กลไกควบคุมคุณภาพการให้บริการ โดยใช้ DiffServ-aware Traffic Engineering

MECHANISM CONTROL QOS USING DIFFSERV-AWARE TRAFFIC ENGINEERING

วิรัช ชัยขุนพล
WIRUSH CHAIKUNPOL

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมโทรคมนาคม
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2552

KMITL-2009-EN-M-010-147

กลไกควบคุมคุณภาพการให้บริการ โดยใช้ DiffServ-aware Traffic Engineering

Mechanism Control QoS Using DiffServ-aware Traffic Engineering

วิรัช ชัยขุนพล

WIRUSH CHAIKUNPOL

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์

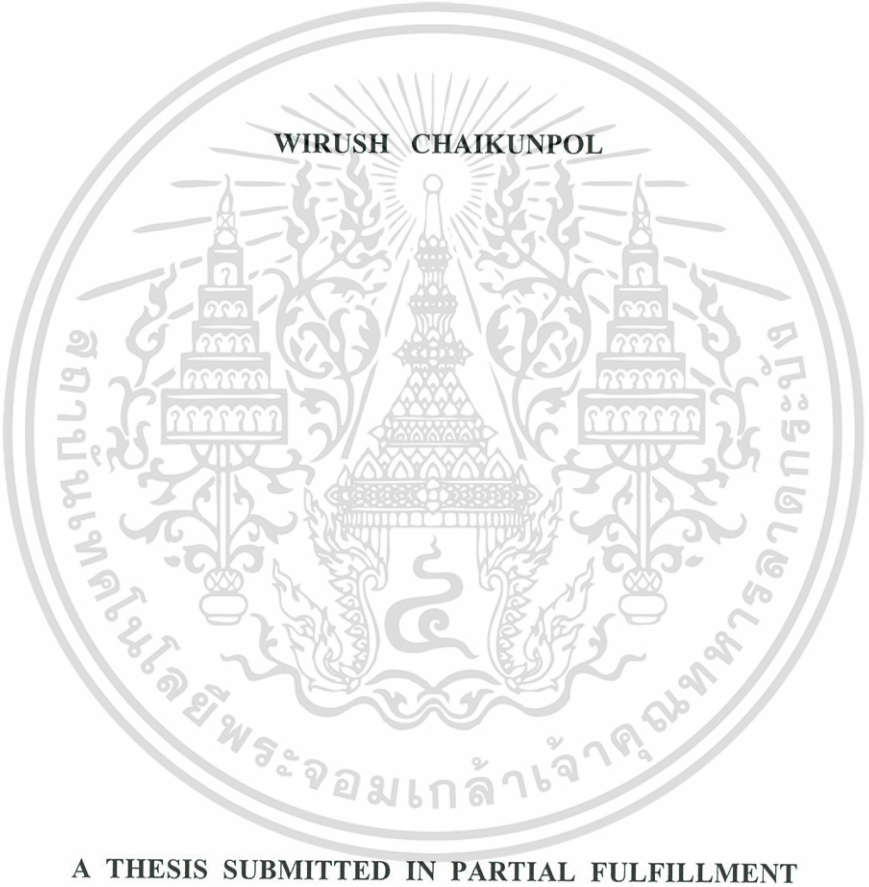
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2552

KMITL 2009-EN-M-010-147

Mechanism Control QoS Using DiffServ-aware Traffic Engineering

WIRUSH CHAIKUNPOL



A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ENGINEERING IN TELECOMMUNICATIONS ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2009

KMITL 2009-EN-M-010-147

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ กลไกควบคุมคุณภาพการให้บริการ โดยใช้ DiffServ-aware Traffic Engineering

Thesis Title Mechanism Control QoS Using DiffServ-aware Traffic Engineering

นักศึกษา นายวิรัช ชัยขุนพล

รหัสประจำตัว 50060926

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมโทรคมนาคม

อาจารย์ที่ปรึกษาวิทยานิพนธ์ รศ.ดร.กอบชัย เดชหาญ

หมายเลขวิทยานิพนธ์ KMITL-2009-EN-M-010-147

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
ดร.สิรภพ	ตู้ประกาย	
รศ.สมยศ	จุณณะปิยะ	
รศ.จิระศักดิ์	ชาญวุฒิธรรม	
รศ.ดร.ฟูศักดิ์	ชีวสุวิทย์	
รศ.ดร.กอบชัย	เดชหาญ	

วัน / เดือน/ ปี ที่สอบ วันศุกร์ที่ 9 ตุลาคม พ.ศ. 2552 เวลา 11.30-13.30 น.

สถานที่สอบ ณ อาคาร A ชั้น 3 ห้องประชุม 1

คณะวิศวกรรมศาสตร์ รับรองแล้ว

(รองศาสตราจารย์ ดร.กอบชัย เดชหาญ)

คณบดี คณะวิศวกรรมศาสตร์

วันที่ 9 ตุลาคม พ.ศ. 2552

หัวข้อวิทยานิพนธ์	กลไกควบคุมคุณภาพการให้บริการ โดยใช้ DiffServ-aware Traffic Engineering
นักศึกษา	นายวิรัช ชัยขุนพล
รหัสนักศึกษา	50060926
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมโทรคมนาคม
พ.ศ.	2552
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รศ.ดร.กอบชัย เดชหาญ

บทคัดย่อ

วิทยานิพนธ์ฉบับนี้เสนอการนำกลไกควบคุม QoS (Quality of Service) ในลักษณะ end-to-end โดยใช้ DS-TE (DiffServ-aware Traffic Engineering) เพื่อควบคุมคุณภาพการให้บริการบนโครงข่าย MPLS ที่มีการรับประกันตามข้อตกลงระดับบริการ (Service Level Agreement) ในด้านคุณภาพของการให้บริการของแอฟปลิเคชั่นประเภท วีดีโอ ในด้านความล่าช้าทางเวลา (Delay), ค่าความแปรผันของความล่าช้าทางเวลา (Jitter) และค่าแพ็กเก็ตที่สูญเสีย (Packet Loss) โดยลักษณะเด่นของวิธีการที่นำเสนอในวิทยานิพนธ์นี้คือ ทดสอบประสิทธิภาพจากระบบที่มีการใช้งานจริง โดยมีการออกแบบ ติดตั้ง และวิเคราะห์ กลไกควบคุม QoS โดยใช้ DS-TE ซึ่งสามารถแสดงให้เห็นประสิทธิภาพการรับประกันคุณภาพของบริการ ในด้านความล่าช้าทางเวลา ค่าความแปรผันของความล่าช้าทางเวลา และแพ็กเก็ตที่สูญหาย แบบ end-to-end ในกรณีที่มีความคับคั่งเกิดขึ้นภายในโครงข่าย ในวิทยานิพนธ์เล่มนี้จะใช้กลไกการทำงานของ DS-TE ในการจัดลำดับความสำคัญของช่อง Video เพื่อควบคุมคุณภาพให้ได้ตามข้อตกลงระดับบริการ ซึ่งในวิทยานิพนธ์เล่มนี้ได้แสดงผลการทดสอบประสิทธิภาพการควบคุมคุณภาพการให้บริการจากการวัดในระบบจริง เพื่อเปรียบเทียบประสิทธิภาพวิธีการที่นำเสนอกับวิธีการแบบเดิม

Thesis Title	Mechanism Control QoS Using DiffServ-aware Traffic Engineering
Student	Mr. Wirush Chaikunpol
Student ID.	50060926
Degree	Master of Engineering
Program	Telecommunications Engineering
Year	2009
Thesis Advisor	Assoc. Prof. Dr. Kobchai Dejhan

ABSTRACT

This thesis proposes a QoS (Quality of Service) controlling mechanism in term of end-to-end by DS-TE (DiffServ-aware Traffic Engineering) with control QoS on MPLS network which committed SLA (Service Level Agreement). A SLA has guaranteed quality of video with delay ,delay jitter and packet loss. The salient feature of this proposal is test performance from real network by designing, implemented and analyzed QoS control mechanism by using DS-TE. Test result can be ability performance for guarantee QoS with latency, jitter and packet loss in case of network congested. This thesis employs the DS-TE set priority of channel-video according to SLA. This thesis presents result of performance test from measurement to control QoS of real network as comparing with that for the conventional mechanism.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้อย่างดีด้วยคำแนะนำ และคำปรึกษาจาก รศ.ดร. กอบชัย เดชหาญ ซึ่งเป็นอาจารย์ผู้ควบคุมวิทยานิพนธ์ ข้าพเจ้ารู้สึกทราบซึ้งในความอนุเคราะห์จากท่านอาจารย์ และขอขอบพระคุณเป็นอย่างสูง

ขอกราบพระคุณคณาจารย์ภาควิชาวิศวกรรมโทรคมนาคม คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ทุก ๆ ท่านที่ได้ประสิทธิ์ประสาทวิชาให้กับข้าพเจ้า

ขอขอบคุณ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ที่ได้สนับสนุนอุปกรณ์และเครื่องมือ ที่ใช้ในการทำวิจัย

ขอขอบคุณเพื่อนๆ พี่ๆ น้องๆ ในภาควิชาวิศวกรรมโทรคมนาคม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ทุกคนที่ให้คำแนะนำต่างๆ และคอยให้กำลังใจเสมอมา

ขอขอบคุณบัณฑิตศึกษา คณะวิศวกรรมศาสตร์ที่ให้ความช่วยเหลือ ในเรื่องต่างๆ

สุดท้ายนี้ข้าพเจ้าขอกราบขอบพระคุณ บิดา มารดา และครอบครัวของข้าพเจ้าที่เป็นกำลังใจและให้การสนับสนุนในทุกเรื่องๆ ทำให้ข้าพเจ้าสามารถทำวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงด้วยดี

คุณค่าและประโยชน์อันพึงมาจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบแด่ผู้มีพระคุณทุกท่าน

