายไปที่ไคลเอนต์ทั้งหมด รวมทั้ง สวิตซ์ที่ถูก Configure เป็น Server mode ใน VTP Management Domain

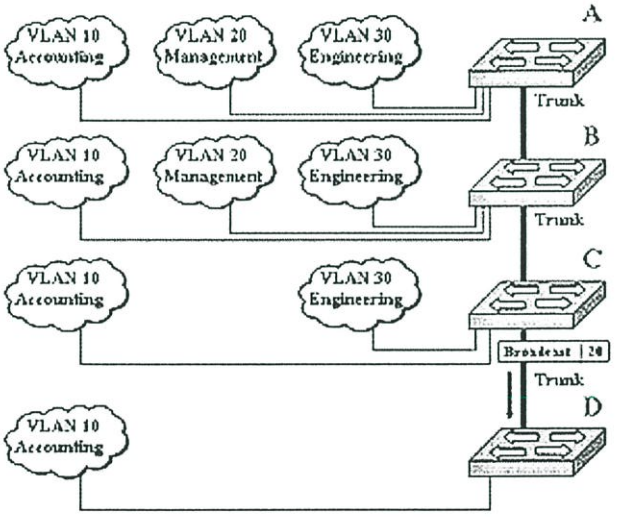
จากรูปที่ 5.13 อธิบายการทำงานได้ดังนี้

1. Switch A รับเอา Broadcast จากพอร์ตVLAN 20

2. Switch A จะ ส่งข้อมูลข่าวสารในรูปแบบ Broadcast เกี่ยวกับ VLAN 20 ออกไปยัง Trunk Port ทั้งหมดในกรณีนี้ Trunk Port ก็คือ สายสัญญาณเชื่อมต่อไปที่ Switch B

3. Switch B จะทำอย่างเดียวกับ Switch A คือ Forward Broadcast ออกไปที่ VLAN 20 ของ Switches B รวมทั้ง Trunk port ที่เชื่อมต่อกับ Switches C

4. Switch C จะทำซ้ำกระบวนการนี้ เพียงแต่ว่ามันไม่มี VLAN 20 ที่ Port ของมัน ดังนั้นมันจะ Forward หรือส่งต่อ เฟรมข้อมูลไปข้างหน้า ซึ่งก็คือไปที่ Trunk port ทั้งหมด



รูปที่ 5.13 แสดงการส่งต่อของข่าวสารเกี่ยวกับ VLAN ภายใต้ VTP

5. เมื่อ Switch D ได้รับ Broadcast สำหรับ VLAN 20 มันจะ ละทิ้งไป เนื่องจาก Switch D ไม่มี port VLAN 20 หรือ Trunk port อื่นนอกจาก Trunk port ที่มันรับ Broadcast เข้ามา จะเห็นว่า Broadcast Traffic ที่วิ่งมาจาก Switch B มายัง C จาก C มายัง D เป็นเรื่องไม่จำเป็น

การใช้ VTP Prunning จะ ทำให้ Switches ทำการกีดกันมิให้มีการ Forward Traffic ที่ไม่จำเป็นเหล่านี้ออกมา โดยการแลกเปลี่ยนข่าวสาร VLAN ที่ Active อยู่ ก็จะทำให้ Switches

จะสามารถล่วงรู้ได้ว่า Traffic ใดเป็นของจำเป็น จากตัวอย่างนี้ VTP Prunning จะป้องกันมิให้ Forward Broadcast ที่ไม่จำเป็นออกมา

แนวทางการทำ VLAN Configuration

- สามารถติดตั้งสูงสุดได้ไม่เกิน 64 VLAN สำหรับ Desk Top Catalyst Switches ทั่วไป เช่น รุ่น 1900
- รุ่น 1900 ได้รับการจัดตั้ง Default ให้ทุก Port เป็น VLAN1 จากโรงงานที่มีการใช้ CDP และ VTP Advertisement
- Catalyst 1900 IP Address จะต้องอยู่ใน VLAN 1 Broadcast Domain (หมายความว่า Catalyst 1900 ต้องการมี IP Address เพื่อที่จะสามารถใช้ Telnet เข้ามา บริหารจัดการ ภายในได้ โดย IP Address นี้จะต้องอยู่ใน VLAN1 โดย Default)
- นอกจาก Telnet แล้ว ยังสามารถใช้ Visual Switch Manager (VSM) โดยทำงาน บน HTTP Browser เพื่อ Configured Switch
- ก่อนที่จะเริ่มสร้าง VLAN Switch จะต้องอยู่ที่ VTP Server Mode หรือ VTP Transparent Mode หากท่านต้องการจะให้ข่าวสาร VLAN วิ่งไปยัง Switch อื่นใน Domain ให้ใช้ Server Mode หากต้องการเพียง Add, VLAN เข้าไปที่ Local Switch ให้ใช้ Transparent Mode

ขั้นตอนการจัด Configuration Mode

1. ก่อนจะสร้าง VLAN ท่านจะต้องตัดสินใจว่าจะให้ใช้ VTP เพื่อดูแลรักษา Global VLAN Configuration Information บน Network หรือไม่?

2. ถ้าต้องการให้ VLAN กระจายไปตาม Switch Hub ต่างๆ ด้วย Single Link ท่านจะต้อง

Configured Fast Ethernet Trunk เพื่อ Interconnect ระหว่าง Switch

3. โดยค่า Default แล้ว Switch ปกติจะถูกจัดเป็น Server Mode อยู่แล้ว ดังนั้นสามารถเพิ่มหรือเปลี่ยนแปลงหรือลง VLAN ได้เลย แต่หาก Switch นั้นถูกตั้งเป็น Client Mode, VLAN จะไม่สามารถถูกเพิ่ม, เปลี่ยนแปลงหรือลบทิ้ง

4. ความเป็นสมาชิกของ VLAN บน Switch Port จะถูกกำหนดได้แบบ Manual แบบที่จะ Port เท่านั้น เมื่อท่านกำหนด Switch Port ให้กับ VLAN

แนวทางการจัด VTP Configuration

- VTP domain name : กำหนดชื่อของ VTP Domain
- VTP mode: Server
- VTP password : None (Option)
- VTP pruning : Disabled
- VTP trap : Enabled

Domain Name สามารถถูกกำหนดโดย Administrator หรือเรียนรู้เองจาก Trunk Line ที่ถูกจัด Configured ไว้แล้ว จาก Server ที่ได้มีการจัดตั้งชื่อ Domain ไว้แล้ว โดย Default แล้ว Domain Name ไม่ถูกจัดตั้งและโดย Default : Switch จะถูก Set เป็น VTP Server Mode

- ท่านสามารถให้ password แก่ VTP Management Domain โดยพาสเวิร์ดที่ใส่เข้าไปจะต้องเหมือนกันกับสวิตช์ทั้งหมดภายใน Domain หากท่าน Configured VTP password, VTP จะทำงานไม่ปกติจนกว่าท่านจะได้กำหนดชื่อ password เดียวกันไปที่สวิตช์ภายใน Domain
- VTP pruning เป็น Parameter หนึ่งของ VLAN ที่จะได้รับการ Advertised โดย VTP Protocol การ Enable หรือ Disable Pruning บน VTP Server จะมีการแพร่ ออกไปทั่วทั้ง Domain การ Enable หรือ Disable VTP Pruning บน VTP Server จะมีผลกระทบต่อ Management Domain ทั่วทั้งหมด
- VTP Trap จะถูก Enable โดย Default ซึ่งจะทำให้ SNMP Message ถูกสร้างขึ้นทุกครั้งที่มีการส่ง VTP Message ใหม่ๆ

5.6 ขั้นตอนการ Configuration VLAN และ VTP

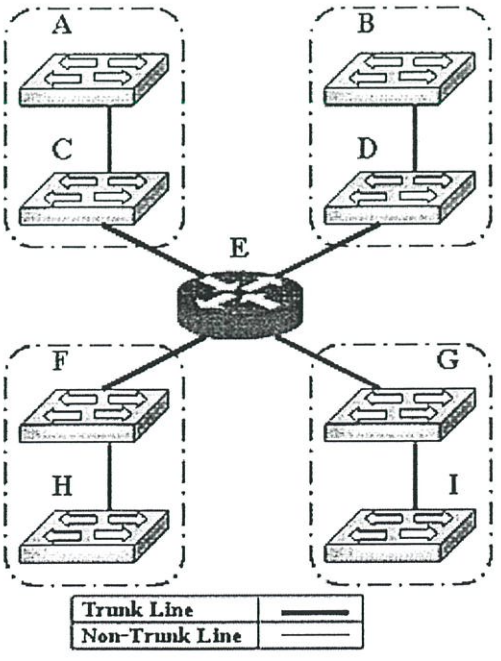
ก่อนที่จะติดตั้ง VLAN จะต้องวางแผนโดยที่ขั้นตอนหรือวิธีการติดตั้ง VLAN ขึ้นอยู่กับลักษณะการเชื่อมต่อของ Switching Hub จำนวนของ VLAN รวมทั้งตำแหน่งของ VLAN ที่กระจัดกระจายไปตาม Switching Hub ต่าง ๆ ถ้าหากบนเครือข่ายมี Switching Hub เพียงตัวเดียว ไม่ว่าจะมี VLAN มากเท่าใดก็ตาม รูปแบบการจัด Configure ก็ยังไม่สลับซับซ้อนเท่ากับ VLAN ที่กระจัดกระจายไปตาม Switching Hub ต่าง ๆ

สมมติว่าท่านมี Switching Hub ที่เชื่อมต่อกันบนเครือข่ายอยู่ 3 ตัว และมีจำนวนของ VLAN อยู่ 3 VLAN ที่กระจัดกระจายไปตาม Switching Hub ทั้ง 3 ลักษณะนี้การติดตั้ง VLAN ขั้นพื้นฐานจะต้องประกอบด้วยขั้นตอนดังต่อไปนี้

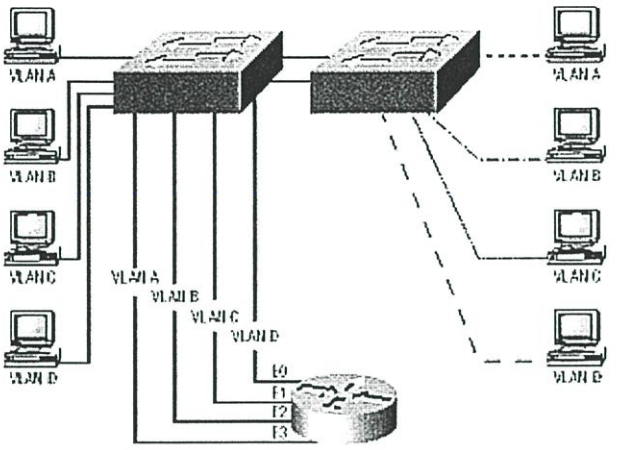
- กำหนดให้มี VTP Domain โดยกำหนดชื่อของ VTP Domain
- กำหนด Mode การทำงานของ Domain (ส่วนนี้ เป็น Option)
- กำหนด Password เพื่อป้องกัน Domain
- กำหนด Version ของ VTP Domain
- กำหนดให้ มีการใช้งาน VTP Pruning
- กำหนดชื่อและเลขหมายของ VLAN ทั้งหมด
- จัดสร้างสมาชิกของแต่ละ VLAN ขึ้น

5.6.1 จัดสร้าง VTP Trunking

กำหนดให้มี VTP Domain เหตุผลของการที่ต้องมี Domain ก็เพื่อให้เกิดประสิทธิภาพในการจัดการ VLAN ที่กระจายไปตาม Switching Hub ต่างๆ ได้เป็นอย่างดี เนื่องจาก VLAN นั้นได้กระจายไปตาม Switching Hub ต่างๆ เพื่อให้ง่ายต่อการจัดการการกำหนดให้มี VTP Domain จะช่วยให้ข้อมูลข่าวสาร ของ VLAN ใน Switching Hub หนึ่งสามารถถูกถ่ายทอดไปยังอีก Switching Hub หนึ่งที่เป็น VLAN เดียวกันได้อย่างง่ายดาย และเป็นไปโดยอัตโนมัติอีกด้วย



รูปที่ 5.14 แสดงลักษณะ VTP Domain



รูปที่ 5.15 แสดงลักษณะการเชื่อมต่อระหว่าง Domain ด้วยเราเตอร์

5.6.2 การจัดตั้ง VTP Domain

วิธีการจัดตั้ง VTP Domain ได้แก่การ ใช้คำสั่ง ดังต่อไปนี้

```
Console> (enable) set vtp domain [ชื่อ]
```

ตัวอย่าง เช่น

```
Console>  (enable)  set  vtp  domain  ABC
VTP  domain  ABC  modified
Console> (enable)
```

หลังจากที่จัดตั้ง VTP Domain เป็นที่เรียบร้อยแล้ว ท่านอ่านพิจารณาเลือก Mode การทำงานของ VTP Domain ซึ่งการเลือก Mode นี้ถือเป็นทางเลือก (option) เท่านั้น ซึ่งปกติ Switching Hub ใดที่ถูกจัดตั้ง Configure ให้เป็น VTP Domain ตัว Domain ใน Switching Hub นั้นๆ จะมีค่าเป็น Server Mode โดยปริยาย (เหตุผลและคุณประโยชน์ในการเลือก VTP Mode ต่างๆ นี้

การเลือก Mode การทำงานของ VTP Domain

ที่ Console ของ Switch ให้ใช้คำสั่ง ดังนี้

```
Console > (enable) set vtp mode [mode ที่จะเลือก]
```

หมายเหตุ : Mode ของ VTP มีอยู่ 3 Mode ได้แก่ Server Mode (default) Client Mode และ Transparent Mode

ตัวอย่าง เช่น หากต้องการเปลี่ยนจากค่าปริยาย (ค่า Default) ที่เป็น Mode Server ให้เป็น Client ดังนี้

```
Console> (enable) set vtp mode client
VTP Domain ABC modified
```

หลังจากที่เปลี่ยนจาก Server Mode เป็น Client Mode แล้ว ลองจัดตั้ง VLAN บน Switching Hub ที่ถูกตั้งให้เป็น VTP Client Mode จะปรากฏข้อความ ดังนี้

```
Console> (enable) set vlan 30
Cannot add/modify VLANs on a VTP Client.
Console> (enable)
```

จากตัวอย่างที่แสดงการเปลี่ยน Mode การทำงานจาก Server Mode มาเป็น Client Mode จะเห็นว่า ท่านไม่สามารถจัดตั้ง VLAN ใดๆ บน VTP Domain ที่ถูกกำหนดให้เป็น Client Mode เนื่องจาก Client Mode ทำหน้าที่รับเอาข้อมูลข่าวสาร เกี่ยวกับ VLAN ที่มาจาก Switching Hub ที่ ถูกจัดตั้งให้เป็น VTP Domain ที่ เป็น Server Mode เพื่อใช้ Update เท่านั้น ดังนั้น หากท่านต้องการสร้าง VLAN ใหม่ๆ เกิดขึ้นที่ Switching Hub ใดก็ตาม ท่านจะต้องให้ Switching Hub นั้น ติดตั้ง VTP Domain ที่ทำงานบน Server Mode เท่านั้น

การยกเลิก VTP Mode

สำหรับ Switching Hub รุ่นใหม่ของ Cisco ที่ใช้ COS Version 7.1.1 จะมีทางเลือกให้สามารถยกเลิกการใช้งาน VT Mode ได้ โดยจุดประสงค์ของการยกเลิก VTP Mode ก็ด้วยเหตุผล ที่ท่านต้องการจะบริหารจัดการกับ VLAN เฉพาะเพียง Hub เดียว โดยไม่ต้องไปยุ่งเกี่ยวกับ Hub อื่นๆ โดยท่านสามารถใช้คำสั่ง ดังนี้

```
Console> (enable) set vtp mode off
```

หลังจากที่ท่านจัดตั้ง VTP Domain แล้ว ท่านสามารถเรียกดู VTP Domain ที่ท่านจัดตั้งขึ้นมา ดังนี้

```
Console> (enable) show vtp domain
```

จะปรากฏหน้าจอ ดังนี้

```
Switch>  show  vtp  domain
Domain Name    Domain Index  VTP Version  Local Mode  Password
Mydomain       1             2            server      -
```

Vlan-count	Max-vlan-strorage	Config Revision	Notifications
15	1023	7	disabled
Last Updater	V2 Mode	Pruning	PruneEligible on Vlans
192.168.1.4	enabled	disabled	2-1000

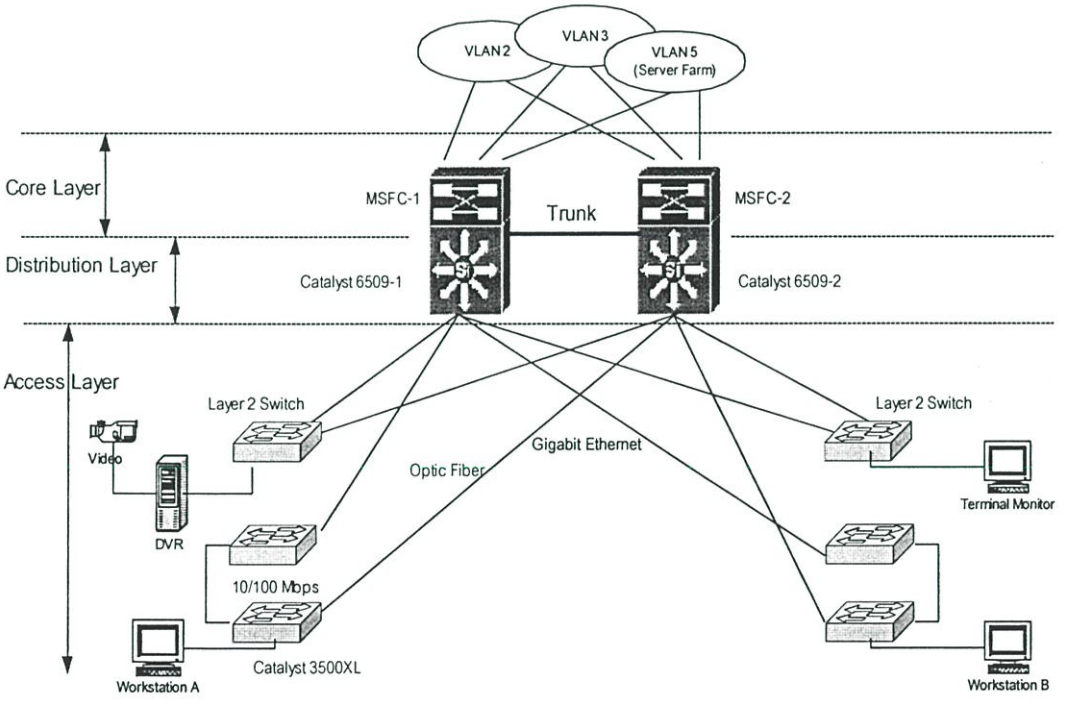
Switch>

จากตัวอย่างที่แสดงนั้นจะเห็นรายละเอียดของ VTP Domain ที่มีอยู่ เช่น ชื่อของ Domain ที่ถูกตั้งขึ้น (ในที่นี้คือ mydomain จำนวนของ Domain Version ของ Domain Mode การทำงานของ Domain สถานะของ VTP Pruning เป็นต้น

บทที่ 6
แบบจำลองการทดสอบเพื่อศึกษาการทำงานของระบบเครือข่าย

6.1 การออกแบบการเชื่อมโยงเพื่อใช้ในการทดสอบ

ในการเลือกใช้อุปกรณ์เพื่อนำมาทำการทดสอบจำเป็นต้องคำนึงถึงอัตราการส่งผ่านแพ็กเกต (Forwarding Packet Rate) ความสามารถในการรองรับภาระร่วม (Load Sharing) และความสามารถในการทำ Redundant Backup ของอุปกรณ์เป็นหลัก เพื่อรองรับการส่งผ่านข้อมูลในเครือข่ายให้ทันต่อการตอบสนองของแอพพลิเคชันต่าง ๆ ได้อย่างรวดเร็ว รวมทั้งสร้างความเสถียรและความมีประสิทธิภาพให้แก่ระบบเครือข่ายได้มากที่สุด โดยกำหนดรูปแบบการเชื่อมต่อ (Topology) ไว้ดังรูปที่ 6.1



รูปที่ 6.1 แบบจำลองโครงสร้างระบบเครือข่าย

จากรูปเป็นการออกแบบระบบเครือข่ายเพื่อทำการทดสอบ โดยแบ่งการเชื่อมต่อให้เป็นลำดับชั้นเพื่อลดการทำงานของ CPU บนอุปกรณ์เครือข่ายในการจัดการกับแพ็กเกตที่ทำการบรอดคาสท์ ซึ่งสามารถแบ่งได้เป็น 3 ลำดับชั้น ดังนี้

1. ลำดับชั้นแกนกลาง (Core Layer)