วิรัช ชัยขุนพล

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันโครงข่าย MPLS (Multi Protocol Label Switch) ถือเป็นโครงข่ายหลักของผู้ให้บริการโทรคมนาคม เนื่องจาก MPLS สามารถรองรับการใช้งาน Application ประเภท Real Time เช่น Voice over IP (VoIP) และ Video on Demand (VoD) นอกเหนือจากข้อมูล (Data) พื้นฐานทั่วไป ซึ่งบริการ VoIP และ VoD ต้องอาศัยกลไกในการควบคุมคุณภาพของการให้บริการ (Quality of Service - QoS) ซึ่งโดยปกติทางเทคนิคจะประกอบไปด้วยค่าแพ็กเก็ตที่สูญเสีย (Packet Loss), ค่าความล่าช้าทางเวลา (Latency หรือ Delay) และค่าแปรผันหน่วงเวลา (Jitter) ซึ่งเป็นพารามิเตอร์ที่สำคัญของ Application ประเภท Real Time ความต้องการคุณภาพของการให้บริการที่ต้องการ การรับประกัน (Assured Forwarding) แบบ end-to-end ให้ได้ตามข้อตกลงของระดับการให้บริการ (Service Level Agreement - SLA) โดยในขณะที่โครงข่าย MPLS เกิดความคับคั่ง การควมคุม QoS ต้องอาศัยกลไกควบคุม QoS ควบคุมการไหลของแต่ละ Application ที่เป็นประเภท Real Time ให้อยู่ในสภาวะที่คงที่หรือมีผลกระทบน้อยที่สุด ซึ่งปัญหาที่เกิดขึ้น หากกลไกควบคุม QoS ไม่สามารถควบคุม QoS ได้ จำนวนค่าการสูญเสียของแพ็กเก็ต การล่าช้าทางเวลา และค่าแปรผันหน่วงเวลาจะเพิ่มขึ้นทั้งหมด ส่งผลให้คุณภาพของ Application แบบ Real Time ลดต่ำลง และไม่สามารถรับประกันได้ตามข้อตกงของระดับการให้บริการ

กระบวนการควบคุมคุณภาพการให้บริการภายในโครงข่าย MPLS นั้นหลัก ๆ จะมีอยู่ 2 วิธีได้แก่ Per-Hop Behavior (PHB) และ DiffServ-aware Traffic Engineering (DS-TE) โดยสำหรับ PHB นั้นจะมีการรับประกันคุณภาพการให้บริการในลักษณะฮอบต่อฮอบ ไม่สามารถรับประกันคุณภาพการให้บริการในลักษณะ end-to-end ได้ แต่มีข้อดีที่สามารถใช้กับโครงข่ายขนาดใหญ่ได้อย่างดี ในขณะที่ DS-TE นั้นมีการจองขนาดช่องสัญญาณ (Bandwidth) ตามระดับการให้บริการได้โดยการใช้ ReSource ReserVation Protocol (RSVP) ทำให้สามารถรับประกันคุณภาพการให้บริการแบบ end-to-end ได้ แต่ความซับซ้อนในการใช้งานก็จะสูงกว่า PHB ทำให้อาจจะไม่สามารถใช้กับโครงข่ายขนาดใหญ่ได้ดีนัก อย่างไรก็ตามข้อสรุปทั้งหมดนี้ส่วนใหญ่มักเกิดจากการจำลองการทำงานด้วยคอมพิวเตอร์หรือการพิสูจน์ทางคณิตศาสตร์ ยังขาดการพิสูจน์โดยการวัดจากระบบที่มีการใช้งานจริง จึงเป็นแนวความคิดของวิทยานิพนธ์ฉบับนี้ที่จะออกแบบติดตั้ง และวิเคราะห์วิธีการควบคุมระดับการให้บริการแบบ PHB และ DS-TE โดยเฉพาะอย่างยิ่งในกรณีที่เกิดความคับคั่งขึ้นภายในโครงข่าย ผลการทดสอบยืนยันว่าการควบคุมคุณภาพการ

ให้บริการด้วย DS-TE สามารถควบคุมความล่าช้าทางเวลา ค่าความแปรผันของความล่าช้าทางเวลา และแพ็กเก็ตที่สูญหาย ได้ดีกว่าวิธี PHB ในกรณีที่มีความคับคั่งเกิดขึ้นภายในโครงข่าย

อย่างไรก็ตามข้อสรุปข้างต้นส่วนใหญ่มักสรุปจากผลการจำลองการทำงาน (Simulation) หรือการพิสูจน์ทางคณิตศาสตร์เท่านั้น ยังขาดข้อมูลผลการจำลองสถานะการณ์ความคับคั่งภายในระบบจริง และตรวจวัดคุณภาพของการให้บริการจากเครื่องมือวัดจริง ซึ่งถ้าผลการวัดสามารถยืนยันผลการจำลองการทำงานหรือการพิสูจน์ทางคณิตศาสตร์ จะทำให้ผู้ให้บริการโทรคมนาคมสามารถใช้เป็นข้อมูลเพื่อออกแบบระบบโครงข่าย MPLS ที่สามารถให้บริการ Application ที่เป็น Real-Time ร่วมกับข้อมูล โดยสามารถรับประกันคุณภาพของการให้บริการได้ตาม SLA ต่อไป

1.2 วัตถุประสงค์ของงานวิจัย

1. เพื่อออกแบบและติดตั้งระบบเพื่อวัดผลของปริมาณทราฟฟิคในระบบ LAN ที่มีผลต่อคุณภาพของการให้บริการในโครงข่าย MPLS
2. เพื่อเปรียบเทียบประสิทธิภาพของวิธีการควบคุม QoS ด้วยวิธี DS-TE, PHB และ BE โดยใช้ตัวแปรคือ Packet Loss, Delay และ Jitter

1.3 สมมติฐานของการศึกษา

ปัจจุบันโครงข่ายของผู้ให้บริการโทรคมนาคมและผู้ให้บริการอินเตอร์เน็ตมีการปรับเปลี่ยนจากระบบเดิมที่ใช้กันมายาวนาน โดยระบบโครงข่ายหลัก (Core network) ของผู้ให้บริการเดิมจะใช้เทคโนโลยี Synchronous Digital Hierarchy (SDH) และอาจจะใช้ร่วมกับเทคโนโลยี Internet Protocol (IP) ในลักษณะ IP over SDH ซึ่งข้อดีหลักของระบบนี้คือตัวโครงข่ายหลัก (SDH) สามารถใช้ส่งข้อมูลได้ทั้งแบบ Time Division Multiplexing (TDM) และ IP ได้พร้อมกัน นอกจากนั้นยังสามารถควบคุมคุณภาพของการให้บริการได้เป็นอย่างดี เนื่องจากคุณลักษณะของระบบ SDH เอง อย่างไรก็ตามเนื่องจากปริมาณการใช้งานข้อมูล (Data) ในโครงข่ายของผู้ให้บริการมีปริมาณเพิ่มขึ้นอย่างมาก ทำให้ลักษณะการส่งข้อมูลในโครงข่ายแบบ IP over SDH นั้นไม่สามารถตอบสนองตามความต้องการได้ เนื่องจากปัญหาคอขวดของระบบ SDH โดยแนวโน้มของผู้ให้บริการโทรคมนาคมและผู้ให้บริการอินเตอร์เน็ตทั่วโลกต่างก็ปรับเปลี่ยนไปเป็นในรูปแบบของ IP over Fiber หรือ IP over DWDM (Dense Wavelength Division Multiplexing) และข้อมูลที่ใช้งานในโครงข่ายทั้งหมดไม่ว่าจะเป็นภาพ เสียง หรือข้อมูลคอมพิวเตอร์ก็จะถูกปรับเปลี่ยนให้มาใช้งานบนเทคโนโลยี IP เป็นหลัก

การใช้เทคโนโลยี IP over Fiber หรือ IP over DWDM นั้นจำเป็นต้องมีการควบคุมคุณภาพของการให้บริการ โดยเฉพาะกับข้อมูลที่เป็นภาพและเสียงเนื่องจากค่อนข้างจะได้รับผลกระทบจากความล่าช้าทางเวลา และค่าความแปรผันของการล่าช้าทางเวลา ค่อนข้างมาก ใน

โครงข่ายที่ขาดการจัดการควบคุมคุณภาพของการให้บริการที่เหมาะสม ค่าความล่าช้าทางเวลาและค่าความแปรผันของการล่าช้าทางเวลาของข้อมูลภาพและเสียง (ซึ่งมักจะเป็นแพ็กเก็ตขนาดสั้นเป็นหลัก) จะได้รับผลกระทบอย่างมากจากการส่งข้อมูลคอมพิวเตอร์ (ซึ่งมักจะเป็นแพ็กเก็ตขนาดยาวเป็นหลัก) ดังนั้นเมื่อมีการใช้งานข้อมูลทั้งหมดร่วมกันในโครงข่าย การควบคุมคุณภาพของการให้บริการจึงเป็นสิ่งที่สำคัญมาก

1.4 ทฤษฎีหรือแนวคิดที่ใช้ในการวิจัย

โครงข่าย IP ซึ่งเป็นโครงข่ายหลักของผู้ให้บริการในปัจจุบันจะใช้ร่วมกับเทคโนโลยี MPLS (MultiProtocol Label Switch) เนื่องจากต้องการความเร็วในการส่งข้อมูลปริมาณมากจากต้นทางไปถึงปลายทาง โดยสามารถควบคุมคุณภาพของการให้บริการได้ โดยในช่วงแรกของการวิจัยนั้นจะมีแนวทางในการควบคุมคุณภาพของการให้บริการได้ 2 รูปแบบคือ Integrated Service (IntServ) และ Differentiated Service (DiffServ) อย่างไรก็ตามหลาย ๆ บทความวิจัยได้ชี้ให้เห็นว่าการควบคุมคุณภาพของการให้บริการแบบ DiffServ นั้นมีความเหมาะสมที่จะใช้งานกับโครงข่ายขนาดใหญ่และมีผู้ใช้งานจำนวนมากได้ดีกว่าแบบ IntServ ดังนั้นในโครงข่ายจริงของผู้ให้บริการในปัจจุบัน ส่วนใหญ่จะใช้รูปแบบการควบคุมคุณภาพของการให้บริการแบบ DiffServ เป็นหลัก

อย่างไรก็ตาม การควบคุมคุณภาพของการให้บริการแบบ DiffServ ก็มีรูปแบบการใช้งานในลักษณะที่มีการควบคุมคุณภาพการให้บริการแบบ Hop by Hop (หรือ Per Hob Behavior) หรือมีการควบคุมคุณภาพการให้บริการแบบ end-to-end (หรือ DiffServe-aware Traffic Engineering – DS-TE) ซึ่งวิทยานิพนธ์ฉบับนี้จะเปรียบเทียบการควบคุมคุณภาพการให้บริการด้วยวิธีทั้งสองเป็นหลัก โดยจะเปรียบเทียบจากผลการวัดในระบบจริง

1.5 การเปรียบเทียบระหว่างวิธีการที่นำเสนอกับวิธีการแบบพื้นฐาน

งานวิจัยที่เกี่ยวข้องรวมถึงข้อสรุปจากบทความต่าง ๆ มักจะเกิดจากผลการจำลองการทำงานด้วยโปรแกรมคอมพิวเตอร์ (Computer Simulation) และ/หรือการพิสูจน์ด้วยคณิตศาสตร์เป็นหลัก ยังขาดการวัดและสรุปผลการเปรียบเทียบการควบคุมคุณภาพของการให้บริการด้วยวิธี DS-TE และ PHB จากการใช้งานในโครงข่ายจริง โดยการทดลองในวิทยานิพนธ์ฉบับนี้จะมีการทดสอบการรับ-ส่งข้อมูลวีดีโอที่มีการกำหนดระดับของการให้บริการ (Service Level Agreement – SLA) ในระดับที่แตกต่างกัน และมีการส่งข้อมูล (Data) ในลักษณะที่มีการ burst ข้อมูลเพื่อทำให้เกิดความคับคั่งในบางช่วงเวลาของโครงข่าย วิทยานิพนธ์ฉบับนี้จะเปรียบเทียบประสิทธิภาพของวิธีการควบคุมคุณภาพของการให้บริการแบบ DS-TE, PHB และ BE โดยจะเปรียบเทียบกันด้วยจำนวนแพ็กเก็ตที่สูญเสีย ความล่าช้าทางเวลา และการแปรผันของการล่าช้าทางเวลา

1.6 ขอบเขตการวิจัย

วิทยานิพนธ์ฉบับนี้มีขอบเขตการวิจัย ดังนี้

1. ติดตั้งระบบและกำหนดค่า (Configuration) โครงข่ายจำลองที่สามารถรับ-ส่งข้อมูลและช่อง Video ในเครือข่าย MPLS ทำงานในระบบ LAN โดยสามารถกำหนดคุณภาพของการให้บริการสำหรับภาพได้อย่างน้อย 3 ระดับการให้บริการ ได้แก่ Gold, Silver และ Bronze Service
2. คุณภาพของการให้บริการสำหรับช่อง Video จะมีการเปรียบเทียบระหว่างวิธี DS-TE และ PHB ในการควบคุมคุณภาพการให้บริการ
3. ปรับอัตราการส่งข้อมูลเพื่อให้ระบบทำงานในสถานะ Underload และ Overload ในแต่ละช่วงเวลา
4. เก็บผลและเปรียบเทียบประสิทธิภาพในการควบคุมคุณภาพของการให้บริการด้วยวิธี DS-TE, PHB และ BE ตามลำดับ

1.7 ขั้นตอนของการศึกษา

วิทยานิพนธ์ฉบับนี้ได้แบ่งเนื้อหาออกเป็น 5 บทด้วยกันคือ

บทที่ 1 กล่าวถึงความเป็นมาของงานวิจัย ความมุ่งหมายและวัตถุประสงค์ สมมติฐาน ทฤษฎีที่ใช้ ขอบเขตของการวิจัย และขั้นตอนการศึกษา

บทที่ 2 กล่าวถึงทฤษฎีพื้นฐานที่ใช้ในการวิจัย และพื้นฐานของการควบคุมคุณภาพของการให้บริการในโครงข่าย MPLS ซึ่งประกอบด้วยเทคนิคแบบ DS-TE และ PHB

บทที่ 3 กล่าวถึงรูปแบบของโครงข่ายที่ได้ออกแบบเพื่อทดสอบประสิทธิภาพของเทคนิคในการรับประกันคุณภาพการให้บริการแบบต่าง ๆ รวมถึงวิธีการติดตั้งค่าพารามิเตอร์ต่าง ๆ ในระบบ

บทที่ 4 กล่าวถึงผลการตรวจวัดค่าแพ็กเก็ตที่สูญเสีย ความล่าช้าทางเวลา และค่าแปรผันหน่วงเวลา ที่ได้จากการวัดในระบบจริง

บทที่ 5 เป็นบทสรุปผลการวิจัยและข้อเสนอแนะสำหรับงานวิจัยในอนาคต

บทที่ 2
ทฤษฎีพื้นฐานที่เกี่ยวข้องกับการวิจัย

ในบทนี้จะกล่าวถึงทฤษฎีพื้นฐานต่าง ๆ ที่เกี่ยวข้องในการวิจัย และพื้นฐานของการจัดการคุณภาพของการให้บริการแบบ Per Hop Behavior (PHB) และ DiffServ-aware Traffic Engineering (DS-TE) ซึ่งเนื้อหาทั้งหมดนี้จำเป็นสำหรับการศึกษา และประเมินประสิทธิภาพของโครงข่าย MPLS สำหรับการให้บริการ

2.1 โครงข่าย Multi Protocol Label Switch (MPLS)

เป็นโปรโตคอลที่ถูกพัฒนาขึ้นมาโดย The Internet Engineering Task Force (IETF) เพื่อให้การส่งต่อข้อมูลโดย IP แพ็กเก็ตนั้นลดกระบวนการต่าง ๆ (เช่นกระบวนการในการหาเส้นทาง) ลง ให้คล้ายกับการส่งข้อมูลด้วยสวิตช์ และยังช่วยให้หน่วยประมวลผลหรือซีพียูของอุปกรณ์ทำงานลดลงตามไปด้วย สุดท้ายผลที่ได้คือ สามารถลดความล่าช้าทางเวลาในการส่งข้อมูลจากจุดหนึ่งไปอีกจุดหนึ่ง และสามารถส่งข้อมูลได้ปริมาณมากขึ้น

โดยปกติการรับส่งข้อมูลด้วยเราเตอร์ที่ใช้ IP แพ็กเก็ตในการรับส่งข้อมูลนั้น จะมีส่วนหัวของแพ็กเก็ตที่ระบุที่อยู่ของต้นทางและปลายทาง การส่งต่อของแพ็กเก็ตจากต้นทางไปยังปลายทางสามารถเกิดความล่าช้าขึ้นได้ ปัญหาความล่าช้าที่สามารถเกิดขึ้นได้จากความเร็วในการค้นหาเส้นทางของที่อยู่ปลายทางของเราเตอร์ ไปจนถึงขั้นตอนและวิธีการส่งต่อ แพ็กเก็ตจากอุปกรณ์ตัวหนึ่งไปยังอีกตัวหนึ่ง

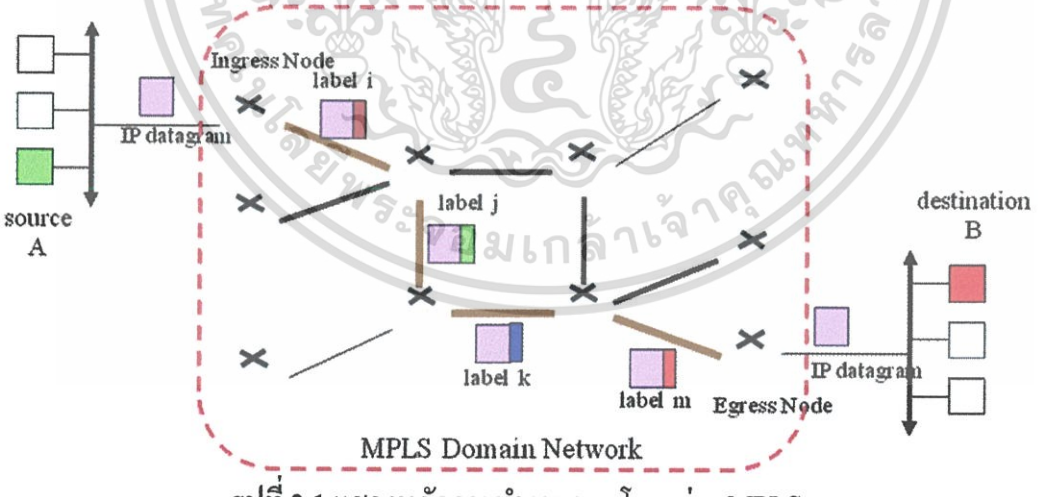
กระบวนการของ MPLS นั้นได้เพิ่มขั้นตอนอย่างหนึ่งเข้าไปใน IP แพ็กเก็ตเพื่อให้การส่งต่อแพ็กเก็ตเร็วขึ้น คือการใส่ป้ายชื่อหรือ Label เข้าไป การใส่ป้ายชื่อนี้เปรียบเสมือนกับการใส่รหัสไปรษณีย์เพิ่มเข้าไปในหน้าซองจดหมาย ผู้คัดแยกจดหมายไม่จำเป็นต้องดูว่าผู้รับเป็นใครเพียงแต่แยกว่ารหัสไปรษณีย์รหัสไหนจะส่งต่อไปภาคไหน หรือจังหวัดไหนเท่านั้น จะเห็นได้ว่าการเพิ่มขั้นตอนเพียงบางส่วนเข้าไป จะสามารถไปลดเวลาการทำงานโดยรวมให้น้อยลงได้ แนวความคิดแบบนี้คล้ายกับวิธีการของ MPLS ที่เกิดขึ้นมาก็เพื่อลด Overhead ในการใช้งาน Virtual Circuit บนเครือข่าย TCP/IP ลงให้มากที่สุด ซึ่งจะเป็นการผนวกโครงข่าย Asynchronous Transfer Mode (ATM) ซึ่งเป็นเครือข่ายแบบ Virtual Circuit Switching และใช้ ATM Switch ในเลเยอร์ที่ 2 เป็นหลัก เข้ากับเครือข่าย TCP/IP ซึ่งเป็นเครือข่ายแบบ Packet Switching และใช้ Router ในเลเยอร์ที่ 3 เป็นหลักเข้าด้วยกัน ประโยชน์ที่ได้รับก็คือการทำวิศวกรรมควบคุมการจราจรบนเครือข่ายที่มีประสิทธิภาพ จากเดิมที่โปรโตคอลสำหรับการกำหนดเส้นทางส่วนใหญ่ในเครือข่ายจะมองในส่วนของระยะทางเป็นหลัก แต่สำหรับ MPLS แล้ว จะมองที่