ในลำดับชั้นนี้ถือได้ว่าเป็นชั้นที่สำคัญที่สุด หรือเรียกว่าแบ็คโบนก็ได้ เพราะอุปกรณ์ในชั้นนี้จะทำงานในระดับเลเยอร์ 3 ของ OSI Model หรือ Network Layer ซึ่งทำหน้าที่หาเส้นทาง และส่งข้อมูลข้ามระหว่าง VLAN ด้วยความเร็วสูง เช่น การแอคเซสระบบฐานข้อมูลข้ามผ่าน VLAN ของผู้ใช้กับ VLAN ของเซิร์ฟเวอร์ เป็นต้น รวมทั้งยังต้องมีการติดต่อกับอุปกรณ์ในเลเยอร์ 2 จึงทำให้อุปกรณ์ในลำดับชั้นนี้มีความสำคัญสูง ดังนั้นในลำดับชั้นนี้เราจึงต้องมีอุปกรณ์สำรอง เพื่อให้คงประสิทธิภาพสูงสุดและสามารถสร้างเส้นทางสำรองได้อย่างรวดเร็วเมื่อเกิดเหตุสุดวิสัยขึ้นกับอุปกรณ์ ในการออกแบบลำดับชั้นนี้ต้องมีความซับซ้อนน้อยสุดและต้องสามารถควบคุมได้ง่าย

ดังนั้นในลำดับชั้นแกนกลางจึงเลือกใช้สวิตช์เลเยอร์ 3 ร่วมกับเทคโนโลยีกิกะบิทอีเทอร์เน็ท เป็นอุปกรณ์ในการส่งผ่านข้อมูล เรียกว่า Multilayer Switch Feature Card (MSFC) โดยทำหน้าที่จัดหาเส้นทางให้กับ multilayer switching (MSL) ที่มีความเร็วในการสลับเส้นทางได้มากที่สุดถึง 15 ล้านแพ็กเกตต่อวินาที (Mpps) เพื่อทำการอินเตอร์เฟสกับอีเทอร์เน็ทสวิตช์ โดยการทำงานของ MLS นั้นสามารถรองรับการใช้งานของโพรโตคอลต่างๆ เช่น IP, IP multicast และ Inter Network Packet Exchange (IPX) เป็นต้น ซึ่งในแบบจำลองการทดลองดังรูปที่ 6.1 ได้ทำการติดตั้ง MSFC ไว้บน Catalyst 6509 ซึ่งทำงานในระดับชั้นการกระจาย (Distribution Layer) ไว้ตัวละ 1 โมดูลเพื่อสร้างความเสถียรให้กับระบบ โดยใช้ฟังก์ชัน Hot Standby Routing Protocol (HSRP) ซึ่ง MSFC ทั้งสองจะทำงานบน routing protocol และตารางเส้นทางเดียวกัน แต่จะไม่ทำงานพร้อมกัน ในที่นี้กำหนดให้ MSFC ตัวที่ 1 มีสภาวะเป็น Active หรือทำงาน และ MSFC ตัวที่ 2 มีสภาวะเป็น Standby หรือพร้อมทำงาน ดังนั้นเวลาที่เกิดความผิดพลาดขึ้นใน MSFC ตัวที่ 1 จะทำให้ MSFC ตัวที่ 2 เปลี่ยนจากสภาวะ Standby เป็น Active ทำให้ไม่ต้องใช้เวลาเพื่อรอรวบรวมตารางเส้นทางใหม่และสามารถส่งผ่านข้อมูลต่อไปได้โดยไม่เกิดการสะดุดของข้อมูล

2. ลำดับชั้นการกระจาย (Distribution Layer)

ลำดับชั้นการกระจายเป็นตัวกลางในเครือข่ายเพื่อเชื่อมระหว่างลำดับชั้นแกนกลางและลำดับชั้นการเข้าถึง อุปกรณ์ในชั้นนี้จะทำงานในระดับเลเยอร์ 2 หรือ Datalink Layer โดยหน้าที่ของลำดับชั้นนี้ คือ ควบคุมการทำงานของอุปกรณ์ในลำดับชั้นการเข้าถึง ซึ่งจะทำให้เกิดความปลอดภัยในเครือข่าย ควบคุมทราฟฟิกในเครือข่ายให้เป็นตามข้อกำหนดในลำดับชั้นแกนกลาง และทำการวิเคราะห์บรอดคาสท์โดเมนส์ เมื่อมีการใช้ VLAN

ในการควบคุมอุปกรณ์ในลำดับชั้นการเข้าถึงได้ใช้ฟังก์ชัน VLAN Trunking Protocol (VTP) โดยกำหนดสถานะเป็นเซิร์ฟเวอร์ ทำให้สามารถสร้างและส่งข้อความแจ้งสถานะของ VLAN ให้ตรงกันระหว่างอุปกรณ์ในลำดับชั้นการกระจายและลำดับชั้นการเข้าถึง ซึ่งในที่นี้คือ Catalyst

6509 และ Catalyst 3500XL ตามลำดับ รวมถึงทำหน้าที่จัดการเกี่ยวกับการเพิ่ม ลบ และเปลี่ยนชื่อของ VLAN บนเครือข่ายได้จากอุปกรณ์ในลำดับชั้นนี้เท่านั้น

การออกแบบในลำดับชั้นนี้ ได้คำนึงถึงความเสถียรของเครือข่าย จึงได้ทำการติดตั้งอุปกรณ์ Catalyst 6509 ไว้ 2 ชุดด้วยกันและทำการเชื่อมต่ออุปกรณ์ทั้งสองเข้าด้วยกันด้วยเทคโนโลยีกิกะบิทอีเทอร์เน็ท (IEEE 802.3z) กอปรกับฟังก์ชัน VLAN Trunking ซึ่งจะทำให้การส่งผ่านข้อมูลระหว่างอุปกรณ์สมบูรณ์มากยิ่งขึ้น

3. ลำดับชั้นการเข้าถึง (Access Layer)

ในลำดับชั้นนี้เป็นการเชื่อมต่อผู้ใช้งานให้สามารถทำการติดต่อกับทรัพยากรที่มีอยู่บนระบบเครือข่ายได้ ซึ่งลำดับชั้นนี้อาจใช้อุปกรณ์สวิตช์ บริดจ์ หรือฮับก็ได้ แต่การออกแบบในที่นี้เราเลือกใช้ สวิตช์เลเยอร์ 2 เป็นอุปกรณ์ในการส่งผ่านข้อมูล เพราะสวิตช์มีกระบวนการที่เรียกว่า Store-and-forward และ cut-through ซึ่งบนบริดจ์จะมีเฉพาะกระบวนการ Store-and-forward เท่านั้น โดยหลักการของบริดจ์เมื่อได้รับข้อมูลเข้ามาจะต้องทำการรอจนได้รับข้อมูลในหนึ่งเฟรมจนครบ จากนั้นจึงจะกำหนดพอร์ทขาออกและทำการคำนวณหา CRC แล้วจึงจะส่งเฟรมนั้น ๆ ไปยังพอร์ทที่ได้ถูกกำหนดไว้ ส่วนการส่งข้อมูลของสวิตช์นั้นจะทำแค่เพียงมองแอดเดรสปลายทางซึ่งอยู่ในฟิลด์แรกของอีเทอร์เน็ทเฟรม แล้วทำการส่งข้อมูลในรูปของบิทออกไปยังพอร์ทขาออกที่ถูกกำหนดไว้

การออกแบบการเชื่อมต่อระหว่างลำดับชั้นการเข้าถึงและลำดับชั้นการกระจาย ใช้รูปแบบการเชื่อมต่อแบบ 2 ทางโดยคำนึงถึงการทำ Redundant Backup กล่าวคือ อุปกรณ์ 1 ตัวในลำดับชั้นการเข้าถึงซึ่งในที่นี้ใช้ Catalyst 3500XL ต่อเข้ากับอุปกรณ์ในลำดับชั้นการกระจาย 2 ตัว ในที่นี้ใช้ Catalyst 6509 ดังแสดงในรูปที่ 6.1โดยใช้โพรโตคอล Spanning-tree (STP) เพื่อจัดการทราฟฟิก และป้องกันการลูปของเครือข่ายในเลเยอร์ 2 ซึ่ง STP จะทำการ Forward แพ็กเกตผ่านพอร์ทที่เป็น root โดยดูจากค่าที่กำหนดในพอร์ท ซึ่งพอร์ทที่มีค่าน้อยที่สุดจะเป็นพอร์ทที่มีค่า priority สูงสุดเป็นพอร์ท root ส่วนพอร์ทที่มีค่า priority ต่ำกว่าจะทำการ Block แพ็กเกตไม่ให้ผ่านพอร์ทนั้น ๆ ในส่วนของการเพิ่มหรือลดจำนวน VLAN จะขึ้นอยู่กับ VTP ที่มีสถานะเป็นเซิร์ฟเวอร์เท่านั้น ในที่นี้ Catalyst 6509 มีสถานะเป็น VTP Server ส่วน Catalyst 3500XL มีสถานะเป็น VTP Client

6.2 การกำหนดพารามิเตอร์ในแบบจำลอง

ในการกำหนดค่าพารามิเตอร์ที่ใช้กับแบบจำลองนี้สามารถแบ่งออกได้เป็น 2 ส่วนหลัก ๆ คือ

1. ค่าพารามิเตอร์ที่ใช้ในการเชื่อมโยงอุปกรณ์ในลำดับชั้นการเข้าถึงและชั้นการกระจาย

การออกแบบการเชื่อมโยงอุปกรณ์ดังกล่าวข้างต้น ก็คือการเชื่อมต่ออุปกรณ์สวิตช์เลเยอร์ 2 กับสวิตช์เลเยอร์ 3 เข้าด้วยกัน ซึ่งหมายถึง Catalyst 3500XL กับ Catalyst 6509 จึงจำเป็นต้องคำนึงถึงความแออัดของข้อมูลที่จะเกิดขึ้นจนเป็นคอขวดได้ ในที่นี้จึงใช้อินเทอร์เฟสแบบกิกะบิทเชื่อมโยงอุปกรณ์เข้าด้วยกันด้วยสายใยแก้วนำแสง (Fiber Optic) เพื่อลดความสูญเสียหรือความผิดพลาดของข้อมูลให้น้อยที่สุด โดยเลือกใช้โพรโตคอล Trunk 802.1q ซึ่งเป็นมาตรฐานของ IEEE ในการเชื่อมโยงสวิตช์เข้าหากัน เพื่อการรับส่งข้อมูลและทราฟฟิกของ VLAN ต่าง ๆ ระหว่างสวิตช์ทั้งสอง รวมถึงการกำหนด VLAN บนพอร์ทสวิตช์ ดังแสดงในตารางที่ 6.1 และ 6.2 ตามลำดับ

ตารางที่ 6.1 ค่าพารามิเตอร์ในการกำหนด VLAN และพอร์ท Trunk บนสวิตช์เลเยอร์ 2

```
Catalyst3500XL#
interface FastEthernet0/1
 switchport access vlan 2
  spanning-tree portfast
!
interface FastEthernet0/2
  switchport access vlan 3
  spanning-tree portfast
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk


interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

ตารางที่ 6.2 ค่าพารามิเตอร์ในการกำหนดพอร์ท Trunk บนสวิตช์เลเยอร์ 3

Catalyst6509_1#	Catalyst6509_2#
set trunk 4/1 on dot1q 1-1005,1025-4094	set trunk 4/1 on dot1q 1-1005,1025-4094
set trunk 4/2 on dot1q 1-1005,1025-4094	set trunk 4/2 on dot1q 1-1005,1025-4094
set trunk 4/3 on dot1q 1-1005,1025-4094	set trunk 4/3 on dot1q 1-1005,1025-4094
set trunk 4/4 on dot1q 1-1005,1025-4094	set trunk 4/4 on dot1q 1-1005,1025-4094
set trunk 4/5 on dot1q 1-1005,1025-4094	set trunk 4/5 on dot1q 1-1005,1025-4094
set trunk 4/6 on dot1q 1-1005,1025-4094	set trunk 4/6 on dot1q 1-1005,1025-4094
set trunk 4/7 on dot1q 1-1005,1025-4094	set trunk 4/7 on dot1q 1-1005,1025-4094
set trunk 4/8 on dot1q 1-1005,1025-4094	set trunk 4/8 on dot1q 1-1005,1025-4094
set trunk 4/9 on dot1q 1-1005,1025-4094	set trunk 4/9 on dot1q 1-1005,1025-4094
set trunk 4/10 on dot1q 1-1005,1025-4094	set trunk 4/10 on dot1q 1-1005,1025-4094
set trunk 4/11 on dot1q 1-1005,1025-4094	set trunk 4/11 on dot1q 1-1005,1025-4094

ในส่วนของการกำหนดพอร์ท root สำหรับโพรโตคอล Spanning-tree และค่าพารามิเตอร์ของสวิตช์ทั้งเลเยอร์ 2 และ 3 ทั้งหมดโดยอ้างอิงจากแบบจำลอง ได้ถูกแสดงในตารางที่ 6.3 และ 6.4

ตารางที่ 6.3 แสดงการกำหนดค่า priority เพื่อกำหนดพอร์ท root ให้กับอุปกรณ์

Catalyst6509_1#	Catalyst6509_2#
set spantree priority 8192 1	set spantree priority 16384 1
set spantree priority 8192 2	set spantree priority 16384 2
set spantree priority 8192 3	set spantree priority 16384 3
set spantree priority 8192 4	set spantree priority 16384 4

ตารางที่ 6.4 แสดงค่าพารามิเตอร์ ของ VLAN บนสวิตช์เลเยอร์ 3

Catalyst6509#
vtp
set vtp domain SCNB
set vtp pruning enable

ตารางที่ 6.4 (ต่อ)

set vlan 1 name default type ethernet mtu 1500 said 100001 state active
set vlan 2 name CB type ethernet mtu 1500 said 100002 state active
set vlan 3 name Existing ethernet mtu 1500 said 100003 state active

2. ค่าพารามิเตอร์ในส่วนของการทำการระบบสำรอง (Redundant backup)

ในส่วนนี้เป็นกำหนดค่าพารามิเตอร์บน MSFC-1 และ MSFC-2 เพื่อสนับสนุนการทำงาน Redundant Backup โดยการระบุค่า priority ต่างกัน ซึ่งจะเป็นตัวกำหนดการทำงานเมื่ออุปกรณ์ตัวใดตัวหนึ่งไม่สามารถใช้งานได้หรือเกิดขัดข้องขึ้น ซึ่งเราใช้ HSRP (Hot Standby Router-Protocol) ในการติดตามและจัดลำดับความสำคัญของอินเตอร์เฟส เพื่อให้ระบบทำงานต่อไปได้ ซึ่งเป็นประโยชน์ต่อเครือข่ายเป็นอย่างมาก

ตารางที่ 6.5 แสดงค่าพารามิเตอร์ ที่ใช้ในการทำระบบสำรอง

MSFC-1#	MSFC-2#
interface Vlan1	interface Vlan1
description FOR DEVICES MANAGEMENT	description VLAN1-Network Management
ip address 11.10.1.2 255.255.0.0	ip address 11.10.1.4 255.255.0.0
ip access-group 160 in	ip access-group 160 in
no ip redirects	no ip redirects
ip ospf priority 90	ip ospf cost 10000
standby 1 ip 11.10.1.254	ip ospf priority 90
standby 1 priority 120	standby 1 ip 11.10.1.254
standby 1 preempt	standby 1 priority 150
!	standby 1 preempt
	!
interface Vlan2	interface Vlan2
description VLAN2-Consumer Banking	description VLAN2-Consumer Banking

ตารางที่ 6.5 (ต่อ)

ip address 172.16.111.253 255.255.248.0	ip address 172.16.111.251 255.255.248.0
no ip redirects	no ip redirects
ip ospf priority 89	ip route-cache flow
ipx network 13A	ip ospf priority 89
standby 2 ip 172.16.104.1	ipx network 13A
standby 2 priority 120	standby 2 ip 172.16.104.1
standby 2 preempt	standby 2 priority 150
bridge-group 1	standby 2 preempt
	bridge-group 1
	!
interface Vlan3	interface Vlan3
description VLAN3-Existing ATM	description VLAN3-Existing ATM
ip address 172.16.99.253 255.255.252.0	ip address 172.16.99.251 255.255.252.0
no ip redirects	no ip redirects
ip ospf priority 90	ip route-cache flow
ipx network 1023204	ip ospf priority 90
standby 3 ip 172.16.96.1	ipx network 3A
standby 3 priority 105	standby 3 ip 172.16.96.1
standby 3 preempt	standby 3 priority 150
standby 33 ip 172.16.96.2	standby 3 preempt
standby 33 priority 120	standby 33 ip 172.16.96.2
standby 33 preempt	standby 33 priority 150
bridge-group 1	standby 33 preempt
	bridge-group 1

6.3 ผลที่ได้จากการทดลอง

จากรูปที่ 6.1 และค่าพารามิเตอร์ที่ใช้ในแบบจำลองเพื่อทำการเชื่อมโยงครือข่าย สามารถแสดงให้เห็นถึงสถานะการเชื่อมต่อของเครือข่ายดังด้านล่าง

```
Catalyst3500XL#sh spanning-tree
Spanning tree 1 is executing the IEEE compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 0004.c105.0f00
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 8192, address 0009.11c8.0800
  Root port is 40, cost of root path is 11
  Topology change flag not set, detected flag not set, changes 124
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0

Interface Gi0/1 (port 40) in Spanning tree 1 is FORWARDING
   Port path cost 4, Port priority 128
   Designated root has priority 8192, address 0009.11c8.0800
   Designated bridge has priority 16384, address 00d0.043a.f400
   Designated port is 198, path cost 7
   Timers: message age 4, forward delay 0, hold 0
   BPDU: sent 29, received 10368544

Interface Gi0/2 (port 48) in Spanning tree 1 is BLOCKING
   Port path cost 4, Port priority 128
   Designated root has priority 8192, address 0009.11c8.0800
   Designated bridge has priority 32768, address 0004.c1d4.ce40
   Designated port is 75, path cost 8
   Timers: message age 12, forward delay 0, hold 0
    BPDU: sent 1, received 10368218
```

รูปที่ 6.2 แสดงสถานะอินเทอร์เฟสกิกะบิทอีเทอร์เน็ทของสวิตซ์ เลเยอร์ 2 (Forwarding / Blocking)

```
Catalyst3500XL#sh vtp status
VTP Version                     : 2
Configuration Revision          : 130
Maximum VLANs supported locally : 254
Number of existing VLANs        : 33
Mode                            : Client
VTP Domain Name                 : SCNB
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Enabled

Catalyst3500XL# sh vlan
VLAN Name                       Status    Ports
1    default                    active
2    CB                         active    Fa0/1,
                                          Fa0/2
3    Existing-Network           active    Fa0/3
```

รูปที่ 6.3 แสดงสถานะของ VTP กับ VLAN ของสวิตช์เลเยอร์ 2

```
MSFC-1#sh standby brief
Interface   Grp  Prio P State    Active addr     Standby addr    Group addr
Vl1           1   120 P Standby  11.10.1.4       local           11.10.1.254
Vl2           2   120 P Standby  172.16.111.251  local           172.16.104.1
Vl3           3   105 P Standby  172.16.99.251   local           172.16.96.1
Vl3           3   120 P Standby  172.16.99.251   local           172.16.96.2
```

รูปที่ 6.4 แสดงสถานะการทำงานของ MSFC ซึ่งอยู่ในสถานะ Standby

```
MFSC-2#sh standby brief
Interface   Grp  Prio P State    Active addr     Standby addr    Group addr
Vl1           1   150 P Active   local           11.10.1.2       11.10.1.254
Vl2           2   150 P Active   local           172.16.111.253  172.16.104.1
Vl3           3   150 P Active   local           172.16.99.253   172.16.96.1
Vl3          33   150 P Active   local           172.16.99.253   172.16.96.2
```

รูปที่ 6.5 แสดงสถานะการทำงานของ MSFC ซึ่งอยู่ในสถานะ Active

6.3.1 การทดสอบประสิทธิภาพของเครือข่าย

การทดสอบประสิทธิภาพของเครือข่ายโดยได้ใช้ software Chariot ในการทดสอบ เราได้ทำการป้อนข้อมูลซึ่งมีขนาดใหญ่ 30 MB และ 40 MB ตามลำดับและได้แบ่งการทดสอบออกเป็น 4 ส่วน ผลที่ได้มาดังรูปที่ 6.10-6.19

การทดลองที่ 1: โดยการทดสอบส่งข้อมูลขนาด 30 MB ระหว่าง workstation 2 เครื่อง ซึ่งอยู่ต่าง VLAN กันผ่านแบบจำลองกิกะบิทอีเทอร์เน็ท

ตารางที่ 6.6 การตั้งค่าของโปรแกรม Chariot

Console version	5.0
Console build level	3547
Console product type	Chariot
Filename	untitled1.tst
Run start time	22 สิงหาคม 2547, 18:48:10
Run end time	22 สิงหาคม 2547, 18:53:11
Elapsed time	00:05:01
How the test ended	Ran to completion
Number of pairs	1

ตารางที่ 6.7 แสดงการทำงานของโปรแกรม

End type	Run until any pair ends
Reporting type	Real-time
Automatically poll endpoints	Yes
Polling interval (minutes)	1
Stop run upon initialization failure	Yes
Connect timeout during test (minutes)	0

Stop test after this many running pairs fail	1
Collect endpoint CPU utilization	No
Validate data upon receipt	No
Use a new seed for random variables on every run	Yes

ตารางที่ 6.8 เมื่อทำการป้อนค่า IP Address ของ workstation ด้านต้นทาง

Group/ Pair	Console Knows Endpoint 1	Console Protocol	Console Service Quality	Pair Comment
All Pairs				
Pair 1	172.21.117.246	TCP	n/a	30MV10_V7

ตารางที่ 6.9 เมื่อทำการป้อน IP Address ของ workstation ด้านปลายทาง

Group/ Pair	Endpoint 1 Knows Endpoint 2 (Setup)	Endpoint 2 Setup Protocol
All Pairs		
Pair 1	172.16.101.150	TCP

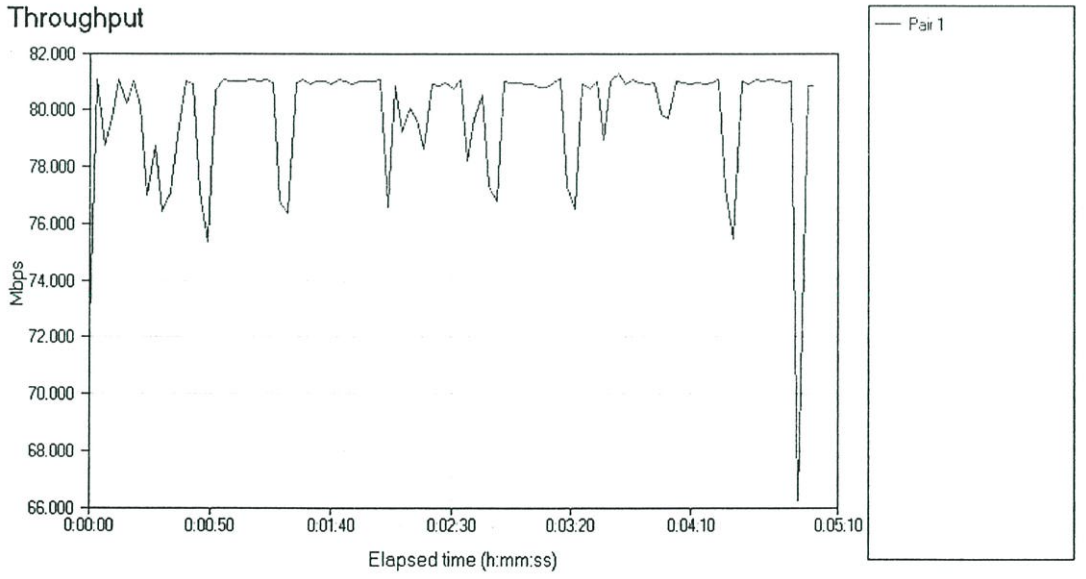
ตารางที่ 6.10 แสดงผลของการป้อนค่า IP Address ที่ Endpoint 1 และ Endpoint 2

Group/ Pair	Endpoint 1	Endpoint 2	Network Protocol	Service Quality	Script Name
All Pairs					
Pair 1	172.16.117.246	172.16.101.150	TCP		Throughput.scr

ผลที่ได้จากการทดสอบส่งข้อมูลขนาด 30MB จาก workstation A ไปยัง workstation B ซึ่งอยู่ต่าง VLAN กัน ซึ่งได้ทั้งค่า Throughput, Transaction, และ Response time ของการส่งข้อมูลดังกล่าว ได้แสดงดังตารางที่ 6.15 ถึงด้านล่าง

ตารางที่ 6.11 แสดงผลของ Throughput ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 30 MB

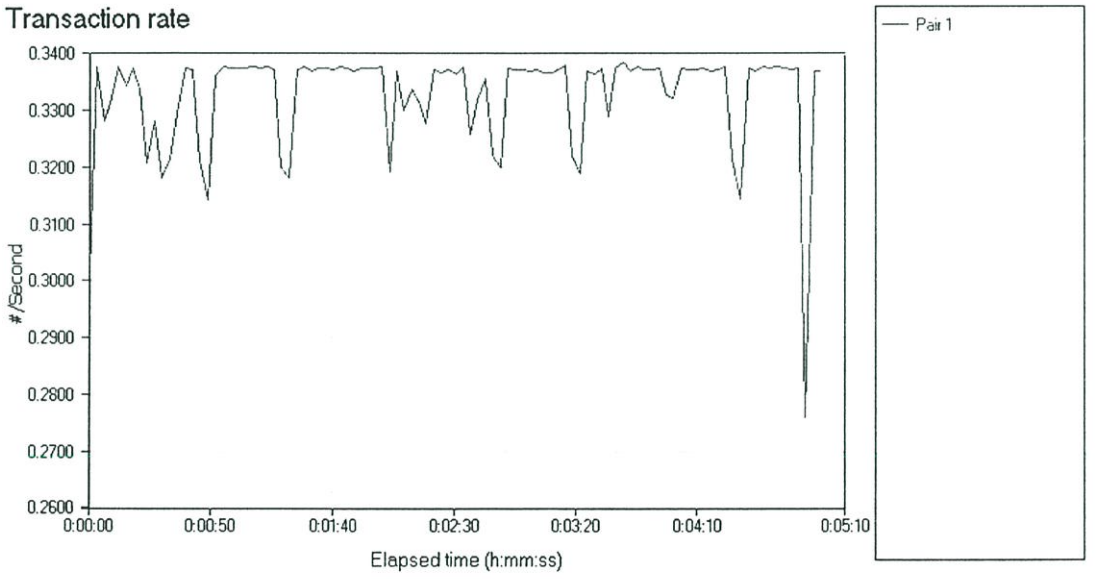
Group/ Pair	Average (Mbps)	Minimum (Mbps)	Maximum (Mbps)	Throughput 95% Confidence Interval	Measured Time (secs)	Relative Precision
All Pairs	79.807	66.262	81.273			
Pair 1	79.822	66.262	81.273	0.486	300.668	0.608
Totals:	79.807	66.262	81.273			



รูปที่ 6.6 แสดงกราฟค่า Throughput ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 30 MB

ตารางที่ 6.12 แสดงผล Transaction Rate ที่ได้จากการ รันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 30 MB

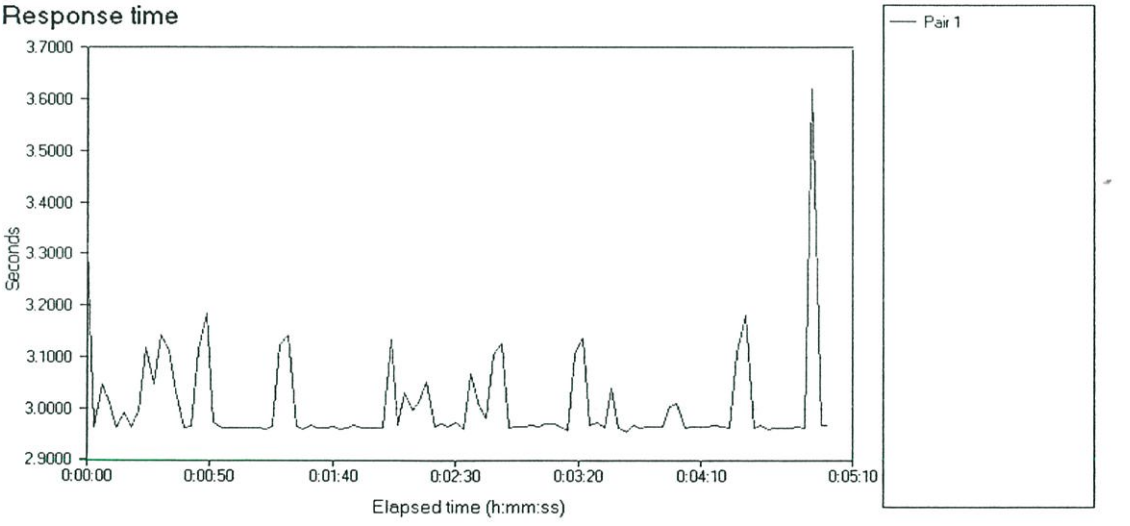
Group/ Pair	Transaction Rate Average	Transaction Rate Minimum	Transaction Rate Maximum	Transaction Rate 95% Confidence Interval	Measured Time (secs)	Relative Precision
All Pairs	0.333	0.276	0.339			
Pair 1	0.333	0.276	0.339	0.002	300.668	0.608
Totals:	0.333	0.276	0.339			



รูปที่ 6.7 แสดงกราฟค่า Transaction rate ที่ได้จากการ รันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 30 Mbps

ตารางที่ 6.13 แสดงผลค่า Response Time ที่ได้จากการ รันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 30 Mbps

Group/ Pair	Response Time Average	Response Time Minimum	Response Time Maximum	Response Time 95% Confidence Interval	Measured Time (secs)	Relative Precision
All Pairs	3.007	2.953	3.622			
Pair 1	3.007	2.953	3.622	0.018	300.668	0.608
Totals:	3.007	2.953	3.622			



รูปที่ 6.8 แสดงกราฟค่า Response time ที่ได้จากการ รันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 30 MB

หลังจาก program Chariot ทำการทดสอบส่งข้อมูลขนาด 30 MB จนได้ผลดังแสดง นอกจากนั้น ผลของการ รันโปรแกรม ดังกล่าวยังสามารถแสดงเวอร์ชั่นของ Endpoint ด้านปลายทาง และสรุปผลที่ได้จาก Raw Data Totals ที่แสดงบน Endpoint

ตารางที่ 6.14 แสดงค่า Endpoint Configuration ที่ได้จากการรันโปรแกรม Chariot

Group/ Pair	E1 Operating System	E1 Version	E1 Build Level	E1 Product Type	E2 Operating System	E2 Version	E2 Build Level	E2 Product Type
All Pairs								
Pair 1	Windows 2000	5.0	3186	Retail	Windows NT	5.0	3186	Retail

ตารางที่ 6.15 แสดงผลที่ได้จาก Raw Data Totals ที่แสดงบน Endpoint

Group/ Pair	Number of Timing Records	Transaction Count	Bytes Sent by E1	Bytes Received by E1	Measured Time (secs)	Relative Precision
All Pairs	100	100	3,000,000,000	100		
Pair 1	100	100	3,000,000,000	100	300.668	0.608
Totals:	100	100	3,000,000,000	100		

การทดลองที่ 2: โดยการทดสอบใส่ข้อมูลขนาด 40 MB เพื่อส่งข้อมูลให้ workstation ซึ่งอยู่คนละ VLAN กัน

ตารางที่ 6.16 การตั้งค่าของโปรแกรม Chariot

Console version	5.0
Console build level	3547
Console product type	Chariot
Filename	untitled1.tst
Run start time	22 สิงหาคม 2547, 18:55:53

Run end time	22 สิงหาคม 2547, 19:02:35
Elapsed time	00:06:42
How the test ended	Ran to completion
Number of pairs	1

ตารางที่ 6.17 แสดงการทำงานของโปรแกรม

End type	Run until any pair ends
Reporting type	Real-time
Automatically poll endpoints	Yes
Polling interval (minutes)	1
Stop run upon initialization failure	Yes
Connect timeout during test (minutes)	0
Stop test after this many running pairs fail	1
Collect endpoint CPU utilization	No
Validate data upon receipt	No
Use a new seed for random variables on every run	Yes

ตารางที่ 6.18 เมื่อทำการป้อนค่า IP Address ของ workstation ด้านต้นทาง

Group/ Pair	Console Knows Endpoint 1	Console Protocol	Console Service Quality	Pair Comment
All Pairs				
Pair 1	172.21.117.246	TCP	n/a	40MV10_V7

ตารางที่ 6.19 เมื่อทำการทดสอบป้อน IP Address ของ Endpoint ด้านต้นทางและปลายทาง

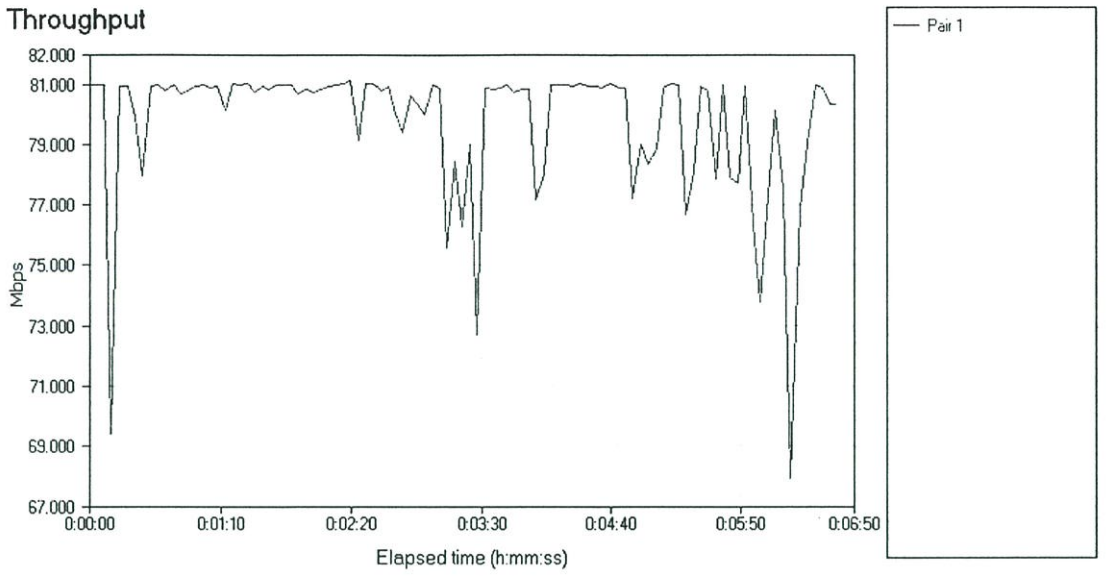
Group/ Pair	Endpoint 1 Knows Endpoint 2 (Setup)	Endpoint 2 Setup Protocol
All Pairs		
Pair 1	172.21.101.150	TCP

ตารางที่ 6.20 แสดงผลของการป้อนค่า IP Address ที่ Endpoint 1 และ Endpoint 2

Group/ Pair	Endpoint 1	Endpoint 2	Network Protocol	Service Quality	Script Name
All Pairs					
Pair 1	172.16.117.246	172.16.101.150	TCP		Throughput.scr

ตารางที่ 6.21 แสดงผลของ Throughput ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 40 MB

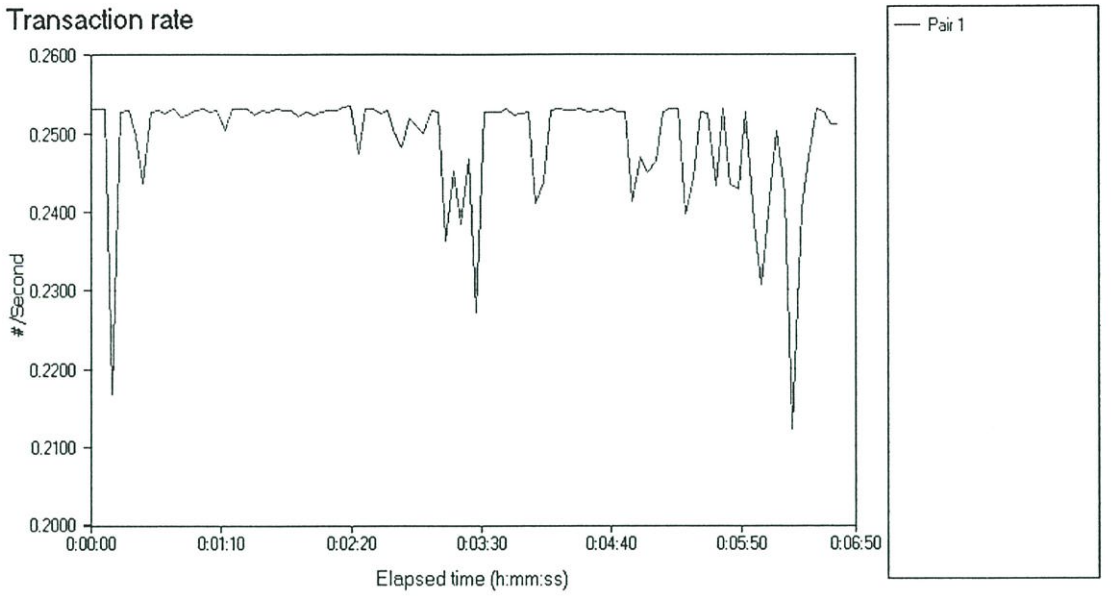
Group/ Pair	Average (Mbps)	Minimum (Mbps)	Maximum (Mbps)	Throughput 95% Confidence Interval	Measured Time (secs)	Relative Precision
All Pairs	79.664	67.926	81.136			
Pair 1	79.676	67.926	81.136	0.505	401.628	0.634
Totals:	79.664	67.926	81.136			



รูปที่ 6.9 แสดงกราฟค่า Throughput ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 40 MB

ตารางที่ 6.22 แสดงผล Transaction Rate ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 40 MB

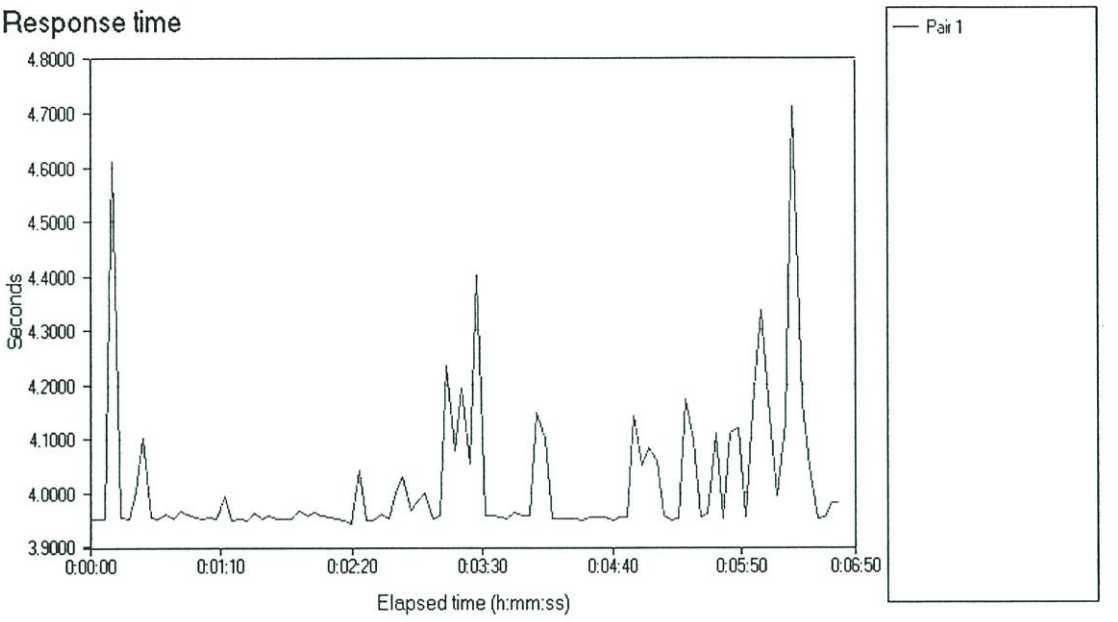
Group/ Pair	Transaction Rate Average	Transaction Rate Minimum	Transaction Rate Maximum	Transaction Rate 95% Confidence Interval	Measured Time (secs)	Relative Precision
All Pairs	0.249	0.212	0.254			
Pair 1	0.249	0.212	0.254	0.002	401.628	0.634
Totals:	0.249	0.212	0.254			



รูปที่ 6.10 กราฟแสดงค่า Transaction rate ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 40 MB

ตารางที่ 6.23 แสดงผลค่า Response Time ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 40 MB

Group/ Pair	Response Time Average	Response Time Minimum	Response Time Maximum	Response Time 95% Confidence Interval	Measured Time (secs)	Relative Precision
All Pairs	4.016	3.944	4.711			
Pair 1	4.016	3.944	4.711	0.025	401.628	0.634
Totals:	4.016	3.944	4.711			



รูปที่ 6.11 แสดงกราฟค่า Response time ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 40 MB

ตารางที่ 6.24 แสดงค่า Endpoint Configuration ที่ได้จากการรันโปรแกรม Chariot

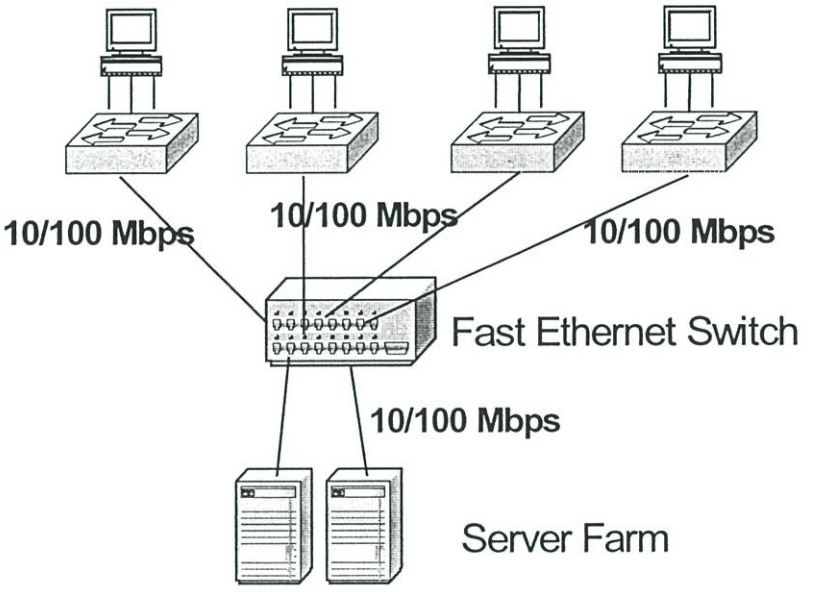
Group/ Pair	E1 Operating System	E1 Version	E1 Build Level	E1 Product Type	E2 Operating System	E2 Version	E2 Build Level	E2 Product Type
All Pairs								