ความสามารถในการไหลไปยังปลายทางของข้อมูลเป็นหลักแทน และมีกระบวนการกำหนดเส้นทางที่ฉลาดว่าผสมกับการใช้งานแบบ Virtual Circuit ที่มีลักษณะการส่งแบบ Streamline แทนการส่งแบบ Connectionless ทำให้สามารถแก้ปัญหาการจราจรบนเครือข่ายได้เป็นอย่างดี

เนื่องจาก MPLS มีการส่งแบบ Streamline ทำให้สามารถรับประกันเกี่ยวกับปริมาณข้อมูลต่อเวลาได้เป็นอย่างดี เพื่อใช้งานในลักษณะ Real-Time เช่น การถ่ายทอดภาพและเสียงผ่านเครือข่ายอินเตอร์เน็ต ได้โดยทั้งภาพและเสียงมีคุณภาพใกล้เคียงกับ คุณภาพที่ได้จากการชมโทรทัศน์หรือฟังวิทยุเลยทีเดียว รวมทั้งสามารถที่จะกำหนดระดับของ QoS ให้เหมาะกับผู้ใช้งานแต่ละรายได้โดยง่าย สามารถใช้งานเป็น Tunnel ให้ VPN ได้เป็นอย่างดี เนื่องจาก ISP ที่ต้องการให้บริการ VPN กับลูกค้าของตนสามารถกำหนด Virtual Circuit ระหว่าง ISP กับลูกค้าเพื่อเพิ่มคุณภาพให้กับ Tunnel แทน VPN แบบเดิม ๆ ที่วิ่งไปบนเครือข่ายแบบไม่มีทิศทาง เนื่องจากใช้งานแบบ Connectionless นั่นเอง สนับสนุนโปรโตคอลได้หลากหลาย ปัจจุบันนอกจากที่สนับสนุนเครือข่าย TCP/IP แล้วยังสามารถนำ MPLS ไปใช้กับเครือข่าย ATM และ Frame Relay หรือแม้กระทั่งใช้บนเครือข่ายทั้งสามซึ่งทำ Overlay Network กันอยู่ก็ได้

หลักการทำงานของ MPLS

โดยทั่วไปแล้วโครงข่าย MPLS จะมีหลักการทำงานดังแสดงในรูปที่ 2.1



รูปที่ 2.1 แสดงหลักการทำงานของโครงข่าย MPLS

หลักการทำงานของ MPLS โดยสังเขปคือการสร้างระบบจัดเส้นทางของ Packet หรือการ Routing ขึ้นใหม่ภายในบริเวณของเครือข่ายที่กำหนด ซึ่งจะขอเรียกเส้นทางนี้ว่า LSP (Label Switch Path) โดยภายนิขอบเขตนี้ Packet ที่วิ่งเข้ามาจะถูกกำหนด Label ประจำตัวให้ใหม่ (โดย Ingress Node) โดยไม่สนใจ Header เดิม (ของ TCP/IP) จากนั้นจึงวิ่งไปตามเส้นทางที่กำหนดไว้ใน LSP สำหรับ Label ชุดนั้นๆ ซึ่งเส้นทางนี้เป็นไปได้ทั้งการกำหนดตายตัวล่วงหน้า

และการกำหนดแบบเปลี่ยนแปลงไปเรื่อย ๆ ตามความเหมาะสม ซึ่งมีความซับซ้อนมากกว่าโปรโตคอลในการกำหนดเส้นทางของข้อมูลที่ใช้อยู่เดิมในเครือข่าย TCP/IP เช่นมีการคำนวณจากจำนวน hop ที่ส่งคำนวณจากเวลาที่ใช้น้อยที่สุด หรือพยายามให้ได้ตามเวลาจริง (Real-Time) เช่นสำหรับการส่งข้อมูลมัลติมีเดียและอื่นๆอีกมาก การทำงานจะทำได้เร็วกว่า Routing แบบเดิม เพราะ การคำนวณเพื่อจัดเส้นทางจะทำไว้ล่วงหน้า และเป็นอิสระจากการรับส่งข้อมูลแต่ละ Packet คือมีหน้าที่จัดเส้นทางใหม่ก็จัดไป เมื่อจัดเสร็จก็เก็บไว้ใช้งาน ส่วนหน้าที่รับส่งข้อมูลก็ทำไปเช่นกันไม่ยุ่งเกี่ยวกัน เมื่อมีข้อมูลเข้ามาถึงจะนำเส้นทางที่ได้เตรียมไว้มาใช้รับส่งข้อมูล เมื่อข้อมูลวิ่งมาถึงปลายสุดของ LSP ก็จะนำ Label ออกจาก Packet โดย Egress Node และปล่อยให้เป็นหน้าที่ของ Header เดิมของ Packet ทำหน้าที่นำข้อมูลส่งถึงปลายทางที่แท้จริง

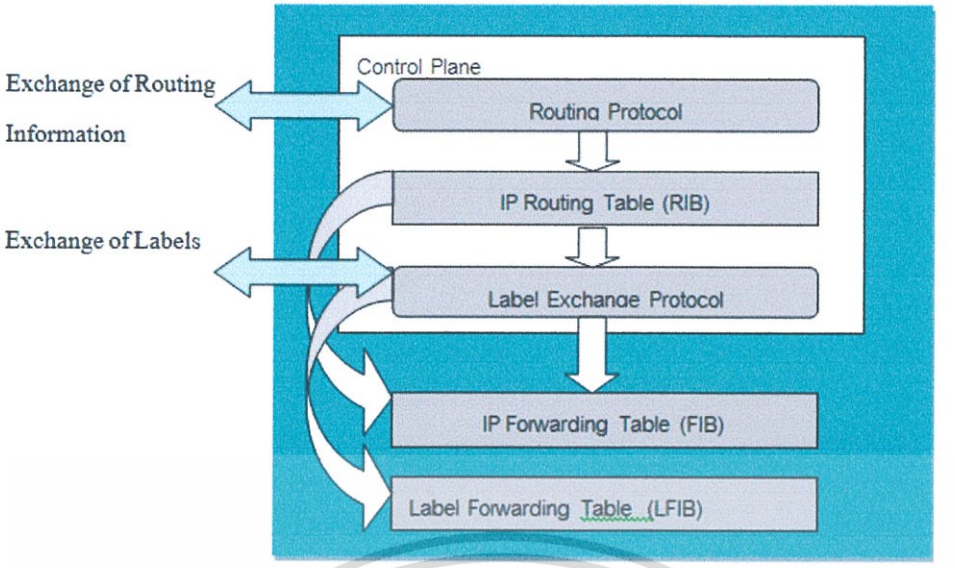
2.1.1 Architectural Components of MPLS

ประกอบด้วย 2 ส่วนประกอบหลักคือ

- **Control Plane** ทำหน้าที่ในควบคุมกระบวนการในการแลกเปลี่ยน Routing Information และ Label ระหว่างอุปกรณ์ที่อยู่ข้างเคียง Control Plane สร้าง Routing Table จาก Routing Protocol หลาย ๆ Routing Protocol เช่น Open Shortest Path First (OSPF) Interior Gateway Routing Protocol(IGRP) Enhanced Interior Gateway Routing Protocol (EIGRP) Intermediate System-to-Intermediate System (IS-IS) Routing Information Protocol (RIP) และ Border Gateway Protocol (BGP) สามารถใช้ใน Control Plane เพื่อควบคุมจัดการกับ Layer 3 Routing นอกจากนี้ Control Plane ยังใช้ Label Exchange Protocol ในการกำหนดและแลกเปลี่ยน Label ระหว่างอุปกรณ์ที่อยู่ข้างเคียง โดย Label Exchange Protocol กำหนดค่า Label ให้กับ Network โดยการเรียนรู้ผ่าน Routing Protocol ซึ่ง Label Exchange Protocol ประกอบด้วย MPLS Label Distribution Protocol (LDP) และ BGP (ใช้สำหรับ MPLS VPN) ส่วน Resource Reservation Protocol (RSVP) ใช้สำหรับ MPLS TE ในการแลกเปลี่ยน Label.