Pair 1	Windows 2000	5.0	3186	Retail	Windows NT	5.0	3186	Retail

ตารางที่ 6.25 แสดงผลที่ได้จาก Raw Data Totals ที่แสดงบน Endpoint

Group/ Pair	Number of Timing Records	Transaction Count	Bytes Sent by E1	Bytes Received by E1	Measured Time (secs)	Relative Precision
All Pairs	100	100	4,000,000,000	100		
Pair 1	100	100	4,000,000,000	100	401.628	0.634
Totals:	100	100	4,000,000,000	100		

6.3.2 ทดสอบประสิทธิภาพของเครือข่ายแบบเดิม

ได้ทำการทดสอบประสิทธิภาพของเครือข่ายแบบเดิม โดยได้ใช้โปรแกรม Chariot ในการทดสอบ เราได้ทำการส่งข้อมูลซึ่งมีขนาดใหญ่ 30 MB และ 40 MB ตามลำดับ ผลที่ได้มาดังรูปที่ 6.2 และผลจากโปรแกรม Chariot ดังที่แสดงข้างล่าง



รูปที่ 6.12 แสดงเครือข่ายก่อนเปลี่ยนมาใช้อุปกรณ์กิกะบิทอีเทอร์เน็ท

การทดลองที่ 3 : ทำการส่งข้อมูลขนาด 30 MB ส่งผ่าน VLAN ในเครือข่ายแบบดั้งเดิม แสดงดังรูปด้านล่าง

ตารางที่ 6.26 การตั้งค่าของโปรแกรม Chariot

Console version	5.0
Console build level	3547
Console product type	Chariot
Filename	untitled1.tst

Run start time	24 สิงหาคม 2547, 22:42:34
Run end time	24 สิงหาคม 2547, 23:18:14
Elapsed time	00:35:40
How the test ended	Ran to completion
Number of pairs	1

ตารางที่ 6.27 แสดงการทำงานของโปรแกรม

End type	Run until any pair ends
Reporting type	Real-time
Automatically poll endpoints	Yes
Polling interval (minutes)	1
Stop run upon initialization failure	Yes
Connect timeout during test (minutes)	0
Stop test after this many running pairs fail	1
Collect endpoint CPU utilization	No
Validate data upon receipt	No
Use a new seed for random variables on every run	Yes

ตารางที่ 6.28 เมื่อทำการป้อนค่า IP Address ของ Endpoint ด้านต้นทาง

Group/ Pair	Console Knows Endpoint 1	Console Protocol	Console Service Quality	Pair Comment
All Pairs				
Pair 1	22.1.0.1	TCP	n/a	30M

ตารางที่ 6.29 เมื่อทำการป้อน IP Address ของ workstation ด้านปลายทาง

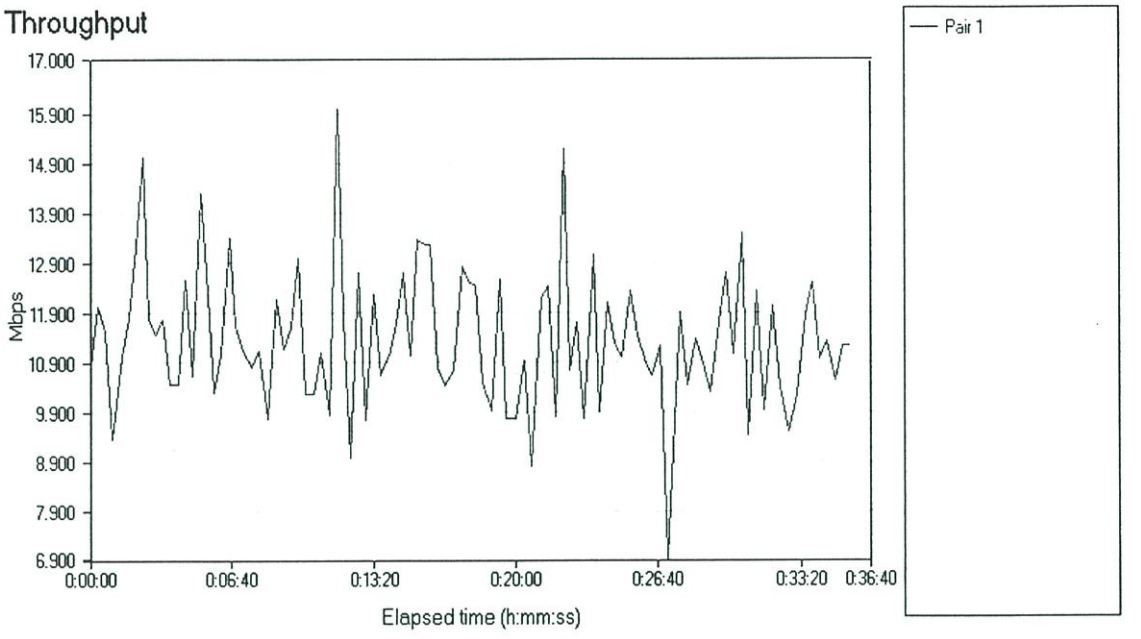
Group/ Pair	Endpoint 1 Knows Endpoint 2 (Setup)	Endpoint 2 Setup Protocol
All Pairs		
Pair 1	11.1.0.1	TCP

ตารางที่ 6.30 แสดงผลของการป้อนค่า IP Address ที่ Endpoint 1 และ Endpoint 2

Group/ Pair	Endpoint 1	Endpoint 2	Network Protocol	Service Quality	Script Name
All Pairs					
Pair 1	22.1.0.1	11.1.0.1	TCP		Throughput.scr

ตารางที่ 6.31 แสดงผลของ Throughput ที่ได้จากการ รันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 30 MB ในเครือข่ายแบบดั้งเดิม

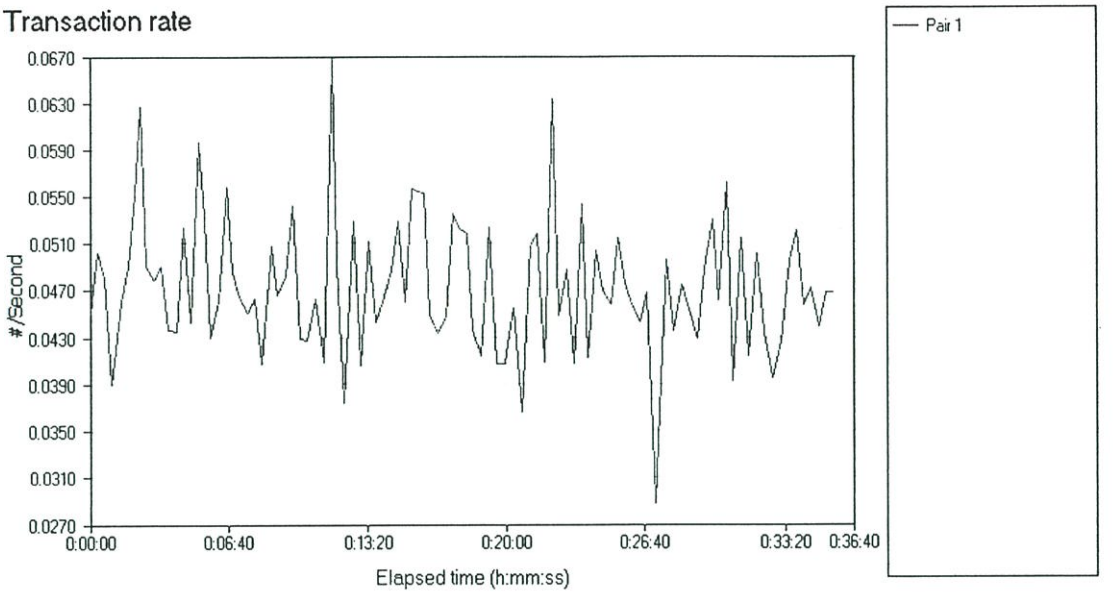
Group/ Pair	Average (Mbps)	Minimum (Mbps)	Maximum (Mbps)	Throughput 95% Confidence Interval	Measured Time (secs)	Relative Precision
All Pairs	11.215	6.913	16.017			
Pair 1	11.215	6.913	16.017	0.285	2,139.918	2.538
Totals:	11.215	6.913	16.017			



รูปที่ 6.13 แสดงกราฟค่า Throughput ที่ได้จากการ รันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 30 MB

ตารางที่ 6.32 แสดงผล Transaction Rate ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 30 MB ในเครือข่ายแบบดั้งเดิม

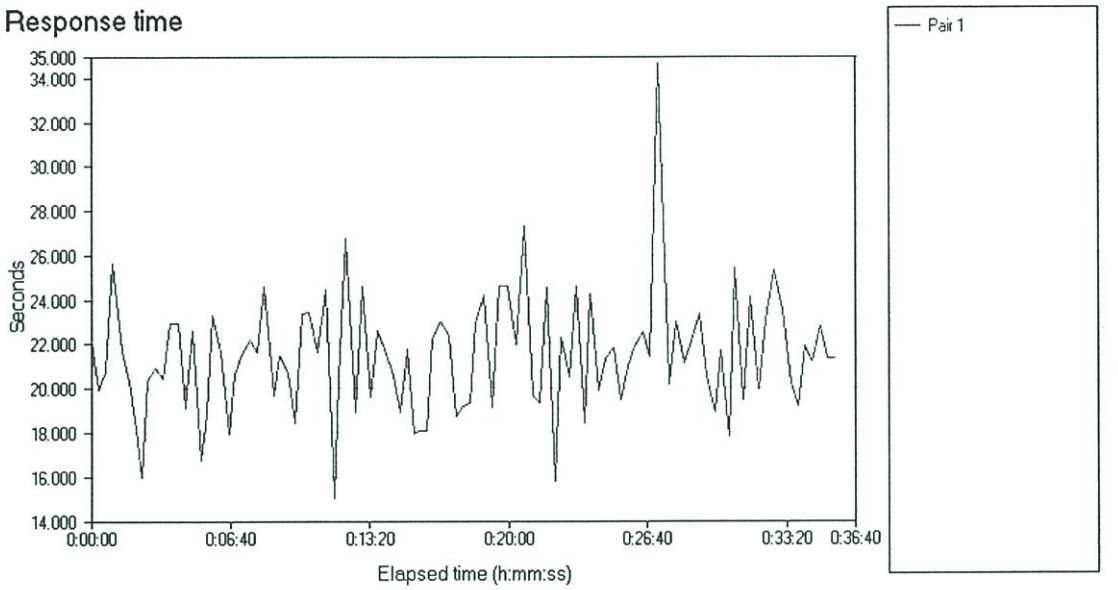
Group/ Pair	Transaction Rate Average	Transaction Rate Minimum	Transaction Rate Maximum	Transaction Rate 95% Confidence Interval	Measured Time (secs)	Relative Precision
All Pairs	0.047	0.029	0.067			
Pair 1	0.047	0.029	0.067	0.001	2,139.918	2.538
Totals:	0.047	0.029	0.067			



รูปที่ 6.14 แสดงกราฟค่า Transaction rate ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 30 MB ในเครือข่ายแบบดั้งเดิม

ตารางที่ 6.33 แสดงผลค่า Response Time ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 30 MB บนเครือข่ายแบบดั้งเดิม

Group/ Pair	Response Time Average	Response Time Minimum	Response Time Maximum	Response Time 95% Confidence Interval	Measured Time (secs)	Relative Precision
All Pairs	21.399	14.984	34.719			
Pair 1	21.399	14.984	34.719	0.543	2,139.918	2.538
Totals:	21.399	14.984	34.719			



รูปที่ 6.15 แสดงกราฟค่า Response time ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 30 MB บนเครือข่ายแบบดั้งเดิม

ตารางที่ 6.34 แสดงค่า Endpoint Configuration ที่ได้จากการรันโปรแกรม Chariot

Group/ Pair	E1 Operating System	E1 Version	E1 Build Level	E1 Product Type	E2 Operating System	E2 Version	E2 Build Level	E2 Product Type
All Pairs								
Pair 1	Windows 2000	5.0	3186	Retail	Windows XP (32-bit)	5.0	3186	Retail (Web-Based)

ตารางที่ 6.35 แสดงผลที่ได้จาก Raw Data Totals ที่แสดงบน Endpoint

Group/ Pair	Number of Timing Records	Transaction Count	Bytes Sent by E1	Bytes Received by E1	Measured Time (secs)	Relative Precision
All Pairs	100	100	3,000,000,000	100		
Pair 1	100	100	3,000,000,000	100	2,139.918	2.538
Totals:	100	100	3,000,000,000	100		

การทดลองที่ 4: ทำการส่งข้อมูลขนาด 40 MB ส่งผ่าน VLAN ในเครือข่ายแบบดั้งเดิม

ตารางที่ 6.36 การตั้งค่าของโปรแกรม Chariot

Console version	5.0
Console build level	3547
Console product type	Chariot
Filename	untitled1.tst
Run start time	25 สิงหาคม 2547, 19:57:41
Run end time	25 สิงหาคม 2547, 21:17:10
Elapsed time	01:19:29
How the test ended	Ran to completion
Number of pairs	1

ตารางที่ 6.37 แสดงการทำงานของโปรแกรม Chariot

End type	Run until any pair ends
Reporting type	Real-time
Automatically poll endpoints	Yes
Polling interval (minutes)	1
Stop run upon initialization failure	Yes
Connect timeout during test (minutes)	0
Stop test after this many running pairs fail	1
Collect endpoint CPU utilization	No
Validate data upon receipt	No
Use a new seed for random variables on every run	Yes

ตารางที่ 6.38 เมื่อทำการป้อนค่า IP Address ของ Endpoint ด้านต้นทาง

Group/ Pair	Console Knows Endpoint 1	Console Protocol	Console Service Quality	Pair Comment
All Pairs				
Pair 1	22.1.0.1	TCP	n/a	40MV3_V2

ตารางที่ 6.39 เมื่อทำการป้อน IP Address ของ workstation ด้านปลายทาง

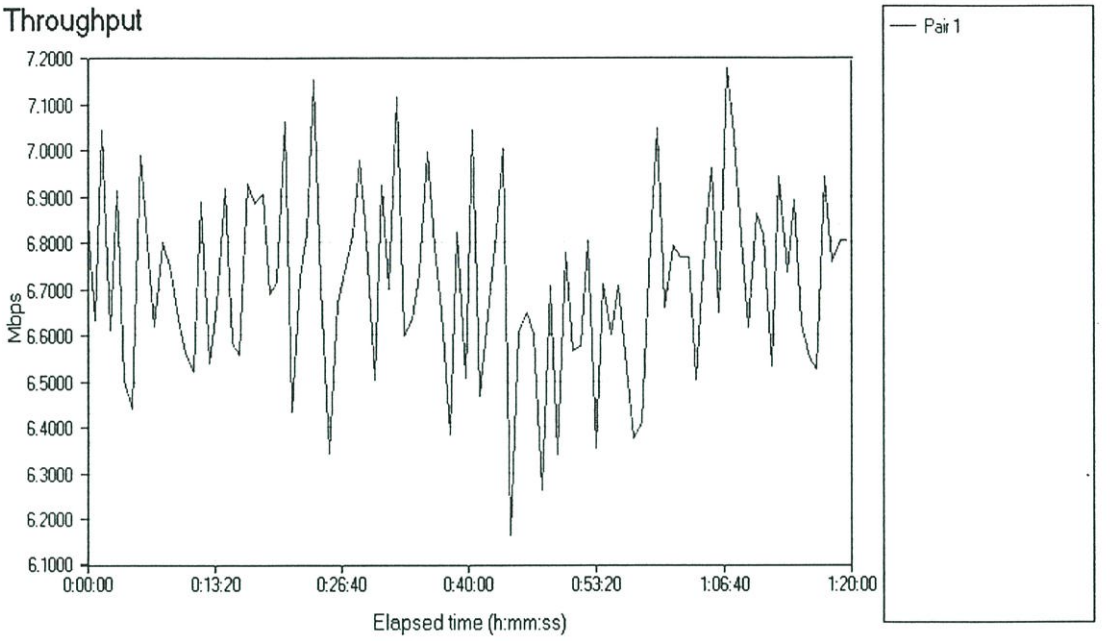
Group/ Pair	Endpoint 1 Knows Endpoint 2 (Setup)	Endpoint 2 Setup Protocol
All Pairs		
Pair 1	11.1.0.2	TCP

ตารางที่ 6.40 แสดงผลของการป้อนค่า IP Address ที่ Endpoint 1 และ Endpoint 2

Group/ Pair	Endpoint 1	Endpoint 2	Network Protocol	Service Quality	Script Name
All Pairs					
Pair 1	22.1.0.1	11.1.0.2	TCP		Throughput.scr

ตารางที่ 6.41 แสดงผลของ Throughput ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 40 MB ในเครือข่ายแบบดั้งเดิม

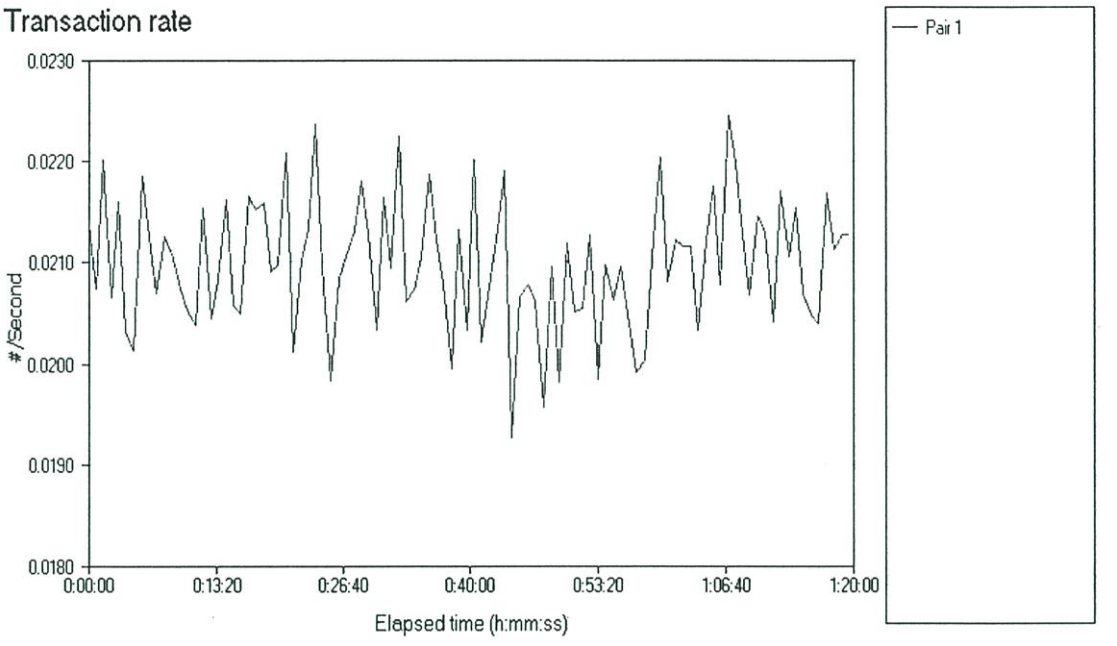
Group/ Pair	Average (Mbps)	Minimum (Mbps)	Maximum (Mbps)	Throughput 95% Confidence Interval	Measured Time (secs)	Relative Precision
All Pairs	6.710	6.163	7.180			
Pair 1	6.710	6.163	7.180	0.041	4,768.879	0.609
Totals:	6.710	6.163	7.180			



รูปที่ 6.16 แสดงกราฟค่า Throughput ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 40 MB

ตารางที่ 6.42 แสดงผล Transaction Rate ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 40 MB ในเครือข่ายแบบดั้งเดิม

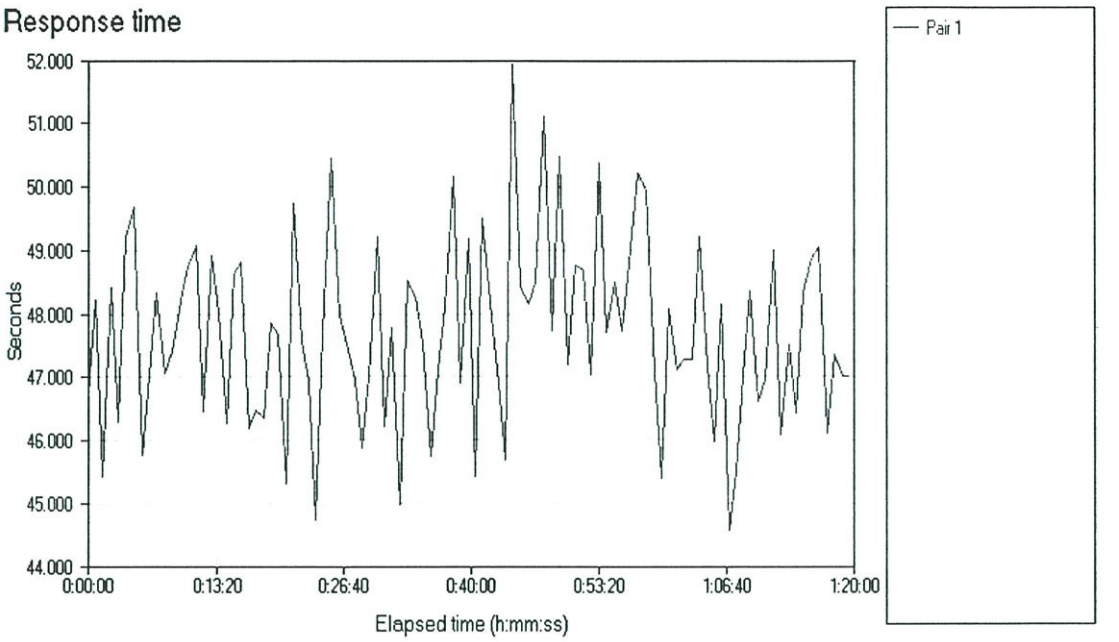
Group/ Pair	Transaction Rate Average	Transaction Rate Minimum	Transaction Rate Maximum	Transaction Rate 95% Confidence Interval	Measured Time (secs)	Relative Precision
All Pairs	0.021	0.019	0.022			
Pair 1	0.021	0.019	0.022	0.000	4,768.879	0.609
Totals:	0.021	0.019	0.022			



รูปที่ 6.17 แสดงกราฟค่า Transaction rate ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 40 Mbps ในเครือข่ายแบบดั้งเดิม

ตารางที่ 6.43 แสดงผลค่า Response Time ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 40 MB บนเครือข่ายแบบดั้งเดิม

Group/ Pair	Response Time Average	Response Time Minimum	Response Time Maximum	Response Time 95% Confidence Interval	Measured Time (secs)	Relative Precision
All Pairs	47.689	44.569	51.922			
Pair 1	47.689	44.569	51.922	0.290	4,768.879	0.609
Totals:	47.689	44.569	51.922			



รูปที่ 6.18 แสดงกราฟค่า Response time ที่ได้จากการรันโปรแกรม Chariot เมื่อทำการป้อนข้อมูลขนาด 40 MB บนเครือข่ายแบบดั้งเดิม

ตารางที่ 6.44 แสดงค่า Endpoint Configuration ที่ได้จากการรันโปรแกรม Chariot

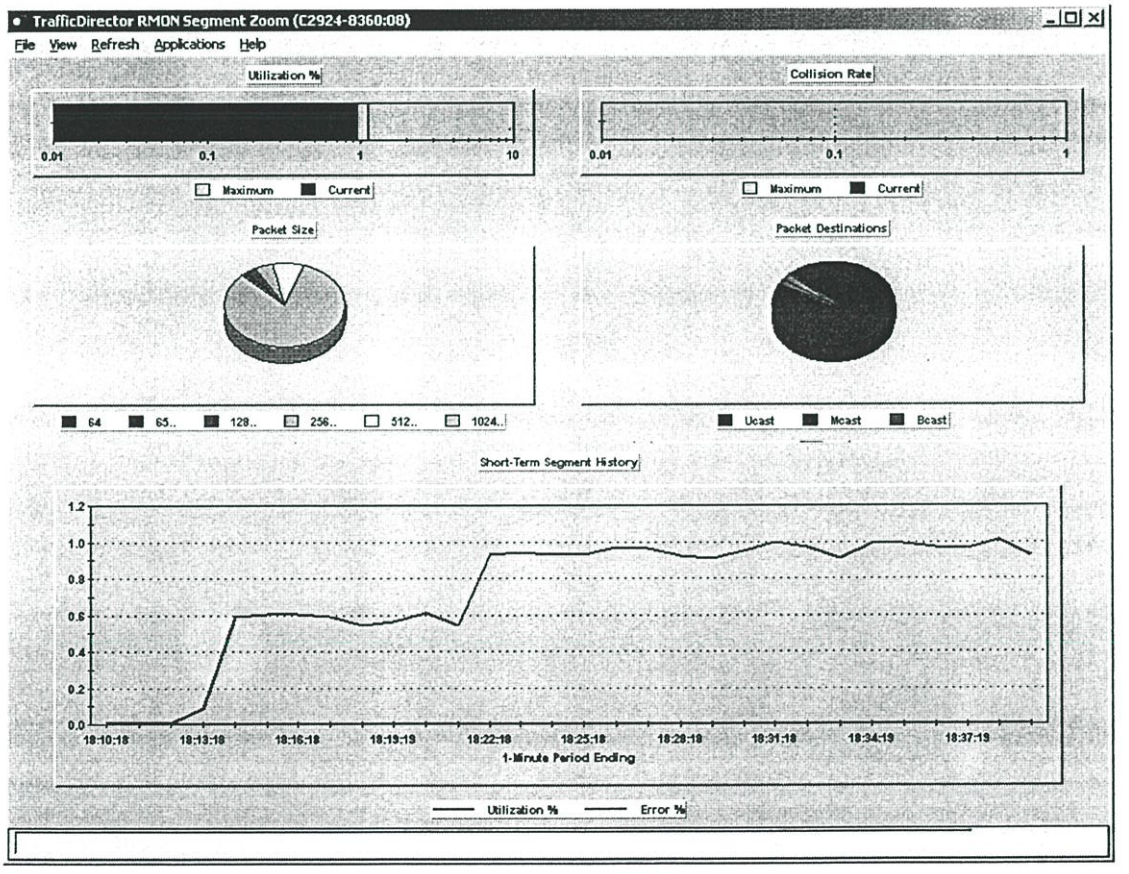
Group/ Pair	E1 Operating System	E1 Version	E1 Build Level	E1 Product Type	E2 Operating System	E2 Version	E2 Build Level	E2 Product Type
All Pairs								
Pair 1	Windows 2000	5.0	3186	Retail	Windows NT	5.0	3186	Retail

ตารางที่ 6.45 แสดงผลที่ได้จาก Raw Data Totals ที่แสดงบน Endpoint

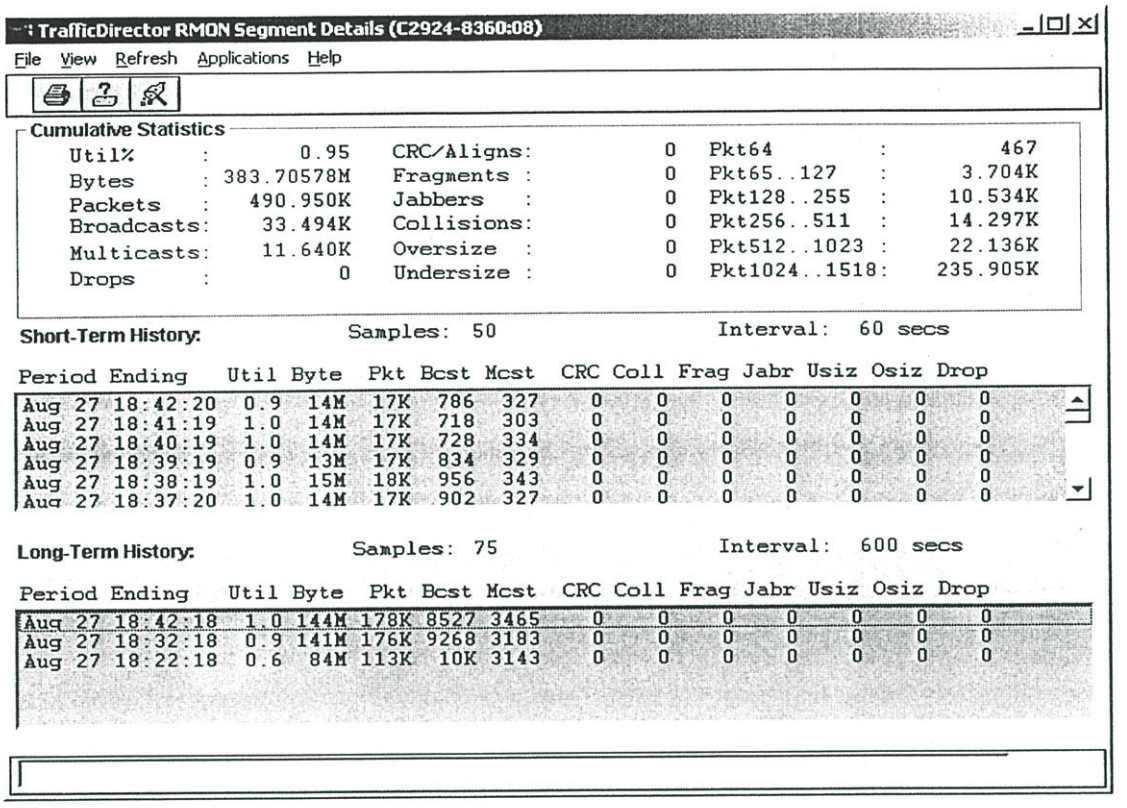
Group/ Pair	Number of Timing Records	Transaction Count	Bytes Sent by E1	Bytes Received by E1	Measured Time (secs)	Relative Precision
All Pairs	100	100	4,000,000,000	100		
Pair 1	100	100	4,000,000,000	100	4,768.879	0.609
Totals:	100	100	4,000,000,000	100		

จากการทดลองทั้ง 4 แบบ สามารถเปรียบเทียบให้เห็นถึงประสิทธิภาพของเครือข่ายกิกะบิทอีเทอร์เน็ทกับเครือข่ายแบบอีเทอร์เน็ทในการรับส่งข้อมูลที่มีปริมาณที่เท่ากัน ซึ่งจะเห็นได้ว่าค่าที่ได้ไม่ว่า response time, transactions rate หรือ throughput จะให้ผลลัพธ์ที่แตกต่างกันอย่างสิ้นเชิง โดยทำให้เรามั่นใจได้ว่าเครือข่ายกิกะบิทอีเทอร์เน็ทจะสามารถรองรับข้อมูลที่ต้องการแบนวิดธ์สูงๆ และค่า response time เป็นแบบ real time

จากรูปที่ 6.19 - 6.20 เป็นการเชื่อมต่ออุปกรณ์ Digital Video Recorder (DVR) เข้ากับเครือข่ายที่ออกแบบไว้ โดย DVR เป็นอุปกรณ์ไว้เชื่อมต่อกล้องโทรทัศน์วงจรปิดแบบอนาลอกเพื่อตรวจสอบความปลอดภัยภายในอาคาร และใช้เทคโนโลยี IP เพื่อทำการรีโมทดูภาพจากกล้องโทรทัศน์วงจรปิดจากระยะไกล แล้ววัดค่าแบนวิดธ์ที่ใช้งาน



รูปที่ 6.19 กราฟแสดง Utilization ของกล้องโทรทัศน์วงจรปิดผ่านเครือข่าย IP



รูปที่ 6.20 แสดงค่าปริมาณทราฟฟิกขณะใช้งานกล้องโทรทัศน์วงจรปิดผ่านเครือข่าย IP

รูปที่ 6.21 แสดงภาพที่ได้จากกล้องโทรทัศน์วงจรปิดผ่านเครือข่าย IP จากจอมอนิเตอร์ระยะไกล

6.3 สรุปผลการทดลอง

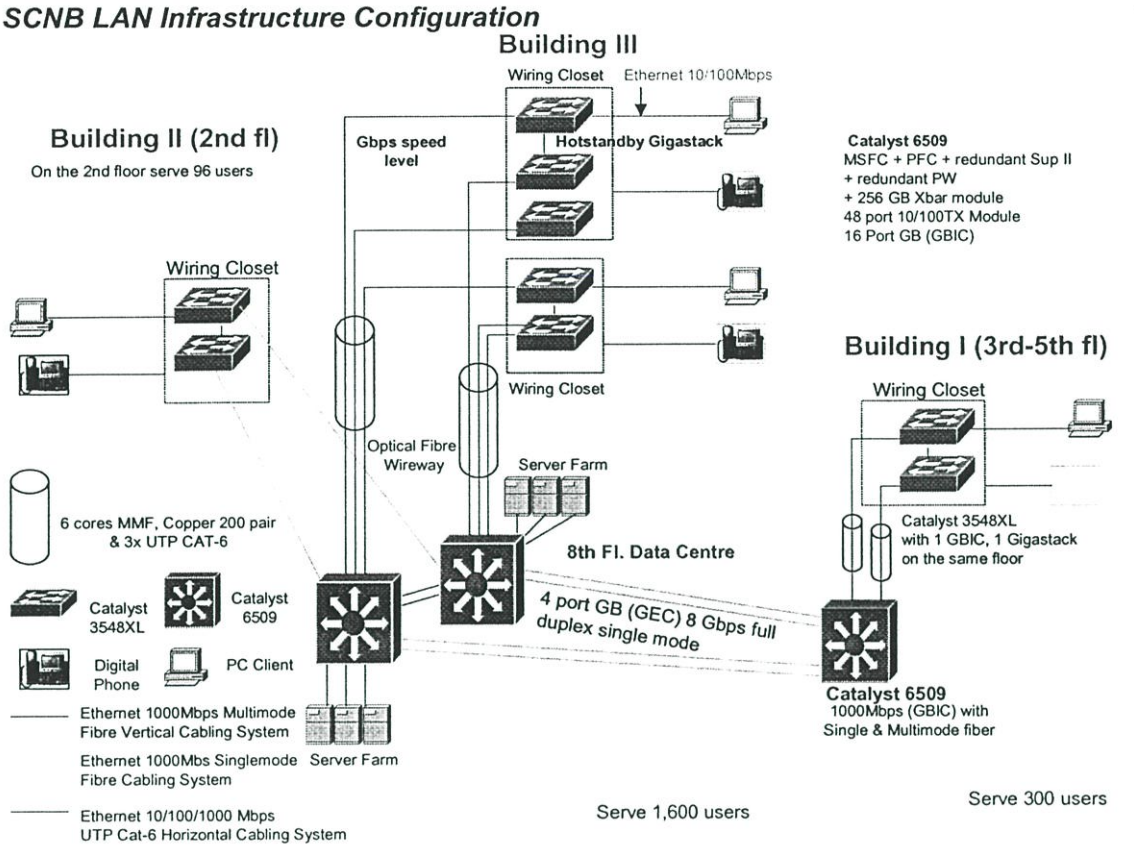
จากผลการทดลองดังกล่าวสามารถสรุปได้ว่าเครือข่ายกิกะบิทอีเทอร์เน็ทที่ได้ทำการออกแบบในวิทยานิพนธ์นี้ สามารถรองรับการใช้งานด้านการสื่อสารข้อมูลด้วยความเร็วสูง รวมถึงการใช้งานด้าน Multimedia ซึ่งมีแนวโน้มว่าจะมีการใช้งานอย่างแพร่หลายในอนาคตอันใกล้ ได้อย่างมีประสิทธิภาพ

บทที่ 7
การประยุกต์ใช้งาน

ในช่วงหลายปีที่ผ่านมา ผู้จัดทำวิทยานิพนธ์ได้มีโอกาสเห็นการพัฒนาเครือข่าย LAN ขององค์กรต่าง ๆ ซึ่งในบางองค์กรผู้ออกแบบเครือข่าย LAN พยายามจะใช้เทคโนโลยีที่ดีเยี่ยม โดยคิดว่าสิ่งที่ตนเองเลือกใช้นั้นเป็นสิ่งที่ดีที่สุด และบางแห่งไม่กังวลแม้เรื่องราคา โดยขาดแนวคิดในการออกแบบ เช่น จำนวนผู้ใช้งาน (Client) ค่าทรูพุท (Throughput) หรือแบ็กเพลน (Backplan) ของอุปกรณ์เครือข่าย ตลอดจนการทำบรอดคาส์ทโดเมน เพื่อหลีกเลี่ยงการบรอดคาส์ทของแพ็กเกต เป็นต้น ทำให้ผลลัพธ์หรือประสิทธิภาพของเครือข่ายที่ได้ไม่คุ้มค่ากับการลงทุนที่ควรจะได้ ดังนั้น การออกแบบจึงเป็นสิ่งสำคัญที่สุดที่จะช่วยพัฒนาเครือข่าย LAN ให้มีประสิทธิภาพได้มากที่สุด

ปัจจุบันเครือข่าย LAN ในองค์กรต่างๆ ไม่ว่าจะเป็นบริษัทเอกชน หรือสถานศึกษาส่วนใหญ่กว่า 80% จะนิยมใช้เครือข่ายอีเทอร์เน็ทเป็นหลัก ส่วนที่เหลือจะเป็นเครือข่าย FDDI และ ATM ด้วยความต้องการส่งผ่านข้อมูลที่เพิ่มขึ้นอย่างรวดเร็วตามขนาดและจำนวนของเครื่องคอมพิวเตอร์ที่ต่ออยู่บนเครือข่าย ตลอดจนการเติบโตของ Internet ที่มีอัตราการเติบโตอย่างรวดเร็วนั้น จึงทำให้เครือข่ายอีเทอร์เน็ทแบบดั้งเดิมที่มีความเร็วในการส่งผ่านข้อมูลอยู่ที่ 10/100 Mbps เริ่มจะไม่สามารถตอบสนองความต้องการของผู้ใช้ได้อย่างเต็มประสิทธิภาพ ดังนั้นกิกะบิทอีเทอร์เน็ท (IEEE802.3z) ซึ่งเป็นมาตรฐานล่าสุดของเทคโนโลยีเครือข่าย LAN ที่พัฒนามาจากเครือข่ายอีเทอร์เน็ทที่มีความเร็ว 10/100 Mbps ให้สามารถรับส่งข้อมูลได้ที่ระดับความเร็ว 1 Gbps ซึ่งกิกะบิทอีเทอร์เน็ท เป็นส่วนเพิ่มขยายจาก 10 Mbps และ 100 Mbps Ethernet (มาตรฐาน IEEE 802.3 และ IEEE802.3u ตามลำดับ) โดยยังคงรับรองการใช้งานร่วมกันกับมาตรฐานแบบเดิมเต็ม 100% ตลอดจนกิกะบิทอีเทอร์เน็ทยังสนับสนุนการทำงานในโหมด full-duplex และ Half-duplex โดยใช้สายสัญญาณได้ทั้งสายทองแดงและสายใยแก้วนำแสง

จากหลักการเชื่อมโยงดังกล่าวข้างต้นผู้จัดทำวิทยานิพนธ์จึงได้นำระบบทดสอบมาประยุกต์ใช้งานกับเครือข่ายที่มีอยู่เดิม เพื่อเพิ่มประสิทธิภาพในการทำงาน และรองรับปริมาณการส่งผ่านข้อมูลจำนวนมาก และแอพพลิเคชัน ดังรูปที่ 7.1



รูปที่ 7.1 รูปแบบการประยุกต์ใช้เครือข่ายกิกะบิทอีเทอร์เน็ทกับองค์กร

7.1 การประยุกต์ใช้เครือข่ายกิกะบิทอีเทอร์เน็ทกับเครือข่ายอีเทอร์เน็ท

จากรูปที่ 7.1 เป็นการนำอุปกรณ์กิกะบิทอีเทอร์เน็ทไปใช้ทดแทนอุปกรณ์ต่างๆ ที่มีอยู่แล้ว เพื่อเพิ่มความเร็วในการรับส่งข้อมูลโดยแบ่งได้เป็น 5 ขั้นตอนดังนี้

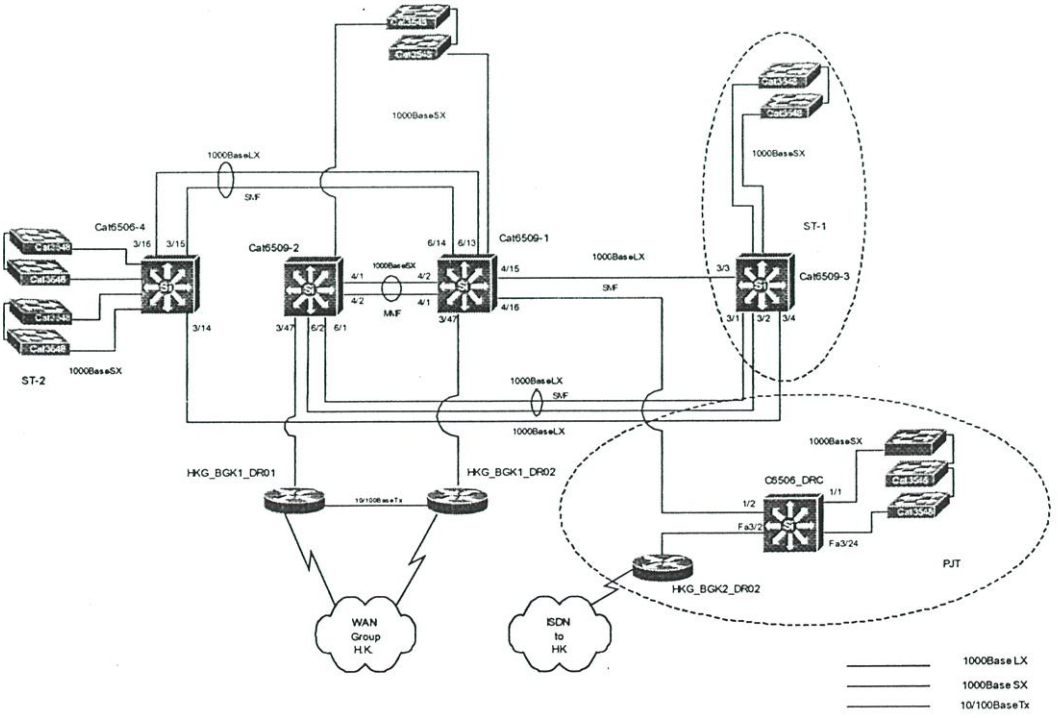
1. เพิ่มความเร็วของ Switch-to-Server Link วิธีการเพิ่มความเร็วที่ง่ายที่สุดก็คือการเพิ่มความเร็วในการรับส่งข้อมูลระหว่างตัวกิกะบิทสวิตช์กับเซิร์ฟเวอร์ประสิทธิภาพสูงซึ่งติดตั้ง Gigabit interface card เปลี่ยนแปลงจากอุปกรณ์เครือข่ายแบบ Ethernet/Fast Ethernet ไปเป็นกิกะบิทอีเทอร์เน็ท

2. การแทนที่เครือข่ายแกนหลักที่ใช้อีเทอร์เน็ตความเร็วสูงอยู่ก่อนแล้วในเครือข่ายขนาดเล็กจนถึงขนาดกลางที่ใช้สวิตช์อีเทอร์เน็ตความเร็วสูง เป็นอุปกรณ์เครือข่ายแกนหลัก (Backbone Switch) ก็อาจจะรองรับความต้องการในรับส่งข้อมูลที่มีปริมาณเพิ่มขึ้นอย่างรวดเร็วไม่ได้ การนำสวิตช์กิกะบิทอีเทอร์เน็ท มาทำหน้าที่เป็นสวิตช์แบ็คโบนแทน จะทำให้สามารถเพิ่มแบนด์วิดท์ได้อย่างเพียงพอต่อความต้องการทั้งในปัจจุบันและอนาคต

3. เพิ่มความเร็วของ Switch-to-Switch Link ในเครือข่ายที่มีขนาดใหญ่ขึ้น และมีสวิตช์กิกะบิทอีเทอร์เน็ท เมื่อความต้องการทำให้มีการส่งข้อมูลผ่านในเครือข่าย ซึ่งมีเซิร์ฟเวอร์ต่ออยู่ด้วยมีปริมาณที่สูงมากจนต้องเกิดความต้องการขยายเพิ่ม การนำกิกะบิทอีเทอร์เน็ทเข้ามาแทนที่ Ethernet/Fast Ethernet ก็จะสามารถเพิ่มประสิทธิภาพโดยรวมของระบบได้ โดยการเปลี่ยนแปลงจากอุปกรณ์เครือข่ายแบบ Ethernet/Fast Ethernet ไปเป็นกิกะบิทอีเทอร์เน็ท

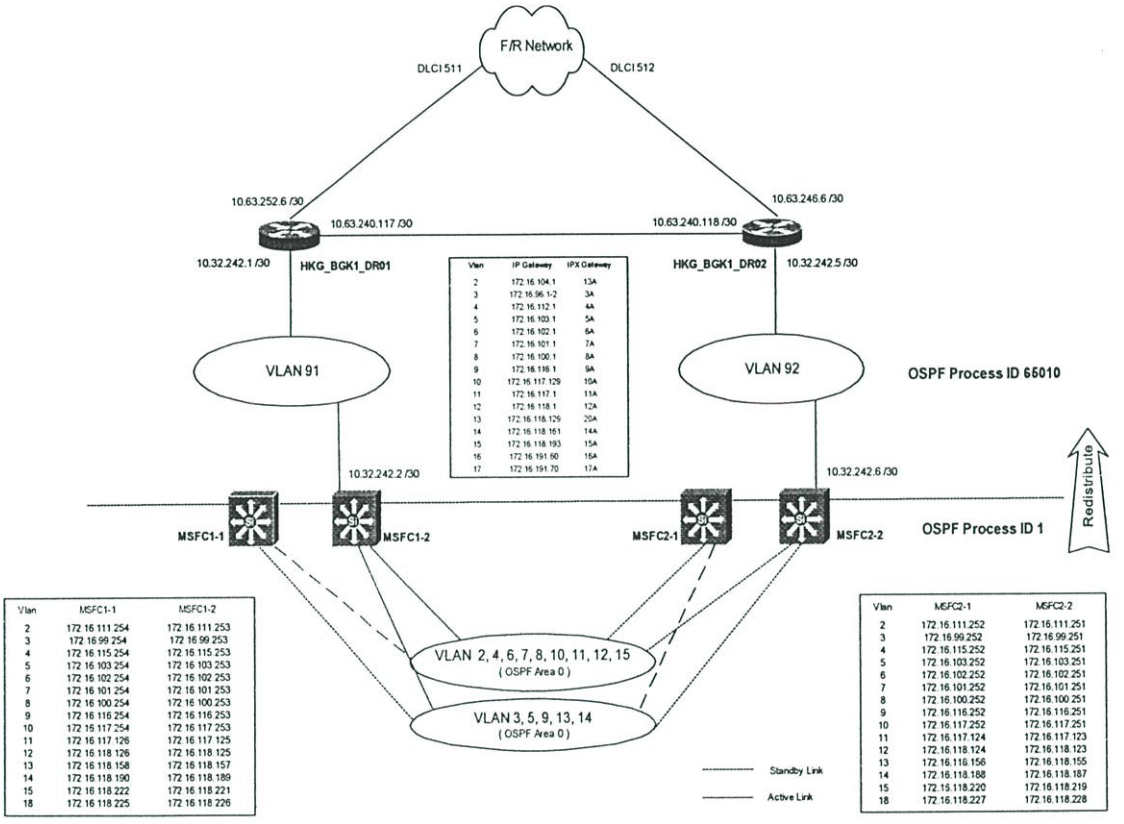
4. การแทนที่เครือข่ายแกนหลักที่ใช้ Shared FDDI อยู่ก่อนแล้ว เครือข่ายที่ใช้เทคโนโลยี FDDI สามารถจะทำการเปลี่ยนมาใช้กิกะบิทอีเทอร์เน็ตได้โดยการนำเอาสวิตช์กิกะบิทอีเทอร์เน็ตไปแทนที่ FDDI Concentrator หรืออาจจะเพียงนำกิกะบิทอีเทอร์เน็ทอินเตอร์เฟสการ์ด (Gigabit Ethernet Interface Card) ไปเปลี่ยนกับ FDDI อินเตอร์เฟสการ์ด ในเราท์เตอร์ที่มีใช้งานอยู่แล้ว ทั้งนี้การเปลี่ยนแปลงนี้ไม่ต้องมีการลงทุนเกี่ยวกับเรื่องสายสัญญาณเลย เนื่องจาก FDDI ส่วนมากจะใช้ เส้นใยแก้วนำแสงเป็นพื้นฐานอยู่แล้ว จึงทำให้สามารถเปลี่ยนอุปกรณ์เครือข่ายแบบ Ethernet/Fast Ethernet ไปเป็นกิกะบิทอีเทอร์เน็ทได้

5. การใช้เน็ทเวอร์คอินเตอร์เฟสการ์ดที่เครื่อง High-end Desktop ในการปรับปรุงเพื่อเพิ่มความเร็วของระบบขั้นสุดท้ายก็คือการเพิ่มความเร็วระหว่าง อุปกรณ์สวิตช์กิกะบิทอีเทอร์เน็ทกับเครื่อง Desktop ระดับ Hi-end ที่ติดตั้งกิกะบิทอีเทอร์เน็ทอินเตอร์เฟสการ์ด ทั้งนี้เพื่อรองรับปริมาณข้อมูลที่สูงมากๆ เช่น แอพพลิเคชั่นประเภทวิดีโอทั้งหลาย (VDO-Editing, VOD) หรืองานประเภท Data Warehouse



รูปที่ 7.2 รูปแบบการเชื่อมโดยรวมของอุปกรณ์หลักภายในเครือข่ายกิกะบิทอีเทอร์เน็ท

จากรูปที่ 7.2 แสดงให้เห็นถึงการเชื่อมต่อเสมือนหรือการเชื่อมต่อโดยรวมของอุปกรณ์หลัก ๆ ภายในเครือข่ายด้วยกิกะบิทอีเทอรเน็ท ซึ่งการเชื่อมต่อนี้เป็นการเชื่อมโยงเครือข่ายของอาคาร 4 ตึกเข้าด้วยกันโดยใช้ฟังก์ชันต่าง ๆ จากการทดลองในบทที่ 6 เช่น มาตรฐาน IEEE 802.1q และฟังก์ชัน VTP เป็นต้น



Vlan	IP Gateway	IPX Gateway
2	172.16.104.1	13A
3	172.16.96.1-2	3A
4	172.16.112.1	4A
5	172.16.103.1	5A
6	172.16.102.1	6A
7	172.16.101.1	7A
8	172.16.100.1	8A
9	172.16.116.1	9A
10	172.16.117.129	10A
11	172.16.117.1	11A
12	172.16.118.1	12A
13	172.16.118.129	20A
14	172.16.118.161	14A
15	172.16.118.193	15A
16	172.16.191.60	16A
17	172.16.191.70	17A

Vlan	MSFC1-1	MSFC1-2
2	172.16.111.254	172.16.111.253
3	172.16.99.254	172.16.99.253
4	172.16.115.254	172.16.115.253
5	172.16.103.254	172.16.103.253
6	172.16.102.254	172.16.102.253
7	172.16.101.254	172.16.101.253
8	172.16.100.254	172.16.100.253
9	172.16.116.254	172.16.116.253
10	172.15.117.254	172.16.117.253
11	172.16.117.126	172.16.117.125
12	172.16.118.126	172.16.118.125
13	172.16.118.158	172.16.118.157
14	172.16.118.190	172.16.118.189
15	172.16.118.222	172.16.118.221
18	172.16.118.225	172.16.118.226

Vlan	MSFC2-1	MSFC2-2
2	172.16.111.252	172.16.111.251
3	172.16.99.252	172.16.99.251
4	172.16.115.252	172.16.115.251
5	172.16.103.252	172.16.103.251
6	172.16.102.252	172.16.102.251
7	172.16.101.252	172.16.101.251
8	172.16.100.252	172.16.100.251
9	172.16.116.252	172.16.116.251
10	172.16.117.252	172.16.117.251
11	172.16.117.124	172.16.117.123
12	172.16.118.124	172.16.118.123
13	172.16.116.156	172.16.118.155
14	172.16.118.188	172.16.118.187
15	172.15.118.220	172.16.118.219
18	172.16.118.227	172.16.118.228

รูปที่ 7.3 รูปแบบการเชื่อมต่อเสมือนภายในเครือข่าย LAN ผ่านเครือข่าย WAN

ในรูปที่ 7.3 แสดงให้เห็นถึงการจัดแบ่ง VLAN รวมถึงการกำหนด Virtual gateway ให้กับ VLAN ในแต่ละวงด้วยโพรโตคอล HSRP ซึ่งจะทำให้ระบบมีความเสถียรมากขึ้น รวมทั้งแสดงให้เห็นถึงการเชื่อมต่อ LAN กับ WAN เข้าด้วยกัน โดยทำการสร้าง VLAN ใหม่เพื่อรองรับการเชื่อมต่อกับ WAN โดยเฉพาะ ซึ่งในที่นี้คือ VLAN 91 และ 92

7.2 สรุป

วิทยานิพนธ์นี้ได้เสนอผลงานวิจัย โครงสร้างของเครือข่ายอีเทอร์เน็ทซึ่งเป็นเครือข่ายแบบดั้งเดิม เปรียบเทียบกับเครือข่ายที่ถูกพัฒนาขึ้นมาในปัจจุบันคือกิกะบิทอีเทอร์เน็ตโดยทำการนำข้อมูลชนิดต่างๆ เช่นข้อมูล สัญญาณภาพ ส่งร่วมกันไปบนเครือข่าย โดยใช้เครือข่ายต่างกัน อีกทั้ง