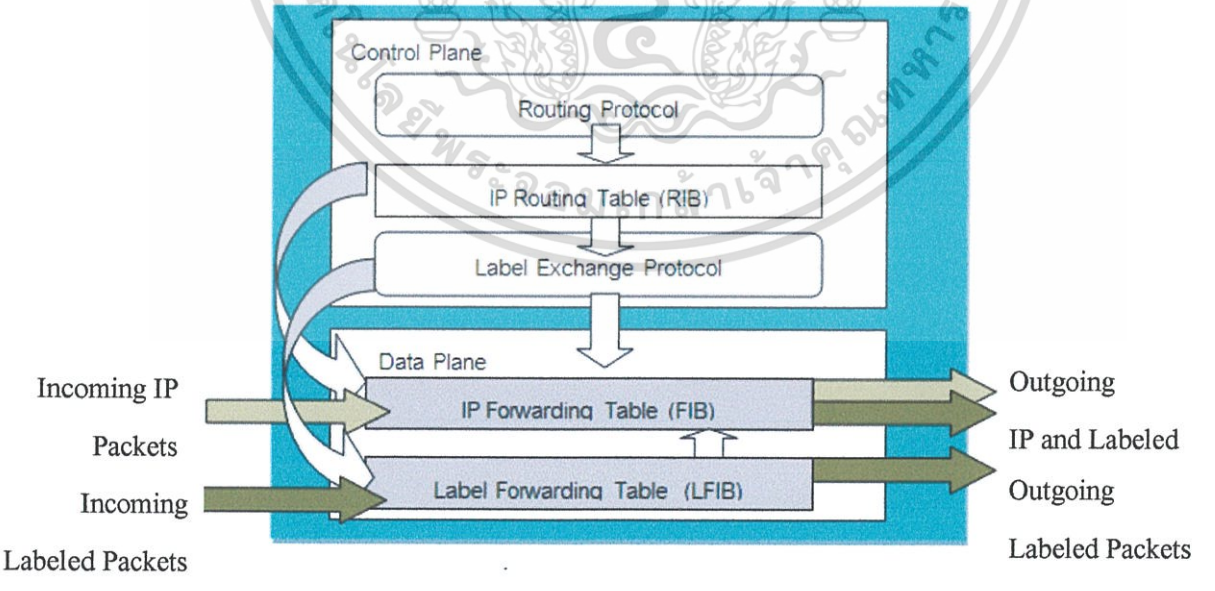
Control Plane ประกอบด้วย Forwarding Table 2 ชนิดคือ

a) FIB ข้อมูลในการสร้าง Table ได้มาจาก RIB
b) Label Forwarding Information Base (LFIB) ข้อมูลในการสร้าง Table มาจาก Label Exchange Protocol และ RIB ซึ่งใน LFIB Table ประกอบด้วยค่า Label ที่สอดคล้องกับ Outgoing Interface สำหรับทุกๆ Network Prefix



รูปที่ 2.2 MPLS Architecture Control Plane

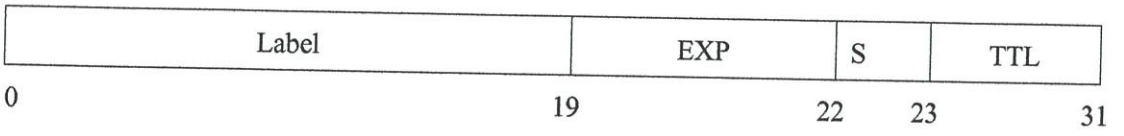
- **Data Plane** - ทำหน้าที่ในการส่ง Packet ข้อมูลโดยสามารถส่ง Packet ด้วย Layer 3 IP packets หรือ Label IP Packet ข้อมูลที่อยู่ใน Data Plane เช่น Label Values ได้มาจาก Control Plane ข้อมูลที่ได้มาจากการแลกเปลี่ยนกันระหว่าง Router ข้างเคียงซึ่งนำมา Mapping กับข้อมูลของ IP Destination Prefixes และ Label ใน Control Plane ซึ่งนำมาใช้ในการ Forward Data Plane Label Packets



รูปที่ 2.3 MPLS Architecture Data Plane

2.1.2 MPLS Labels and Label Stacks

MPLS Labels มีขนาด 20 bit และถูกกำหนดเป็น Prefix แบบปลายทางด้วยการกำหนดบน Router กำหนดคุณสมบัติเพื่อให้มีการนำส่งข้อมูลสำหรับส่งไปยังปลายทางได้ด้วยรูปแบบ MPLS Label ที่แสดงในรูปที่ 2.4



รูปที่ 2.4 MPLS Label

MPLS Label ประกอบไปด้วย

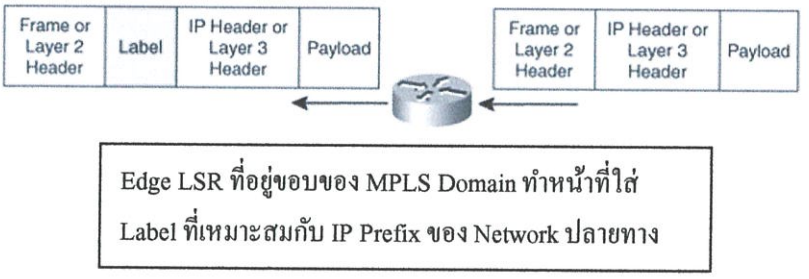
- 20 bit เป็นค่า Label
- 3 bit เป็นค่า Experimental filed
- 1 bit เป็นตัวแสดงว่าเป็น Bottom-of-Stack
- 8 bit เป็นส่วนตรวจสอบ Time-to-Live Field

20 bit แรกเป็นค่าที่กำหนดโดย Router ด้วยการ Identifies Prefix โดย Labels สามารถกำหนดด้วย Interface หรือกำหนดด้วย Chassis ส่วน Experimental bit จะกำหนด QoS ที่ได้รับจาก IP Packet ซึ่งกำหนดไว้แล้วด้วย Label โดย Experimental Bit สามารถ Map กับค่า IP Precedence เพื่อกำหนดค่า IP QoS ของ Packet ที่อยู่ใน MPLS Domain

Label Stack คือ Label ที่มีคุณสมบัติพิเศษที่บอกถึงลักษณะของ Label ถ้า Router (Edge LSR) มีการใส่ Label มากกว่า 1 Label บน IP Packet เดียว ซึ่งเรียกว่า Label Stack ดังนั้นการจะรู้ได้ว่ามีการใส่ Label มากกว่า 1 Label ใน IP Packet เดียวโดยดูจาก Bottom-of-Stack Indicator ซึ่ง Label ตัวสุดท้าย (Bottom Label) ค่าของ Bottom-of-Stack Indicator จะถูกตั้งค่าเป็น 1

TTL จะเหมือนค่า Function TTL ของ IP ซึ่ง Packet จะถูกละทิ้งเมื่อค่า TTL เป็น 0 เพื่อเป็นการป้องกันการเกิด Loop เมื่อใดก็ตามที่ Packet ถูกส่งไปตามเส้นทางของ LSR ค่า Label TTL จะลดลงทีละ 1

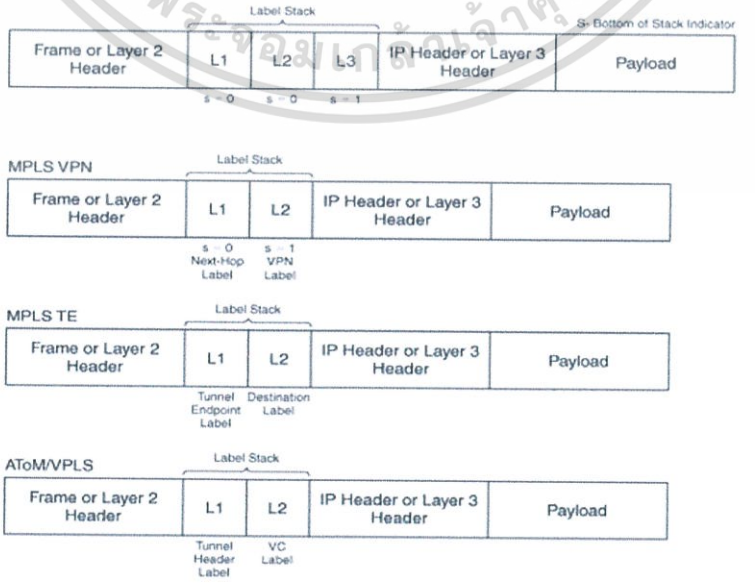
Label จะถูกใส่เพิ่มเข้าไประหว่าง Frame Header และ Layer 3 Header รูปที่ 7 แสดงให้เห็นการเพิ่ม Label เข้าไปใน Layer 2 และ Layer 3 header ใน IP Packet



รูปที่ 2.5 MPLS Label Imposition

ถ้าค่าของ S bit (ค่า Label ตัวสุดท้าย) ใน Label มีค่าเป็น 0 Router จะเข้าใจว่ามีการใช้งาน Label Stack โดย LSR จะเปลี่ยนเฉพาะ Label บนสุด ใน Label Stack อย่างไรก็ตาม Edge LSR จะทำการถอด Label ต่อไปจนกระทั่งพบว่าค่า S bit มีค่าเป็น 1 ซึ่งเป็นเครื่องหมายแสดงว่าเป็น Label สุดท้าย หลังจาก Router ได้รับ Stack ค่าสุดท้าย Router จะพบกับค่า IP Layer 3 Header และปลายทางที่เหมาะสมที่สุดในการส่ง Packet ในกรณี ของ Ingress Edge LSR ซึ่งอาจจะมีการใส่ Label เข้าไปมากกว่า 1 Label Stack ตรง Stack Function

Label Stack เป็นเครื่องมือเพื่อให้บริการ MPLS-Base เช่น MPLS VPN หรือ MPLS Traffic Engineering ใน MPLS VPN Label ที่สองใน Label Stack จะกำหนดค่า VPN ส่วน MPLS Traffic Engineering Label บนสุด(Top Label) จะกำหนดจุดสิ้นสุดของ TE Tunnel และ Label ที่สอง(Bottom Label) จะกำหนดปลายทาง สำหรับการทำ MPLS Layer 2 VPN เช่น AToM และ VPLS Label บนสุด (Top Label) เป็น Tunnel Header หรือ Endpoint, และ Label ที่สอง (Bottom Label) จะกำหนด VC ที่กล่าวมาทั้งหมดแสดงในรูปที่ 2.6



รูปที่ 2.6 MPLS Label Stack

2.1.3 จุดเด่นของโครงข่าย MPLS

- มีความเร็วและความปลอดภัยสูงในการรับ-ส่งข้อมูล
- สามารถส่งข้อมูลด้วยช่องสัญญาณ (Bandwidth) สูงสุดถึง 10 Gbps
- ในการใช้งานสามารถเลือกความเร็วได้ตั้งแต่ 64 Kbps-1 Gbps
- รองรับ IP Applications ต่าง ๆ ไม่ว่าจะเป็น VoIP, Routing Protocol, QoS, Multicast และ VDO Conference เพื่อตอบสนองชีวิตการทำงาน แบบที่จะเป็นที่นิยมในอนาคต โดยการรวมเทคโนโลยีต่างๆ ไว้เข้าด้วยกัน เพื่ออำนวยความสะดวกในการทำงาน

2.2 การรับประกันคุณภาพของการให้บริการ (QoS) ในโครงข่าย MPLS

QoS (Quality of Service) เป็นมาตราที่ใช้ในการวัดการรับส่งข้อมูล การยอมรับในเรื่องคุณภาพ ซึ่งเป็นระดับที่บางครั้งก็ยากแก่การกำหนดว่า มาตรฐานคุณภาพบนอินเทอร์เน็ตเป็นอย่างไร แต่หากพิจารณา QoS ในเชิงเทคนิค พอจะนิยามได้ด้วยพารามิเตอร์ดังต่อไปนี้

การมีให้ใช้งานได้ (Availability) ในทางอุดมคติต้องได้ 100 เปอร์เซ็นต์ของเวลาการใช้งาน หรือกล่าวได้ว่า เวลาที่ไม่สามารถใช้งานระบบได้ (Downtime) มีค่าเป็นศูนย์ แต่ในทางปฏิบัติ อาจจะไม่มีเครือข่ายใดจะให้บริการได้ 100 เปอร์เซ็นต์ หากกำหนดค่าการมีให้ใช้งานได้เป็น 99.999 (Five Nine) เปอร์เซ็นต์ ก็แปลความได้ว่า ในหนึ่งปีจะต้องมีเวลาที่ไม่สามารถใช้งานโครงข่ายได้ หรือโครงข่ายขัดข้องได้ไม่เกิน 5 นาที โดยทั่วไปในทางปฏิบัติเพื่อให้ระบบที่ออกแบบมีค่าการมีให้ใช้งานได้สูง อุปกรณ์ในระบบจะต้องหลีกเลี่ยงจุดที่เป็น Single Point of Failure ซึ่งโดยทั่วไปจะใช้วิธีการออกแบบให้อุปกรณ์เหล่านี้มี Redundancy หรือมี Fail Tolerance

ช่องสัญญาณที่ส่งได้ (Throughput) หมายถึง การรับส่งข้อมูลจากปลายหนึ่งไปยังอีกปลายหนึ่งได้ด้วยอัตราการส่งข้อมูลเท่าไรในหน่วยจำนวนบิตต่อวินาที ค่านี้มิได้หมายถึงค่าสูงสุดของช่องสัญญาณที่จะรับส่งได้ ทั้งนี้เพราะช่องสัญญาณที่ใช้รับส่งได้ มีแพ็กเก็ตและข้อมูลของผู้อื่นร่วมอยู่ด้วย ช่องสัญญาณของผู้ส่งต่อกับผู้รับ มีลักษณะการส่งรวมกับผู้อื่น ค่า Throughput นี้อาจใช้ค่าที่ ISP รับประกันช่องสัญญาณน้อยที่สุดที่จะต้องส่งได้ หรือที่เรียกว่า Minimum Throughput Guarantee เช่น เราเช่าสาย วงจรเช่าขนาด 64 กิโลบิตต่อวินาที แต่มีการรับประกันว่าเราจะใช้ได้ไม่ต่ำกว่า 32 กิโลบิตต่อวินาที ค่า 32 จึงเป็นค่า Throughput แต่เมื่อใช้กับงานบริการเฉพาะบางอย่าง จาเป็นต้องมีการประกันช่องสัญญาณ เช่น การส่งสัญญาณเสียง สัญญาณวิดีโอ เป็นต้น

แพ็กเก็ตที่สูญเสีย (Packet Loss) เมื่อพิจารณาที่สวิตช์หรือเราเตอร์ที่ต้องรับแพ็กเก็ตไว้เป็นจำนวนมาก แต่ไม่สามารถให้บริการได้ทัน ถ้าหน่วยความจำ (Buffer) ของเราเตอร์ใกล้เต็ม จำเป็นต้องทิ้งข้อมูลของบางแพ็กเก็ตไป แพ็กเก็ตที่หายไปโดยไม่สามารถส่งจากผู้ส่งไปยังผู้รับได้เรียกว่า ค่าการหายของแพ็กเก็ต เมื่อแพ็กเก็ตหายไป ผู้ส่งข้อมูลจำเป็นต้องส่งแพ็กเก็ตข้อมูลใหม่

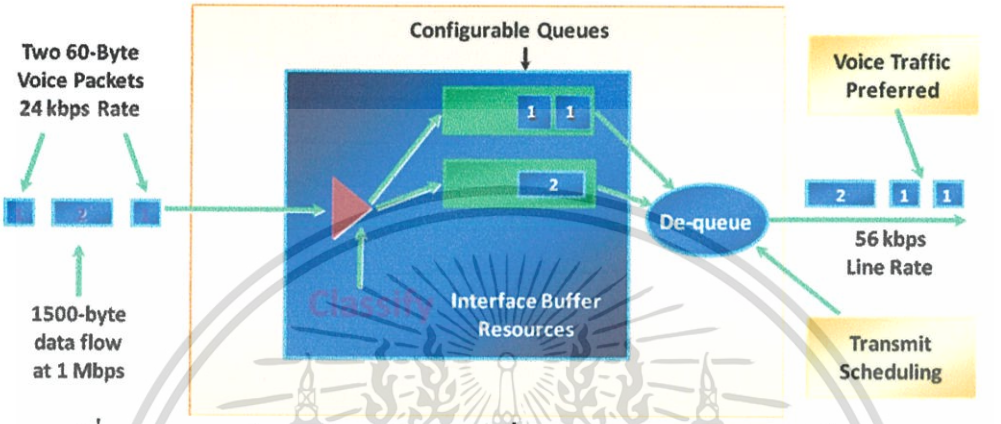
ซึ่งมีโอกาสที่จะทำให้ปริมาณของข้อมูลในระบบเพิ่มมากขึ้น ซึ่งก็จะเป็นการเพิ่มโอกาสที่แพ็กเก็ตข้อมูลในระบบจะสูญหายมากขึ้นด้วยเช่นกัน

ความล่าช้าทางเวลา (Latency หรือ Delay) ค่าความล่าช้าทางเวลาเป็นค่าเวลาที่เริ่มนับจากที่ผู้ส่งเริ่มการส่งแพ็กเก็ตข้อมูล จนกระทั่งแพ็กเก็ตข้อมูลเดินทางถึงยังปลายทาง ในทางเทคนิค โดยปกติแล้วค่าความล่าช้าทางเวลาจะประกอบไปด้วยส่วนประกอบย่อย ๆ ดังนี้

- ความล่าช้าทางเวลาที่เกิดจากระยะทาง (Propagation Delay) คือ ความล่าช้าทางเวลาที่เกิดจากการเดินทางของพาหะ (ซึ่งในโครงข่ายหลัก พาหะจะคือแสงที่อยู่ภายในเส้นใยแก้วนำแสง) ความล่าช้าทางเวลาที่เกิดจากระยะทางจะแปรผันโดยตรงกับระยะห่างระหว่างผู้ส่งและผู้รับในโครงข่าย
- ความล่าช้าทางเวลาที่เกิดจากการแปลงข้อมูลจากอนุกรมเป็นขนาน (Serialization Delay) โดยปกติแล้วกระบวนการจัดการข้อมูลในระบบคอมพิวเตอร์จะมีลักษณะแบบขนานแต่เนื่องจากการส่งข้อมูลจำเป็นต้องส่งแบบอนุกรม ดังนั้นที่ด้านส่งจำเป็นต้องมีการแปลงลักษณะข้อมูลจากแบบขนานให้เป็นแบบอนุกรม ในขณะที่ด้านรับจะต้องมีการแปลงลักษณะข้อมูลจากแบบอนุกรมให้เป็นแบบขนาน
- ความล่าช้าทางเวลาที่เกิดจากการประมวลผลข้อมูล (Processing Delay) จะเกิดขึ้นในทุกจุดที่ต้องมีการทำงานโดยอุปกรณ์อิเลคทรอนิกส์ ตัวอย่างเช่น ความล่าช้าทางเวลาที่เกิดจากการแปลงข้อมูลจาก Analog เป็น Digital (ขึ้นกับประเภทของ CODEC) ความล่าช้าทางเวลาที่เกิดขึ้นจากการคำนวณเส้นทางในอุปกรณ์ค้นหาเส้นทาง (Router) เป็นต้น
- ความล่าช้าทางเวลาที่เกิดจากคิวข้อมูล (Queuing Delay) ในกรณีที่แพ็กเก็ตข้อมูลด้านขาเข้าอุปกรณ์มีปริมาณมากกว่าปริมาณแพ็กเก็ตด้านขาออกจากอุปกรณ์ ผลที่เกิดขึ้นคือจะมีแพ็กเก็ตข้อมูลถูกเก็บอยู่ใน Queuing หรือ Buffer ผลที่ตามมาคือแต่ละแพ็กเก็ตที่อยู่ใน Queuing หรือ Buffer จะมีความล่าช้าทางเวลาเกิดขึ้นนั่นเอง
- ความล่าช้าทางเวลาที่เกิดจาก Dejitter Buffer ในบางกรณี (เช่นการดูภาพยนต์หรือฟังข้อความเสียงผ่านอินเตอร์เน็ต) ที่ด้านรับ จำเป็นต้องมีการเก็บ Queuing หรือ Buffer แพ็กเก็ตข้อมูลให้ได้จำนวนหนึ่ง ก่อนที่จะถูกแปลง (Decode) เป็นภาพหรือเสียง วัตถุประสงค์คือเพื่อให้ภาพหรือเสียงที่ด้านผู้รับนั้นมีความต่อเนื่อง ในกรณีที่เกิดความคับคั่งขึ้นกับโครงข่ายอินเตอร์เน็ต ลักษระการเก็บ Queuing หรือ Buffer ที่ด้านผู้รับนี้ก็จะทำให้เกิดความล่าช้าทางเวลาขึ้นในระบบ