สามารถตรวจวัดปริมาณของ Throughput และ Response Time บนเครือข่ายที่ถูกใช้ผ่านเครือข่ายด้วย สำหรับการทดสอบครั้งนี้ผู้ทำวิทยานิพนธ์ได้ทำการออกแบบระบบเครือข่ายกิกะบิทอีเทอร์เน็ท และทำการเปรียบเทียบประสิทธิภาพกับเครือข่ายอีเทอร์เน็ท ซึ่งก็ได้ผลการทดสอบดังกล่าวไว้ในบทที่ 6 กล่าวคือ เครือข่ายกิกะบิทอีเทอร์เน็ทจะให้ Data Throughput ที่สูง Response Time ที่เร็วทำให้การส่งสัญญาณภาพ และข้อมูลร่วมกันไปในเครือข่ายได้พร้อมกัน นับเป็นการใช้ช่องทางการสื่อสารข้อมูลอย่างคุ้มค่า และมีประสิทธิภาพ ซึ่งรูปแบบการวิจัยนี้พิสูจน์ให้เห็นวัตถุประสงค์หลักของประโยชน์การนำโครงสร้างหรือคุณสมบัติของเครือข่ายกิกะบิทอีเทอร์เน็ทมาใช้งาน

จากการนำอุปกรณ์ Digital Video Recorder (DVR) ซึ่งเป็นอุปกรณ์แปลงสัญญาณภาพจากกล้องโทรทัศน์วงจรปิดแบบอนาลอกเป็นสัญญาณดิจิตอล ซึ่งเชื่อมต่อเข้ากับเครือข่าย LAN ได้ทำให้เราสามารถรีโมทดูความเคลื่อนไหวของภาพโดยไม่เกิดอาการสะดุดของภาพ ก็เป็นผลลัพธ์อีกทางหนึ่งที่ได้จากการใช้เครือข่ายกิกะบิทอีเทอร์เน็ท

บรรณานุกรม

[1] Sackert, G. and Sackert, N. 1999. **Internetworking SNA with CISCO Solutions.** Indianapolis : Cisco Press.

[2] Doyle, J. 1998. **CCIE Professional Development : Routing TCP/IP.** Indianapolis : Cisco Press.

[3] Halsall, F. 1995. **Data Communications Computer Networks and Open Systems.** New York : Addison-Wesley.

[4] http://cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/dlsw.htm

ภาคผนวก ก.

อภิธานศัพท์
ค่าพารามิเตอร์

อภิธานศัพท์

ATM	Asynchronus Transfer Mode ด้วยการทำงานแบบ ATM ข้อมูล (เช่นเสียง ภาพเคลื่อนไหวหรือไฟล์ข้อมูล)จะถูกส่งออกไปเป็นส่วนๆในขนาดที่คงที่ (ต่างจากการส่งแบบแพ็กเก็ต (packet) ที่ขนาดของข้อมูลที่ถูกแบ่งแต่ละส่วนจะยาวไม่เท่ากัน เช่น อีเทอร์เน็ต หรือ FDDI) ด้วยวิธีส่งแบบนี้ทำให้การส่งข้อมูลมีความเร็วสูงมาก และทำให้ ATM เป็นที่นิยม ในการติดตั้งระบบเครือข่ายแกนหลักด้วยอุปกรณ์ที่มีอยู่ในปัจจุบันทำให้ ATM ยังสามารถใช้ในการส่งแบบ WAN ได้อีกด้วยเหมาะสำหรับองค์กรขนาดใหญ่ที่ขยายตัวเร็ว
Backbone	ส่วนระบบเครือข่ายที่ทำหน้าที่เป็นเส้นทางหลักในการรับส่งข้อมูลระหว่างระบบเครือข่ายแต่ละส่วน
Bandwidth	ความสามารถในการส่งข้อมูลของระบบเครือข่ายโดยใช้เป็นหน่วยของความเร็ว เช่น อีเทอร์เน็ตมีความสามารถในการรับส่งข้อมูล 10 ล้านบิทต่อวินาที ฟาสต์อีเทอร์เน็ตมีความสามารถในการรับส่งข้อมูล 100 ล้านบิทต่อวินาที ซึ่งมีแบนวิดธ์มากกว่า 10เท่า
Bridge	อุปกรณ์ที่ใช้ส่งข้อมูลระหว่างส่วนย่อยของระบบเครือข่ายที่ติดต่อกันโดยใช้โพรโตคอลเดียวกันถ้าหากข้อมูลที่ส่งไปยังผู้รับที่อยู่ในส่วนเดียวกับผู้ส่ง Bridge จะป้องกันให้ข้อมูลนั้นไม่ออกไปจากระบบเครือข่ายย่อยที่ส่งมาแต่หากผู้รับไม่ได้อยู่ในส่วนเดียวกันกับผู้ส่ง Bridge จะผ่านข้อมูลหลัก
Client	เครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องเทอร์มินอลที่ใช้บริการรวมกับเครื่องอื่นๆ โดยที่บริการนี้เก็บอยู่หรือดูแลอยู่โดยเครื่องเซิร์ฟเวอร์
DSL	Digital Subscriber Line เป็นเทคโนโลยีทางด้านระบบเครือข่ายที่ทำให้สามารถส่งข้อมูลด้วยแบนวิดธ์ที่มากบนสายทองแดงแบบปกติ โดยมีข้อจำกัดที่ระยะทาง DSL มี 4 ชนิด ได้แก่ ADSL,HDSL,SDSL,และ VDSL ทุกชนิดทำงานด้วยโมเด็ม 2 เครื่อง เครื่องหนึ่งอยู่ที่ผู้ให้บริการ อีกเครื่องที่ผู้ใช้บริการเพราะเทคโนโลยี DSL ไม่ได้ใช้แบนวิดธ์ทั้งหมดของสายทำให้มีพื้นที่จะใช้เป็นช่องสัญญานเสียงได้
Ethernet	เทคโนโลยีด้านแลนที่ได้รับความนิยม ซึ่งใช้ CSMA/CD (การตรวจสอบการชนของข้อมูล)ในการเคลื่อนย้ายแพ็กเก็ตระหว่างเครื่องข่ายในระบบเครือข่าย และทำงานได้บนสายสัญญาณหลายชนิดที่ความเร็ว 10 ล้านบิทต่อวินาที หรือนิยมเรียกว่า10BaseT
Extranet	ระบบเครือข่ายที่อนุญาตให้บุคคลภายนอก (เช่นผู้จัดส่งสินค้า พนักงานขายสิน

	ค้าอิสระ หรือผู้ค้าปลีก) เข้ามาใช้เอกสารของทางบริษัท เช่น รายการราคาสินค้า ตารางขนส่งสินค้าและอื่นๆ
Fast Ethernet	ใช้วิธีส่งข้อมูลเช่นเดียวกับอีเทอร์ แต่ทำงานที่ความเร็ว 100 ล้านบิทต่อวินาที เร็วกว่าอีเทอร์เน็ต 10 เท่า ฟาสต์อีเทอร์เน็ตยังเป็นการแก้ปัญหาความคั่งคับที่ดีและเพิ่มประสิทธิภาพให้แก่ระบบเครือข่ายแบบอีเทอร์เน็ตอย่างมากโดยมีปัญหาตามมาน้อยที่สุด เพราะสามารถทำงานได้บนสายสัญญาณ,โปรแกรม, หรืออุปกรณ์ตรวจสอบสภาพระบบเครือข่ายเดียวกับอีเทอร์เน็ตทันที
FDDI	Fiber Distributed Data Interface เทคโนโลยีของแลนที่ทำงานด้วยความเร็ว 100 ล้านบิทต่อวินาทีบนสายใยแก้วนำแสง นิยมใช้เป็นระบบเครือข่ายแกนหลักในองค์กรขนาดใหญ่
Frame Relay	บริการแบบ WAN ที่สามารถเปิดและปิดการเชื่อมต่อระหว่างสถานที่ห่างกันได้
FTP	File Transfer protocol ส่วนที่สำคัญมากที่สุดส่วนหนึ่งของ Internet Protocol Stack (TCP/IP) ใช้สำหรับถ่ายโอนไฟล์จากอีเทอร์เน็ตเซิร์ฟเวอร์สู่เครื่องของคุณ
HTML	Hypertext markup Language ภาษาสำหรับจัดรูปแบบเอกสารเพื่อ ใช้แสดงผลโดย World Wide Web Browse
HTTP	Hypertext transmission protocol โพรโทคอลที่ควบคุมการส่งเอกสาร HTML ผ่านทางอินเทอร์เน็ต
Hub	อุปกรณ์ที่ใช้เชื่อมต่อระหว่างไคลเอ็นต์ และเซิร์ฟเวอร์ รวมถึงสามารถขยายสัญญาณที่ส่งได้ด้วย เปรียบ ได้กับฮับชุมสายในระบบเครือข่ายที่มีโครงสร้างแบบดาว
Internet	ระบบเครือข่ายระดับโลกขนาดมหึมาที่มีเครื่องคอมพิวเตอร์เชื่อมต่ออยู่หลายพันเครื่องครอบคลุมทั่วโลก และสามารถเข้าใช้งานได้โดยใช้โมเด็ม หรือเราเตอร์และซอฟต์แวร์ที่เหมาะสม
Intranet	ระบบเครือข่ายภายในที่สามารถใช้งานบางอย่างที่นิยมบนอินเทอร์เน็ตได้ เช่น บราวเซอร์เพื่อดูรูปสินค้า HTML เพื่อเตรียมเอกสารของบริษัทหรือประกาศต่างๆ
ISDN	Integrated Service Digital Network การติดต่อสื่อสารที่ให้บริการโดยผู้ให้บริการโทรศัพท์มีความเร็วสูงและครอบคลุมพื้นที่ใช้งานอย่างกว้างขวาง
LAN	Local Area Network ระบบเครือข่ายเดี่ยวๆ หรือกลุ่มของระบบเครือข่ายย่อยที่จำกัดอยู่ภายในอาคารหรือมหาวิทยาลัย มีความหมายตรงข้ามกับ WAN

Modem	อุปกรณ์ที่ทำให้เครื่องคอมพิวเตอร์สามารถเชื่อมต่อเข้ากับเครื่องอื่นๆ และระบบเครือข่ายโดยใช้สายโทรศัพท์ธรรมดา โมเด็มมาจากคำว่า “modulate” แปลว่าสัญญาณดิจิตอลจากเครื่องคอมพิวเตอร์จะถูกแปลงเป็นสัญญาณอะนาล็อก เพื่อส่งออกไปทางสายโทรศัพท์ และคำว่า “demodulate” หมายถึง แปลงสัญญาณอะนาล็อกที่ได้รับกลับไปเป็นสัญญาณดิจิตอลที่เครื่องคอมพิวเตอร์เข้าใจ
Packet	ส่วนของข้อมูลที่มี ‘ส่วนหัว (header) ติดเพิ่มเข้าไปซึ่งส่วนหัวนี้จะช่วยระบุว่าแพ็กเกจนี้เป็นข้อมูลชนิดใดและจะส่งไปยังที่ใด ถ้าเปรียบข้อมูลเหมือนกับเนื้อความในจดหมาย ส่วนหัวก็คือการจ่าหน้าซอง
Remote	อุปกรณ์ที่ใช้รองรับผู้ที่ติดต่อเข้ามายังระบบเครือข่ายผ่านทางสายโทรศัพท์เพื่อใช้งานที่อยู่บนระบบเครือข่ายของเซิร์ฟเวอร์สำหรับการเข้าถึงจากระยะไกล (Remote Access Server) สามารถจะหาช่องสัญญาณที่ว่างอยู่ให้แก่ผู้ติดต่อเข้ามาโดยอัตโนมัติ
Router	อุปกรณ์ที่เคลื่อนย้ายข้อมูลระหว่างส่วนระบบเครือข่ายของย่อยและมีความสามารถในการอ่านส่วนหัวของแพ็กเก็ตที่ส่งมาเพื่อตัดสินใจเลือกเส้นทางในการส่งข้อมูลต่อไป นอกจากนั้น เราเตอร์ยังสามารถเชื่อมต่อส่วนของระบบเครือข่ายที่ใช้โพรโตคอลต่างกันและยังช่วยให้ผู้ใช้หลายคนสามารถเชื่อมต่ออินเตอร์เน็ตพร้อมกันผ่านสายออกสู่อินเตอร์เน็ตเพียงสายเดียวได้
Server	เครื่องหรือซอฟแวร์ที่ให้บริการแก่ไคลเอ็นต์ เช่นให้บริการโปรแกรมต่างๆ,เครื่องพิมพ์,แฟกซ์หรือโมเด็ม
Switch	อุปกรณ์ที่เพิ่มประสิทธิภาพให้แก่ระบบเครือข่ายด้วยการแบ่งระบบเครือข่ายออกเป็นส่วนย่อยๆและลดการแย่งกันใช้แบนวิดธ์ เมื่อสวิตซ์ได้รับแพ็กเก็ตที่ส่งมา มันจะส่งต่อข้อมูลนี้ไปสู่ส่วนของระบบเครือข่ายที่มีผู้รับอยู่ภายในเท่านั้น ทำ ให้สามารถลดปริมาณการแย่งแบนวิดธ์ระหว่างไคลเอ็นต์,เซิร์ฟเวอร์ หรือเวิร์กกรุ๊ปที่เชื่อมต่อกับสวิตซ์ได้เป็นอย่างมาก
Token Ring	เทคโนโลยีของแลนที่จัดส่งแพ็กเก็ตระหว่างเครื่องโดยผ่านการเชื่อมต่อแบบวงแหวน ทำงานที่ความเร็ว 4 ถึง 16 ล้านบิทต่อนาที
VPN	ระบบเครือข่ายส่วนตัวเสมือน (Virtual PrivateNetwork-VPN) ทำให้การติดติอแบบไอพีสามารถเดินทางบน TCP/IP สาธารณะ(อินเทอร์เน็ต) ได้อย่างปลอดภัย โดยการเข้ารหัสข้อมูลทุกอันสู่ปลายทาง VPN ใช้การสร้างอุโมงค์เพื่อเข้ารหัสข้อมูลในระดับไอพี

ค่าพารามิเตอร์

ตัวอย่างค่าพารามิเตอร์ของ Switch Layer 2 ที่ใช้เชื่อมกับ Switch 3

Catalyst 3500XL#sh run

Building configuration...

Current configuration:

!

! Last configuration change at 21:04:06 UTC Sat Aug 28 2004 by scnbadm

! NVRAM config last updated at 15:41:32 UTC Sat Aug 21 2004 by scnbadm

!

version 12.0

no service pad

service timestamps debug uptime

service timestamps log datetime

service password-encryption

!

hostname switch layer2

!

aaa new-model

aaa authentication login default local

aaa authentication login loginauthen group tacacs+ local

aaa authentication enable default group tacacs+ enable

aaa authorization exec default local

aaa authorization exec exccauthor group tacacs+ if-authenticated local

aaa accounting exec execacc start-stop group tacacs+

aaa accounting commands 15 execacc stop-only group tacacs+

enable secret 5 1aXpe$qlshuOYGp1bfjjrdub7WS1

!

username scnbtelecom password 7 111F1000001D05001D

!