โดยปกติแล้วความล่าช้าทางเวลาที่มีผลกับประสิทธิภาพของระบบมากคือความล่าช้าทางเวลาที่เกิดจากการแปลงข้อมูลจากอนุกรมเป็นขนาน แต่อย่างไรก็ตามในทางปฏิบัติเราจะไม่สามารถลดค่าความล่าช้าทางเวลาส่วนนี้ได้นอกจากการเพิ่มความเร็วของการประมวลหรือแปลงข้อมูลให้สูงขึ้นเช่นเดียวกับความล่าช้าทางเวลาที่เกิดจากการประมวลผลข้อมูล ในส่วนของความ

ล่าช้าทางเวลาที่เกิดจากระยะทางนั้นจะถือว่าเป็นค่าคงตัวของระบบใด ๆ เลยก็ได้ การจัดการควบคุมคุณภาพของการให้บริการในส่วนของความล่าช้าทางเวลาในโครงข่าย MPLS นั้น ความล่าช้าทางเวลาที่จะสามารถลดได้เพื่อเพิ่มประสิทธิภาพการทำงานของระบบหลัก ๆ ก็คือ ความล่าช้าทางเวลาที่เกิดจากคิวข้อมูล กล่าวคือจะมีการแยกคิวข้อมูลตามประเภทความสำคัญของข้อมูล ดังแสดงในรูปที่ 2.7



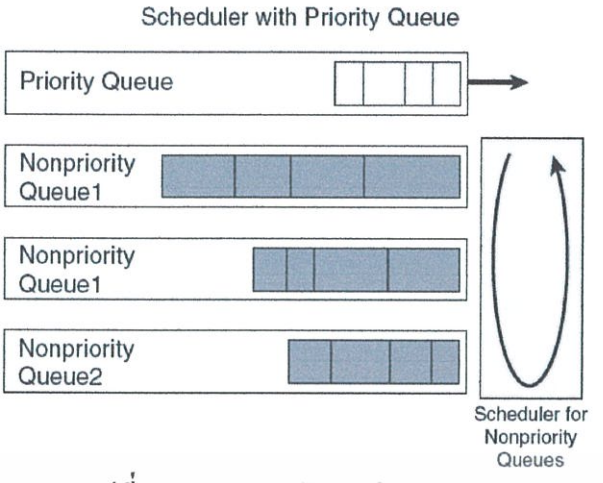
รูปที่ 2.7 แสดงหลักการจัดการคิวข้อมูลเพื่อควบคุมคุณภาพของการให้บริการ

ประเภทของการจัดการคิวข้อมูลโดยทั่วไปที่ใช้งานอยู่จะสามารถแบ่งได้เป็น

- Weight Fair Queuing (WFQ) ในลักษณะนี้แต่ละ Session ที่มีในระบบ จะมีการจัดการข้อมูล (Queuing) ในระบบแยกเป็นอิสระต่อกัน โดยอัตราการส่งข้อมูลออกจากแต่ละคิวจะขึ้นอยู่กับความสำคัญของคิวข้อมูล ตัวอย่างเช่น มีการส่งข้อมูลจำนวน N Session ในระบบ โดยแต่ละ Session มีน้ำหนัก (ความสำคัญ) เป็น W_1, W_2, W_3, …, W_N สำหรับ Session ที่ 1, 2, 3, …, N ตามลำดับ ในกรณีนี้ข้อมูลจะถูกส่งออกจากคิวข้อมูลแต่ละคิวโดยมีอัตราส่งข้อมูลจากคิวข้อมูลที่ i เป็น $W_iL/(W_1 + W_2 + W_3 + \ldots + W_N)$ เมื่อ L คืออัตราการส่งข้อมูล (Bandwidth) สูงสุดของการเชื่อมต่อใด ๆ

  โดยทั่วไปแล้วการจัดการคิวข้อมูลแบบ WFQ นี้จะสามารถรับประกันอัตราการส่งข้อมูลหรือคุณภาพของการให้บริการได้ดีในระดับหนึ่ง นอกจากนั้นจะยังช่วยรับประกันเรื่องความเท่าเทียมกัน (Fairness) ในการส่งข้อมูลด้วย

- Priority Queuing (PQ) มีลักษณะใกล้เคียงกับการจัดการคิวข้อมูลแบบ WFQ คือ แต่ละคิวข้อมูลจะมีความสำคัญไม่เท่ากัน ข้อแตกต่างหลักคือข้อมูลในคิวที่มีความสำคัญสูงสุดจะถูกส่งออกจากคิวจนหมด หลังจากนั้นข้อมูลที่มีความสำคัญน้อยกว่าจึงจะถูกส่งออกจากคิวข้อมูล เป็นเช่นนี้เรียงไปเรื่อย ๆ ดังที่แสดงในรูปที่ 2.8



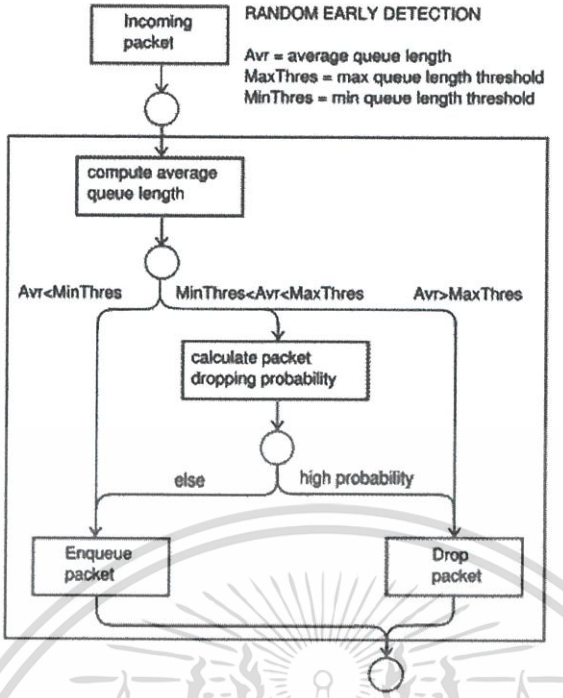
รูปที่ 2.8 แสดงการจัดการคิวแบบ PQ

ข้อดีของการจัดการคิวข้อมูลด้วยวิธี PQ คือ ระบบจะสามารถควบคุมคุณภาพของการให้บริการของข้อมูลที่มีความสำคัญสูงได้เป็นอย่างดี โดยกรณีที่เลวร้ายที่สุดคือข้อมูลในคิวที่มีความสำคัญต่ำ ๆ อาจจะไม่ได้ถูกส่งออกจากคิวข้อมูลเลยในกรณีที่มีข้อมูลที่สำคัญกว่าเข้ามาใหม่อยู่ตลอดเวลา กล่าวคือ อาจจะมีปัญหาเรื่องความเท่าเทียมกันของข้อมูลในระบบ

- Class Based Weight Fair Queuing (CBWFQ) มีลักษณะใกล้เคียงกับการจัดการคิวข้อมูลแบบ WFQ กล่าวคือคิวข้อมูลแต่ละคิวจะมีความสำคัญแตกต่างกันตามประเภทข้อมูล แต่การจัดการคิวข้อมูลแบบ CBWFQ นั้นรองรับการตั้งระดับ (Class) ของข้อมูลโดยผู้ใช้งานเอง เช่น ผู้ใช้งานอาจจะตั้งระดับของข้อมูลตามประเภทของโปรโตคอล หรือ Access Control List (ACL) หรือการเชื่อมต่อ (Interface)
- Low Latency Queuing (LLQ) มีลักษณะเป็นรูปผสมระหว่างการจัดการคิวแบบ PQ และ CBWFQ กล่าวคือผู้ใช้งานอาจจะมีการตั้งระดับของข้อมูล (ตามระดับความสำคัญ) โดยข้อมูลที่มีความสำคัญสูงสุดจะถูกส่งออกจากคิวข้อมูลจนหมดก่อนที่ข้อมูลซึ่งมีความสำคัญน้อยกว่าจะถูกส่งออกจากคิวข้อมูลเป็นเช่นนี้เรียงไปเรื่อย ๆ

โดยทั่วไปแล้วสำหรับข้อมูลที่คุณภาพของการให้บริการขึ้นกับความล่าช้าทางเวลาและค่าความแปรผันของความล่าช้าทางเวลาจะถูกกำหนดให้มีการจัดการคิวข้อมูลแบบ PQ หรือ LLQ เป็นหลัก

นอกเหนือจากเรื่องการจัดคิวข้อมูลแล้ว ในกรณีที่คิวข้อมูลเต็ม (หรือใกล้จะเต็ม) ก็จำเป็นต้องมีการละทิ้ง (Drop) แพ็กเก็ตข้อมูล โดยพื้นฐานของวิธีการละทิ้งแพ็กเก็ตข้อมูลจะใช้วิธีที่มีชื่อเรียกว่า Random Early Detection (RED) โดยมีหลักการทำงานดังแสดงในรูปที่ 2.9



รูปที่ 2.9 แสดงหลักการของ Random Early Detection (RED)