```
!
!
ip subnet-zero
no ip finger
no ip domain-lookup

interface FastEthernet0/1
 switchport access vlan 2
spanning-tree portfast
!
interface FastEthernet0/2
 switchport access vlan 2
 spanning-tree portfast
!
interface FastEthernet0/3
 description
 switchport access vlan 5
spanning-tree portfast
!
interface FastEthernet0/4
 switchport access vlan 5
 spanning-tree portfast
!
interface FastEthernet0/5
 switchport access vlan 7
  spanning-tree portfast
!
interface FastEthernet0/6
 switchport access vlan 4

  spanning-tree portfast
```

```
!
interface FastEthernet0/7
 description
 switchport access vlan 7
  spanning-tree portfast
!
interface FastEthernet0/8
spanning-tree portfast
!
interface FastEthernet0/9
 switchport access vlan 7
  spanning-tree portfast
!
interface FastEthernet0/10
 switchport access vlan 7
  spanning-tree portfast
!
interface FastEthernet0/11
 description
 switchport access vlan 7
  spanning-tree portfast
!
interface FastEthernet0/12
 switchport access vlan 7
  spanning-tree portfast
!
interface FastEthernet0/13
 switchport access vlan 7
  spanning-tree portfast
!
interface FastEthernet0/14
```

```
 switchport access vlan 7
 spanning-tree portfast
interface FastEthernet0/15
 switchport access vlan 5
spanning-tree portfast
!
interface FastEthernet0/16
 switchport access vlan 7
spanning-tree portfast
!
interface FastEthernet0/17
 switchport access vlan 7
spanning-tree portfast
!
interface FastEthernet0/18
 switchport access vlan 8
  spanning-tree portfast
!
interface FastEthernet0/19
 switchport access vlan 5
spanning-tree portfast
!
interface FastEthernet0/20
 switchport access vlan 7
  spanning-tree portfast
!
interface FastEthernet0/21
 switchport access vlan 7
spanning-tree portfast
!
interface FastEthernet0/22
```

```
 switchport access vlan 7
spanning-tree portfast
interface FastEthernet0/23
 description
 switchport access vlan 8
  spanning-tree portfast
!
interface FastEthernet0/24
 switchport access vlan 7
spanning-tree portfast
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 !
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 !
interface VLAN1
 description FOR DEVICES MANAGEMENT
 ip address 11.10.73.1 255.255.0.0
 no ip directed-broadcast
 no ip route-cache
!
ip default-gateway 11.10.1.254
no ip http server
logging trap warnings
logging 11.10.1.100
snmp-server engineID local 0000000902000004C1050F00
snmp-server community scnbmon RO
```

```
snmp-server community scnbsup RW
snmp-server enable traps snmp authentication linkdown linkup coldstart
snmp-server enable traps vlan-membership
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps vtp
snmp-server enable traps cluster
snmp-server host 11.10.1.100 trap scnbmon
tacacs-server host 11.10.1.103
tacacs-server key scnbl0ck
banner exec ^C
AUTHORIZED ACCESS ONLY
THIS SYSTEM IS THE PROPERTY OF SCNB
DISCONNECT IMMEDIATEDLY IF YOUR ARE NOT AN AUTHORIZED USER !
^C
banner login ^C
AUTHORIZED ACCESS ONLY
THIS SYSTEM IS THE PROPERTY OF SCNB
DISCONNECT IMMEDIATELY IF YOU ARE NOT AN AUTHORIZED USER!^C
privilege exec level 1 show startup-config
!
line con 0
 password 7 010614035E0512
 transport input none
 stopbits 1
line vty 0 4
 password 7 110A1016141D
 authorization exec execauthor
 accounting commands 15 execacc
 accounting exec execacc
```

```
 login authentication loginauthen
line vty 5 15
!
ntp clock-period 11259804
ntp server 11.10.1.1 prefer
ntp server 11.10.1.3
ntp server 11.10.1.2
end
```

ตัวอย่างค่าพารามิเตอร์ของ Catalyst 6509

```
Catalyst 6509 (enable) sh run
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Sat Aug 28 2004, 00:58:09
!
#version 6.4(3)
!
!
#system web interface version Engine Version: 5.3.4 ADP Device: Cat6000 ADP Vers
ion: 1.9 ADK: 40
!
set password $2$/Wi.$SFPWsvIF4Rih4Rukku6RL.
set enablepass $2$dXe.$U2yylft27WfNSwA0FG9UU1
set prompt Cat6509-2->
set banner motd ^C
```

```
AUTHORISED ACCESS ONLY
THIS SYSTEM IS THE PROPERTY OF SCNB
DISCONNECT IMMEDIATELY IF YOU ARE NOT AN AUTHORIZED USER!

Catalyst 6509-2 at ST-3
Software Release 6.1.2
IP address 11.10.83.2
^C

!
#errordetection
set errordetection portcounter enable
!
#system
set system name  Catalyst6509 -2
set system location ST-3
set system contact  IBM Thailand
set system highavailability enable
!
#!
#snmp
set snmp community read-only     scnbmon
set snmp community read-write     scnbsup
set snmp community read-write-all scnbsup
set snmp rmon enable
set snmp trap 11.10.1.100 scnbmon port 162 owner mswinusr@nms1 [99730 index 1
set snmp trap 172.21.103.244 scnbmon port 162 owner  index 2
set snmp trap 172.21.103.243 scnbmon port 162 owner CLI index 3
!
```

```
#vtp
set vtp domain SCNB
set vtp pruning enable
set vlan 1 name default type ethernet mtu 1500 said 100001 state active
set vlan 2 name CB type ethernet mtu 1500 said 100002 state active
set vlan 3 name Existing-Network type ethernet mtu 1500 said 100003 state active
set vlan 4 name C&IB type ethernet mtu 1500 said 100004 state active
set vlan 5 name Server_Farm type ethernet mtu 1500 said 100005 state active
set vlan 6 name SS&PM type ethernet mtu 1500 said 100006 state active
set vlan 7 name Group-Techology type ethernet mtu 1500 said 100007 state active
set vlan 8 name Treasury type ethernet mtu 1500 said 100008 state active
set vlan 9 name Finance type ethernet mtu 1500 said 100009 state active
set vlan 10 name Human-Resource type ethernet mtu 1500 said 100010 state active
set vlan 11 name Audit type ethernet mtu 1500 said 100011 state active
set vlan 12 name Legal&Complianc type ethernet mtu 1500 said 100012 state active
set vlan 13 name External-Affair type ethernet mtu 1500 said 100013 state active
set vlan 14 name Risk-Management type ethernet mtu 1500 said 100014 state active
set vlan 15 name CEO type ethernet mtu 1500 said 100015 state active
set vlan 16 name DLSw-SSH_DR03 type ethernet mtu 1500 said 100016 state active
set vlan 17 name DLSw-SSH_DR04 type ethernet mtu 1500 said 100017 state active
set vlan 18 name Nortel-Intermediate-Net type ethernet mtu 1500 said 100018 state
        active
set vlan 19 name Development type ethernet mtu 1500 said 100019 state active
set vlan 51 name DLSw type ethernet mtu 1500 said 100051 state active
set vlan 52 name WAN_DR type ethernet mtu 1500 said 100052 state active
set vlan 53 name Existing type ethernet mtu 1500 said 100053 state active
set vlan 54 name User type ethernet mtu 1500 said 100054 state active
set vlan 55 name Server_Farm_DR type ethernet mtu 1500 said 100055 state active
set vlan 91 name BGK1_DR01 type ethernet mtu 1500 said 100091 state active
set vlan 92 name BGK1_DR02 type ethernet mtu 1500 said 100092 state active
set vlan 94 name BGK2_DR02 type ethernet mtu 1500 said 100094 state active
```

```
set vlan 99 rspan name RSPAN-VLAN state active
set vlan 1002 name fddi-default type fddi mtu 1500 said 101002 state active
set vlan 1004 name fddinet-default type fddinet mtu 1500 said 101004 state active
        stp ieee
set vlan 1005 name trnet-default type trbrf mtu 1500 said 101005 state active stp ibm
set vlan 93
set vlan 1003 name token-ring-default type trcrf mtu 1500 said 101003 state acti
ve mode srb aremaxhop 0 stemaxhop 0 backupcrf off
!
#ip
set interface sc0 1 11.10.83.2/255.255.0.0 11.10.255.255


set ip route 0.0.0.0/0.0.0.0      11.10.1.254
set ip alias default      0.0.0.0
!
#command alias
set alias sw1 telnet 11.10.83.1
set alias sw3 telnet 11.10.31.1
set alias sw4 telnet 11.10.22.51
!
#spantree
#vlan                  <VlanId>
set spantree priority 16384  1
set spantree priority 16384  2
set spantree priority 16384  3
set spantree priority 16384  4
set spantree priority 16384  5
set spantree priority 16384  6
set spantree priority 16384  7
set spantree priority 16384  8
set spantree priority 16384  9
```

```
set spantree priority 16384  10
set spantree priority 16384  11
set spantree priority 16384  12
set spantree priority 16384  13
set spantree priority 16384  14
set spantree priority 16384  15
set spantree priority 16384  16
set spantree priority 16384  17
set spantree priority 16384  18
set spantree priority 16384  19
set spantree priority 16384  91
set spantree priority 16384  92
set spantree priority 16384  99
!
#syslog
set logging server enable
set logging server 11.10.1.100
set logging server severity 7
!
#ntp
set ntp client enable
set ntp server 11.10.1.2
!
#set boot command
set boot config-register 0x2
set boot system flash bootflash:cat6000-sup2cv.6-4-3.bin
!
#igmp
set igmp disable
!
#mls
```

```
set mls agingtime ipx 0
!
#qos
set qos wred 1p2q2t tx queue 1 40:80 70:100
set qos wred 1p2q2t tx queue 2 40:80 70:100
!
#port channel
set port channel 4/3-4 98
set port channel 6/1-2 99
set port channel 8/29-32 104
set port channel 8/33-36 105
set port channel 9/1 106
set port channel 9/2 107
set port channel 9/3 108
set port channel 9/4 109
set port channel 9/5 110
set port channel 9/6 111
set port channel 9/7 112
set port channel 9/8 113
set port channel 9/9 114
set port channel 9/10 115
set port channel 9/11 116
set port channel 9/12 117
set port channel 9/13 118
set port channel 9/14 119
set port channel 9/15 120
set port channel 9/16 121
set port channel 4/1-2 134
!
# default port status is enable
!
```

```
!
#module 1 : 2-port 1000BaseX Supervisor
set module name    1
!
#module 2 : 2-port 1000BaseX Supervisor
set module name    2
!
#module 3 : 48-port 10/100BaseTX Ethernet
set vlan 2    3/23
set vlan 3    3/42,3/45
set vlan 4    3/20,3/25-30,3/32-38
set vlan 5    3/22,3/24,3/31,3/39-41,3/43-44,3/46
set vlan 7    3/17
set vlan 8    3/1-16,3/18-19
set vlan 9    3/21
set vlan 17   3/48
set port speed     3/3,3/7,3/19,3/43,3/46  10
set port speed     3/1-2,3/5-6,3/15-16,3/18,3/24,3/26-27,3/39,3/42,3/44-45,3/47
-48  100
set port duplex    3/1-3,3/5-6,3/16,3/18,3/24,3/26-27,3/39,3/42,3/44-45,3/47-48
  full
set port name      3/1  SCTHTR1T B7-01
set port name      3/2  SCTHTR3T B7-02
set port name      3/3  WINFAX B8-01
set port name      3/4  SCTHTR4T B8 02
set port name      3/5  SCNBBKTSY_S2 B9-01
set port name      3/6  SCTHTR2T B9-02
set port name      3/7  TR01_TRD B10-01
set port name      3/8  SCTH001G B10-02
set port name      3/9  TIBCOSPOKE1 B11-01
set port name      3/10 TIBCOSPOKE2 B11-02
```

set port name 3/11 DDISUB1 B11-03

set port name 3/12 DDISUB2 B11-04

set port name 3/13 PR1_THPROCO1 B12-04

set port name 3/14 DDI B12-02

set port name 3/15 TCSS_7563076 B2-01

set port name 3/16 DTS B2-02

set port name 3/17 BPECTHRO02

set port name 3/18 SCNBBKTYOA1_S2 B9-03

set port name 3/19 FEDS TN6-02

set port name 3/20 NPS_SUBSYSTEM D2-03

set port name 3/21 SCTHRSR1_S8 D2-01

set port name 3/22 SCTHTS14G E13-01

set port name 3/23 CAPSTHSVR D3-01

set port name 3/24 SCTHTS7G_1 E14-1

set port name 3/25 STS C6-01

set port name 3/26 STS TH04 AS400-04

set port name 3/27 STS TH03 AS400-05

set port name 3/28 NCS_TH01 AS400-06

set port name 3/29 PSB3 C4-03

set port name 3/30 OSF FAX FORMAT C3-01

set port name 3/31 APRNBKKDNSSVR01

set port name 3/32 PSB1 C2-01

set port name 3/33 PSB2 C2-02

set port name 3/34 NCCS C4-02

set port name 3/35 CANDLESVR C4-01

set port name 3/36 OSF FAX UPLOAD C3-02

set port name 3/37 NCSTHSVR C5-01

set port name 3/38 NCSEOD C5-02

set port name 3/39 SCTHTS1G_IP E14-2

set port name 3/40 SCTHTS11G_1 E12-01

set port name 3/41 APRNBKKDNSSVR01

```
set port name       3/42 AS/400 PROD TN9-01
set port name       3/43 NDM-COA0006 E1-3
set port name       3/44 AS/400_SCNB_3
set port name       3/45 SCTH005F_S6 D2-02
set port name       3/46 NDM-COA001R E1-4
set port name       3/47 BGK1_DR02 TN5-5
set port name       3/48 Bridge_DR02 TN5-3
set trunk 3/47 on isl 1-1005,1025-4094
set spantree portfast    3/1-48 enable
!
#module 4 : 16-port 1000BaseX Ethernet
set module name    4
set port trap       4/1-16  enable
set port name       4/1  Cat6509-1_p4/2
set port name       4/2  Cat6509-1_p4/1
set port name       4/3  C3548-331
set port name       4/4  C3548-8354
set port name       4/5  C3524-1231
set port name       4/6  C3524-731
set port name       4/7  C3548-1731
set port name       4/8  C3548-1131
set port name       4/9  C3548-231
set port name       4/10 C3548-631
set port name       4/11 C3524-1133
set udld enable 4/13-16
set trunk 4/1  on dot1q 1-1005,1025-4094
set trunk 4/2  on dot1q 1-1005,1025-4094
set trunk 4/3  on dot1q 1-1005,1025-4094
set trunk 4/4  on dot1q 1-1005,1025-4094
set trunk 4/5  on dot1q 1-1005,1025-4094
set trunk 4/6  on dot1q 1-1005,1025-4094
```

```
set trunk 4/7  on dot1q 1-1005,1025-4094
set trunk 4/8  on dot1q 1-1005,1025-4094
set trunk 4/9  on dot1q 1-1005,1025-4094
set trunk 4/10 on dot1q 1-1005,1025-4094
set trunk 4/11 on dot1q 1-1005,1025-4094
set trunk 4/12 on isl 1-1005,1025-4094
set trunk 4/13 on isl 1-1005,1025-4094
set trunk 4/14 on isl 1-1005,1025-4094
set trunk 4/15 on isl 1-1005,1025-4094
set trunk 4/16 on isl 1-1005,1025-4094
set spantree portvlancost 4/3  cost 7 2
set port channel 4/1-2 mode on
set port channel 4/3-4 mode off
!
#module 5 : 0-port Switch Fabric Module
set module name    5    Switch Fabric Module
!
#module 6 : 16-port 1000BaseX Ethernet
set module name    6
set vlan 5    6/16
set port trap      6/1-15  enable
set port name      6/1  Cat6509-3_p3/1
set port name      6/2  Cat6509-3_p3/2
set port name      6/3  C3524-1634
set port name      6/4  C3548-531
set port name      6/5  C3548-1531
set port name      6/6  C3548-1533
set port name      6/7  C3524-8352
set port name      6/8  C3524-1733
set port name      6/9  C3548-1331
set port name      6/10 C3548-2031
```

```
set port name       6/11 C3548-1631
set port name       6/12 C3524-432
set port name       6/13 C3524-131
set port name       6/16 AS/400 Ver7
set udld enable 6/14-15
set trunk 6/1  on dot1q 1-1005,1025-4094
set trunk 6/2  on dot1q 1-1005,1025-4094
set trunk 6/3  on dot1q 1-1005,1025-4094
set trunk 6/4  on dot1q 1-1005,1025-4094
set trunk 6/5  on dot1q 1-1005,1025-4094
set trunk 6/6  on dot1q 1-1005,1025-4094
set trunk 6/7  on dot1q 1-1005,1025-4094
set trunk 6/8  on dot1q 1-1005,1025-4094
set trunk 6/9  on dot1q 1-1005,1025-4094
set trunk 6/10 on dot1q 1-1005,1025-4094
set trunk 6/11 on dot1q 1-1005,1025-4094
set trunk 6/12 on dot1q 1-1005,1025-4094
set trunk 6/13 on dot1q 1-1005,1025-4094
set trunk 6/14 on isl 1-1005,1025-4094
set trunk 6/15 on isl 1-1005,1025-4094
set trunk 6/16 off isl 1-1005,1025-4094
set port channel 6/1-2 mode on
!
#module 7 : 2-port Network Analysis Module
!
#module 8 : 48-port 10/100BaseTX Ethernet
set vlan 2    8/15,8/26,8/43-45,8/47-48
set vlan 3    8/1-5,8/7-11,8/13-14,8/16-21,8/23,8/25
set vlan 5    8/12,8/24,8/27-29,8/32-37,8/39-41,8/46
set vlan 8    8/30
set vlan 16   8/6,8/22,8/31,8/38,8/42
```

```
set port speed    8/13,8/28-29,8/37,8/39-41  10
set port speed    8/6,8/15,8/21-23,8/27,8/31,8/36,8/42,8/46  100
set port duplex   8/6,8/15,8/21-23,8/27,8/31,8/36,8/42,8/46  full
set port name     8/1  APRNBKKDMNIXPAA A2-1
set port name     8/2  APRNBKKDRNIXP01 A2-2
set port name     8/3  APRNBKK001 A3-01
set port name     8/4  SCBAPRNBKK001 A3-2
set port name     8/5  SCBAPRNBKK002 A3-3
set port name     8/6  E14-3
set port name     8/7  SCTH4FSVR E4-01
set port name     8/8  PRINT SERVER E4-03
set port name     8/9  NORTON E5-01
set port name     8/10 SCNBBK01F E5-02
set port name     8/11 SCNBBK04F E6-01
set port name     8/12 SCNB99844 C12-1
set port name     8/13 TRANS MDS E8-01
set port name     8/14 FAX SERVER1 E9-01
set port name     8/15 SCTHLAPSSVR D9-08
set port name     8/16 FAX DATABASE E10-01
set port name     8/17 SCTHEP2N_S6 E11-01
set port name     8/18 SCTHEP2N_S7 E11-02
set port name     8/19 SCTHBDC2F-S6 E11-3
set port name     8/20 ANNEX3 TN3-02
set port name     8/21 AS/400_PROD2 TN9-4
set port name     8/22 SCTHTS1G_Brdg E14-4
set port name     8/23 AS/400_3_TEST AS400
set port name     8/24 SCBTHA199047 E5-03
set port name     8/25 SCTHBDC2F-S7 E11-4
set port name     8/26 SCTHIVRSVR02_I B13-1
set port name     8/27 AS/400-V7-2
set port name     8/28 NDM-COA0004 E1-1
```

```
set port name      8/29 NDM-COA000X E2-1
set port name      8/30 FEDS ROUTER DIRECT
set port name      8/31 E13-3
set port name      8/32 SCTH002F D1-02
set port name      8/33 SCBAPRNBKK003 A1-2
set port name      8/34 APRNBKK002 A1-01
set port name      8/35 APRNBKKDMIXPAB A1-3
set port name      8/36 SCTH7FSVR D6-01
set port name      8/37 NDM-COA0005 E1-2
set port name      8/38 SCTHIVRSVR02_B B13-2
set port name      8/39 NDM_IPX2003 E2-2
set port name      8/40 NDM_IPX2007 E2-3
set port name      8/41 NDM_COA001Y E2-4
set port name      8/42 SCTHTS13G_Brdg E13-4
set port name      8/43 SCTHSCTSVR-S0 C8-1
set port name      8/44 SCTHSCTSVR-S1 C8-2
set port name      8/45 SCTHACCSVR C8-03
set port name      8/46 SCTHTS13G_IP E13-2
set port name      8/47 SCTHMINIDWSVRI C9-01
set port name      8/48 APRNBKKNAS01 C10-1
set spantree portfast    8/1-48 enable
!
#module 9 : 16-port 1000BaseX Ethernet
set module name    9
set port trap      9/1-16  enable
set port name      9/1  C3548-1032
set port name      9/2  C3548-1033
set port name      9/3  C3524-932
set port name      9/4  C3548-733
set port name      9/5  C3548-1333
set port name      9/6  C3548-1432
```

```
set port name       9/7  C3548-1433
set port name       9/8  C3548-1834
set port name       9/10 C3548-1932
set port name       9/11 C3548-2033
set port name       9/12 C3548-1931
set port name       9/13 C3524-433
set port name       9/14 C3548-1832
set udld enable 9/9
set trunk 9/1  on dot1q 1-1005,1025-4094
set trunk 9/2  on dot1q 1-1005,1025-4094
set trunk 9/3  on dot1q 1-1005,1025-4094
set trunk 9/4  on dot1q 1-1005,1025-4094
set trunk 9/5  on dot1q 1-1005,1025-4094
set trunk 9/6  on dot1q 1-1005,1025-4094
set trunk 9/7  on dot1q 1-1005,1025-4094
set trunk 9/8  on dot1q 1-1005,1025-4094
set trunk 9/9  on isl 1-1005,1025-4094
set trunk 9/10 on dot1q 1-1005,1025-4094
set trunk 9/11 on dot1q 1-1005,1025-4094
set trunk 9/12 on dot1q 1-1005,1025-4094
set trunk 9/13 on dot1q 1-1005,1025-4094
set trunk 9/14 on dot1q 1-1005,1025-4094
set trunk 9/15 on isl 1-1005,1025-4094
set trunk 9/16 on isl 1-1005,1025-4094
set port channel 9/1-16 mode off
!
#module 15 empty
!
#module 16 : 1-port Multilayer Switch Feature Card
!
#switch port analyzer
```

```
set rspan destination  7/1  99  inpkts disable learning enable create
end
```

ตัวอย่างค่าพารามิเตอร์ของ MFSC

```
MFSC-2-2#
MFSC-2-2#sh run
Building configuration...

Current configuration : 11078 bytes
!
! Last configuration change at 22:57:02 UTC Sun Aug 8 2004 by scnbadm
! NVRAM config last updated at 22:59:08 UTC Sun Aug 8 2004 by scnbadm
!
version 12.1
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname MFSC-2-2
!
boot system flash bootflash:c6msfc2-jsv-mz.121-13.E6
boot bootldr bootflash:c6msfc2-boot-mz.121-13.E6
aaa new-model
aaa authentication login default local
aaa authentication login loginauthen group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default local
aaa authorization exec execauthor group tacacs+ if-authenticated local
aaa accounting exec execacc start-stop group tacacs+
aaa accounting commands 15 execacc stop-only group tacacs+
```

```
enable secret 5 $1$LDRz$4Qw.9IQazv2/GZk8UBXgy/
!
username ibmadmin password 7 13061E010803
username scnbadmin privilege 15 password 7 12101503111B58
username scnbtelecom privilege 12 password 7 150402091325252831
ip subnet-zero
!
!
ip telnet source-interface Vlan7
no ip domain-lookup
ip host bay1 172.21.191.57
ip host msfc11 11.10.1.1
ip host msfc12 11.10.1.2
ip host msfc21 11.10.1.3
ip host msfc22 11.10.1.4
ip host cat65091 11.10.83.1
ip host cat65092 11.10.83.2
ip host cat65093 11.10.31.1
!
ipx routing 00d0.0449.abfd
ipx maximum-paths 4
ipx ping-default diagnostic
ipx per-host-load-share
!
!
!
interface Vlan1
 description VLAN1-Network Management
 ip address 11.10.1.4 255.255.0.0
 ip access-group 160 in
 no ip redirects
```

```
 ip ospf cost 10000
 ip ospf priority 90
 standby 1 ip 11.10.1.254
 standby 1 priority 150
 standby 1 preempt
!
interface Vlan2
 description VLAN2-Consumer Banking
 ip address 172.21.111.251 255.255.248.0
 ip helper-address 172.21.103.9
 no ip redirects
 ip route-cache flow
 ip ospf priority 89
 ipx network 13A
 standby 2 ip 172.21.104.1
 standby 2 priority 150
 standby 2 preempt
 bridge-group 1
!
interface Vlan3
 description VLAN3-Existing ATM
 ip address 172.21.99.251 255.255.252.0
 no ip redirects
 ip route-cache flow
 ip ospf priority 90
 ipx network 1023204
 standby 3 ip 172.21.96.1
 standby 3 priority 150
 standby 3 preempt
 standby 33 ip 172.21.96.2
 standby 33 priority 150
```

```
 standby 33 preempt
 bridge-group 1
!
interface Vlan4
 description VLAN4-C&IB
 ip address 172.21.115.251 255.255.252.0
 ip helper-address 172.21.103.9
 no ip redirects
 ip ospf priority 89
 ipx network 4A
 standby 4 ip 172.21.112.1
 standby 4 priority 150
 standby 4 preempt
 bridge-group 1
!
interface Vlan5
 description VLAN5-SERVER FARM
 ip address 172.21.103.251 255.255.255.0
 ip helper-address 172.21.103.9
 no ip redirects
 ip route-cache flow
 ip ospf priority 90
 ipx network 5A
 standby 5 ip 172.21.103.1
 standby 5 priority 150
 standby 5 preempt
 bridge-group 1
!
interface Vlan6
 description VLAN6-SS&PM
 ip address 172.21.102.251 255.255.255.0
```

```
 ip helper-address 172.21.103.9
 no ip redirects
 ip ospf priority 89
 ipx network 6A
 standby 6 ip 172.21.102.1
 standby 6 priority 150
 standby 6 preempt
 bridge-group 1
!
interface Vlan7
 description VLAN7-Group Techology
 ip address 172.21.101.251 255.255.255.0
 ip helper-address 172.21.103.9
 no ip redirects
 ip route-cache flow
 ip ospf priority 90
 ipx network 7A
 standby 7 ip 172.21.101.1
 standby 7 priority 150
 standby 7 preempt
 bridge-group 1
!
interface Vlan8
 description VLAN8-Treasury
 ip address 172.21.100.251 255.255.255.0
 no ip redirects
 ip ospf priority 89
 ipx network 8A
 standby 8 ip 172.21.100.1
 standby 8 priority 150
 standby 8 preempt
```

```
 bridge-group 1
!
interface Vlan9
 description VLAN9-Finance
 ip address 172.21.116.251 255.255.255.0
 ip helper-address 172.21.103.9
 no ip redirects
 ip ospf priority 90
 ipx network 9A
 standby 9 ip 172.21.116.1
 standby 9 priority 150
 standby 9 preempt
 bridge-group 1
!
interface Vlan10
 description VLAN10-Human Resource
 ip address 172.21.117.251 255.255.255.128
 ip helper-address 172.21.103.9
 no ip redirects
 ip ospf priority 89
 ipx network 10A
 standby 10 ip 172.21.117.129
 standby 10 priority 150
 standby 10 preempt
 bridge-group 1
!
interface Vlan11
 description VLAN11-Audit
 ip address 172.21.117.123 255.255.255.128
 ip helper-address 172.21.103.9
 no ip redirects
```

```
 ip ospf priority 90
 ipx network 11A
 standby 11 ip 172.21.117.1
 standby 11 priority 150
 standby 11 preempt
 bridge-group 1
!
interface Vlan12
 description VLAN12-Legal and Compliance
 ip address 172.21.118.123 255.255.255.128
 ip helper-address 172.21.103.9
 no ip redirects
 ip ospf priority 89
 ipx network 12A
 standby 12 ip 172.21.118.1
 standby 12 priority 150
 standby 12 preempt
 bridge-group 1
!
interface Vlan13
 description VLAN13-External Affair
 ip address 172.21.118.155 255.255.255.224
 ip helper-address 172.21.103.9
 no ip redirects
 ip ospf priority 90
 ipx network 20A
 standby 13 ip 172.21.118.129
 standby 13 priority 150
 standby 13 preempt
 bridge-group 1
!
```

```
interface Vlan14
 description VLAN14-Risk Management
 ip address 172.21.118.187 255.255.255.224
 ip helper-address 172.21.103.9
 no ip redirects
 ip ospf priority 89
 ipx network 14A
 standby 14 ip 172.21.118.161
 standby 14 priority 150
 standby 14 preempt
 bridge-group 1
!
interface Vlan15
 description VLAN15-CEO
 ip address 172.21.118.219 255.255.255.224
 ip helper-address 172.21.103.9
 no ip redirects
 ip ospf priority 90
 ipx network 15A
 standby 15 ip 172.21.118.193
 standby 15 priority 150
 standby 15 preempt
 bridge-group 1
!
interface Vlan17
 ip address 172.21.191.69 255.255.255.248
 no ip redirects
 ip route-cache flow
 shutdown
 ipx encapsulation ARPA
 ipx network 1023DB8
```

```
 standby 1 ip 172.21.191.70
 standby 1 priority 100
 standby 1 preempt
!
interface Vlan18
 ip address 172.21.118.228 255.255.255.240
 shutdown
!
interface Vlan92
 description BGK1_DR02
 ip address 10.32.242.6 255.255.255.252
 ip access-group 110 in
!
router ospf 1
 router-id 11.10.1.4
 log-adjacency-changes
 summary-address 192.0.0.0 255.0.0.0
 summary-address 10.0.0.0 255.0.0.0
 passive-interface Vlan17
 passive-interface Vlan18
 passive-interface Vlan92
 network 11.10.0.0 0.0.255.255 area 0
 network 172.21.96.0 0.0.3.255 area 0
 network 172.21.100.0 0.0.0.255 area 0
 network 172.21.101.0 0.0.0.255 area 0
 network 172.21.102.0 0.0.0.255 area 0
 network 172.21.103.0 0.0.0.255 area 0
 network 172.21.104.0 0.0.7.255 area 0
 network 172.21.112.0 0.0.3.255 area 0
 network 172.21.116.0 0.0.0.255 area 0
 network 172.21.117.0 0.0.0.127 area 0
```

```
 network 172.21.117.128 0.0.0.127 area 0
 network 172.21.118.0 0.0.0.127 area 0
 network 172.21.118.128 0.0.0.31 area 0
 network 172.21.118.160 0.0.0.31 area 0
 network 172.21.118.192 0.0.0.31 area 0
 maximum-paths 1
!
router ospf 65010
 log-adjacency-changes
 redistribute ospf 1 metric 10000 subnets route-map PERMIT_ONLY_THAILAND_NET
 passive-interface Vlan1
 passive-interface Vlan2
 passive-interface Vlan3
 passive-interface Vlan4
 passive-interface Vlan5
 passive-interface Vlan6
 passive-interface Vlan7
 passive-interface Vlan8
 passive-interface Vlan9
 passive-interface Vlan10
 passive-interface Vlan11
 passive-interface Vlan12
 passive-interface Vlan13
 passive-interface Vlan14
 passive interface Vlan15
 network 10.32.242.4 0.0.0.3 area 4.0.0.1
 distribute-list PERMIT_ONLY_NON-THAILAND_NET in Vlan92
!
ip classless
ip route 203.155.210.237 255.255.255.255 172.21.103.249
no ip http server
```

```
!
!
ip access-list standard PERMIT_ONLY_NON-THAILAND_NET
 deny   172.21.119.2
 deny   172.21.119.3
 deny   172.21.119.1
 deny   172.21.128.0 0.0.15.255
 deny   172.21.144.0 0.0.15.255
 deny   172.21.104.0 0.0.7.255
 deny   172.21.96.0 0.0.3.255
 deny   172.21.116.0 0.0.0.255
 deny   172.21.117.0 0.0.0.255
 deny   172.21.118.0 0.0.0.127
 deny   172.21.118.128 0.0.0.31
 deny   172.21.118.160 0.0.0.31
 deny   172.21.118.192 0.0.0.31
 deny   172.21.191.56 0.0.0.7
 deny   172.21.191.64 0.0.0.7
 deny   172.21.118.224 0.0.0.15
 deny   166.81.116.0 0.0.0.63
 deny   10.32.64.0 0.0.7.255
 deny   172.21.112.0 0.0.3.255
 deny   172.21.100.0 0.0.3.255
 permit any
ip access list standard PERMIT_ONLY_THAILAND_NET
 permit 172.21.119.2
 permit 172.21.119.3
 permit 172.21.119.1
 permit 172.21.128.0 0.0.15.255
 permit 172.21.144.0 0.0.15.255
 permit 172.21.104.0 0.0.7.255
```

```
 permit 172.21.96.0 0.0.3.255
 permit 172.21.116.0 0.0.0.255
 permit 172.21.117.0 0.0.0.255
 permit 172.21.118.0 0.0.0.127
 permit 172.21.118.128 0.0.0.31
 permit 172.21.118.160 0.0.0.31
 permit 172.21.118.192 0.0.0.31
 permit 172.21.191.56 0.0.0.7
 permit 172.21.191.64 0.0.0.7
 permit 172.21.118.224 0.0.0.15
 permit 166.81.116.0 0.0.0.63
 permit 10.32.64.0 0.0.7.255
 permit 172.21.112.0 0.0.3.255
 permit 172.21.100.0 0.0.3.255
 permit 172.21.120.0 0.0.0.255
 deny   any log
!
logging trap debugging
logging source-interface Vlan1
logging 11.10.1.100
access-list 1 deny   11.0.0.0 0.255.255.255
access-list 1 deny   10.32.0.0 0.0.255.255
access-list 1 permit any
access-list 110 deny   53 any any
access-list 110 deny   55 any any
access-list 110 deny   77 any any
access-list 110 deny   pim any any
access-list 110 deny   tcp any any eq 1433
access-list 110 deny   udp any any eq 1434
access-list 110 deny   udp any eq 1434 any
access-list 110 deny   tcp any any eq 445
```

```
access-list 110 deny   tcp any any eq 4444
access-list 110 deny   tcp any eq 4444 any
access-list 110 permit ip any any
access-list 120 deny   udp any any eq 1434
access-list 120 permit ip any any
access-list 160 deny   ip host 11.10.1.100 10.32.242.0 0.0.0.255
access-list 160 deny   ip host 11.10.1.100 10.63.0.0 0.0.255.255
access-list 160 permit ip any any
route-map PERMIT_ONLY_THAILAND_NET permit 10
 match ip address PERMIT_ONLY_THAILAND_NET
!
route-map PERMIT_ONLY_NON-THAILAND_NET permit 10
 match ip address PERMIT_ONLY_NON-THAILAND_NET
!
snmp-server community scnbmon RO
snmp-server community scnbsup RW
snmp-server enable traps snmp authentication warmstart
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server host 11.10.1.100 scnbmon
!
tacacs-server host 11.10.1.103
tacacs-server key scnbl0ck
bridge 1 protocol dec
banner exec ^CC
AUTHORISED ACCESS ONLY
THIS SYSTEM IS THE PROPERTY OF SCNB
DISCONNECT IMMEDIATELY IF YOU ARE NOT AN AUTHORISED USER !
^C
banner login ^CC
AUTHORISED ACCESS ONLY
```

```
THIS SYSTEM IS THE PROPERTY OF SCNB
DISCONNECT IMMEDIATELY IF YOU ARE NOT AN AUTHORISED USER !
^C
alias configure nlc no logging console
alias configure lc logging console
alias exec sir show ip route
alias exec sion show ip ospf neighbor
alias exec siod show ip ospf database
alias exec srb show run | b
alias exec sri show run | i
privilege exec level 12 show
privilege exec level 1 show startup-config
!
line con 0
 password 7 1515040D132B32
line vty 0 4
 exec-timeout 15 0
 password 7 094F471A1A0A
 authorization exec execauthor
 accounting commands 15 execacc
 accounting exec execacc
 logging synchronous
 login authentication loginauthen
 transport input lat pad mop telnet rlogin udptn nasi
!
ntp clock-period 17179899
ntp peer 11.10.1.1 prefer
ntp peer 11.10.1.2
end
```

ผลงานที่ได้รับการตีพิมพ์

1. ธวัชชัย มะพะสาธุโร กอบชัย เดชหาญ และ ชาลิน สุวรรณวงศ์, "การออกแบบระบบเครือข่ายภายในความเร็วสูงโดยใช้เทคโนโลยีกิกะบิทอีเทอร์เน็ทร่วมกับสวิตช์เลเยอร์3", วิศวสารลาดกระบัง ปีที่ 21 ฉบับที่ 2 เดือนมิถุนายน 2547

ประวัติผู้เขียน

ชื่อ-นามสุกล	นายธวัชชัย มะพะสาธุโร
วัน เดือน ปี เกิด	26 กรกฎาคม พ.ศ. 2512 ที่กรุงเทพมหานคร
ที่อยู่	144/1 ซอยจ่าโสด ถนนสรรพาวุธ แขวงบางนา เขตบางนา กรุงเทพฯ 10260 โทร.0-2398-4777
ประวัติการศึกษา	2535 วิศวกรรมศาสตร์บัณฑิต คณะวิศวกรรมศาสตร์ สาขาวิชาวิศวกรรมอิเล็กทรอนิกส์ มหาวิทยาลัย เอเชียอาคเนย์

ความชำนาญเฉพาะด้าน 1.) ระบบโทรคมนาคม

2.) ระบบเครือข่าย

ประสบการณ์การทำงานและผลงานวิจัย

พ.ศ. 2536 – 2544	ตำแหน่งวิศวกรข่ายสื่อสารข้อมูล ธนาคารกรุงเทพ จำกัด (มหาชน)
พ.ศ. 2544 - ปัจจุบัน	ตำแหน่ง Technical Analyst ธนาคาร สแตนดาร์ดชาร์เตอร์ดนครธน จำกัด (มหาชน)