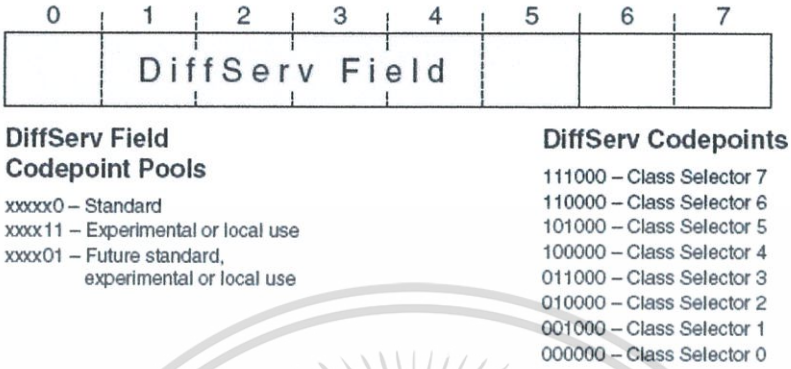
จากรูปที่ 2.9 จะมีการจำนวนค่าความยาวคิวข้อมูลโดยเฉลี่ย และนำค่าไปเปรียบเทียบกับค่า Low Threshold และ High Threshold ถ้าค่าความยาวคิวข้อมูลโดยเฉลี่ยสั้นกว่าค่า Low Threshold แพ็กเก็ตนั้นจะถูกจัดเก็บในคิวข้อมูล (ไม่ได้ถูกละทิ้ง) ในกรณีที่ค่าความยาวคิวข้อมูลโดยเฉลี่ยอยู่ระหว่างค่า Low และ High Threshold ก็จะมีการคำนวณค่าความน่าจะเป็นที่จะละทิ้งแพ็กเก็ตข้อมูล ถ้าคำนวณได้ค่าความน่าจะเป็นมีค่าสูง แพ็กเก็ตข้อมูลนั้นก็จะถูกละทิ้ง แต่ถ้าค่าความน่าจะเป็นที่คำนวณได้มีค่าต่ำ แพ็กเก็ตนั้นก็จะถูกจัดเก็บเข้าคิวข้อมูล ท้ายสุดถ้าค่าความยาวคิวข้อมูลโดยเฉลี่ยมีความยาวมากกว่าค่า High Threshold แพ็กเก็ตข้อมูลนั้นก็จะถูกละทิ้งในทันที

กระบวนการละทิ้งแพ็กเก็ตข้อมูลแบบ RED มีการพัฒนาต่อเป็นแบบ Weighted Random Early Detection (WRED) โดยสิ่งที่มีการเพิ่มเติมคือ แต่ละคิวข้อมูลจะสามารถมีระดับ Threshold แยกอิสระต่อกันได้ และอาจจะมีวิธีในการคำนวณความน่าจะเป็นที่จะละทิ้งข้อมูล (ในกรณีที่ความยาวคิวโดยเฉลี่ยอยู่ระหว่างค่า Low และ High Threshold) แยกเป็นอิสระต่อกัน ส่งผลให้สามารถมีกรรมวิธีที่จะละทิ้งแพ็กเก็ตข้อมูลแยกตามความสำคัญของแพ็กเก็ตข้อมูลได้ดีกว่าแบบ RED เดิม

ค่าแปรผันหน่วงเวลา (Jitter) อาจกล่าวได้ง่าย ๆ ว่าเป็นค่าการปรวนแปรของค่าเวลาลาเทนซี่ กล่าวคือ แพ็กเก็ตที่เคลื่อนที่จากต้นทางไปยังปลายทางหลาย ๆ แพ็กเก็ต ปรากฏว่าการไปถึงปลายทางใช้ระยะเวลาต่างกันทาให้ข้อมูลบางส่วนที่ไปก่อนอาจถึงทีหลัง หรือมีเวลาเหลื่อมกัน ทาให้การตรวจสอบลาดับของแพ็กเก็ตในผู้รับต้องกระทาด้วย ข้อมูลที่ใช้ในการรับส่งบนเครือข่ายอินเทอร์เน็ตจึงมีลักษณะที่ต้องการในคุณสมบัติที่แตกต่างกัน

2.3 การรับประกันคุณภาพการให้บริการในโครงข่าย MPLS

ตามมาตรฐาน RFC2474 และ RFC3260 ของ IETF แพ็กเก็ตข้อมูล IP (ทั้ง IPv4 และ IPv6) จะถูกกำหนดให้มีความสำคัญที่แตกต่างกันตามค่าใน DiffServ Field ความยาว 6 บิต ดังแสดงในรูปที่ 2.10



รูปที่ 2.10 แสดง DiffServ Field ใน IP Header ตามมาตรฐาน RFC2474 และ RFC3260

จากรูปที่ 2.10 จะให้ความสนใจเฉพาะส่วนที่เป็นมาตรฐาน (Standard) กล่าวคือกรณีที่บิตที่ 5 (บิตทางขวามือสุด) มีค่าเป็น 0 (ศูนย์) เท่านั้น โดยจากบิตทั้งหมด 6 บิตจะแยกเป็น 2 ส่วนมีความยาวส่วนละ 3 บิตเท่ากัน โดยส่วนที่เป็น 3 บิตแรก (DiffServ Code Point – DSCP) จะบอกถึงความสำคัญของแต่ละแพ็กเก็ต ดังนั้นจะสามารถมีแพ็กเก็ตที่มีความสำคัญแตกต่างกันได้สูงสุด $2^3 = 8$ รูปแบบ ส่วนที่เป็น 3 บิตหลังจะใช้บอกถึงความสำคัญของแพ็กเก็ตซึ่งจะมีผลกับกระบวนการเลือกทิ้งแพ็กเก็ตในกรณีที่เกิดความคับคั่งในระบบ

โดยปกติแล้วการควบคุมคุณภาพของบริการด้วยวิธี DiffServ จะมีการระบุถึงความสำคัญของแต่ละ Class ของแพ็กเก็ตข้อมูลด้วย DSCP ซึ่งมีการนำมาใช้ทดแทน TOS (Type Of Service) Field ภายในส่วนหัวของแพ็กเก็ต IP โดยการควบคุมคุณภาพของบริการด้วยวิธี DiffServ นั้นมีแนวความคิดหลักคือพยายามจะควบคุมคุณภาพของบริการให้ได้ใกล้เคียงกับวิธี IntServ ให้ได้มากที่สุด โดยที่ไม่ต้องมีการจัดการทราฟฟิคในทุก ๆ การเชื่อมต่อ (Per-Flow Basis) ทำให้การควบคุมคุณภาพของบริการด้วยวิธี DiffServ นั้นสามารถใช้กับโครงข่ายขนาดใหญ่หรือมีปริมาณทราฟฟิคมากได้เป็นอย่างดี (Scalability)

2.3.1 MPLS Per-Hop Behavior (PHB)

อุปกรณ์ Router ในเส้นทางจะพิจารณาและส่งแพ็กเก็ตข้อมูลตามความสำคัญของแต่ละ Class ในแต่ละฮอบ หรือที่เรียกว่า Per-Hop Behavior (PHB) ตลอดเส้นทางไปจนถึงปลายทาง ซึ่งโดยทั่วไปแล้วจะสามารถแบ่งระดับ Class ใน PHB ออกได้เป็น 4 รูปแบบคือ

- Default PHB ใช้สำหรับข้อมูลแบบ Best Effort (BE) (RFC2474)

- Class selector PHB ใช้สำหรับให้ PHB สามารถใช้งานร่วมกับระบบที่ไม่รองรับการใช้งานแบบ DiffServ (RFC2474)
- Expedited Forwarding (EF) PHB ใช้งานกับข้อมูลที่ต้องการให้มีการรับประกันขนาดของช่องสัญญาณ (Bandwidth) และต้องการความล่าช้าทางเวลาและความแปรผันของความล่าช้าทางเวลาต่ำ (RFC2598)
- Assured Forwarding (AF) PHB ใช้งานกับข้อมูลที่ต้องการให้มีการรับประกันขนาดของช่องสัญญาณ (RFC2597)

ข้อแตกต่างอีกประการหนึ่งของ EF และ AF PHB คือในกรณีของ EF นั้นจะไม่ยอมให้แหล่งกำเนิดข้อมูลส่งข้อมูลด้วยอัตราส่งข้อมูลสูงกว่าที่ระบบรับประกัน หรืออาจจะกล่าวได้ว่าข้อมูลส่วนที่เกินกว่าค่าช่องสัญญาณที่รับประกันจะถูกทิ้งไป ในขณะที่สำหรับ AF นั้น แหล่งกำเนินอาจจะสามารถส่งข้อมูลด้วยอัตราที่สูงกว่าช่องสัญญาณที่รับประกันได้ ในกรณีที่ระบบมีช่องสัญญาณเหลืออยู่ แต่อย่างไรก็ตามข้อมูลในส่วนเกินนี้อาจจะถูกทิ้งโดย Router ในระบบได้ถ้าเกิดความคับคั่งในระบบ

ตารางที่ 2.1 แสดงข้อมูลสำหรับการจับคู่ระหว่าง PHB และ DSCP ที่แนะนำโดย IETF

PHB	DSCP (Decimal)	DSCP (Binary)
EF	46	101110
AF43	38	100110
AF42	36	100100
AF41	34	100010
AF33	30	011110
AF32	28	011100
AF31	26	011010
AF23	22	010110
AF22	20	010100
AF21	18	010010
AF13	14	001110
AF12	12	001100
AF11	10	001010
CS7	56	111000
CS6	48	110000
CS5	40	101000
CS4	32	100000
CS3	24	011000
CS2	16	010000
CS1	8	001000
Default	0	000000

จากตารางที่ 2.1 จะเห็นได้ว่า AF ที่แนะนำโดย IETF จะแบ่งย่อยได้เป็นอีก 4 ระดับคือ AF1x, AF2x, AF3x และ AF4x ตามลำดับ โดยที่ x หมายถึงนโยบายในการละทิ้งแพ็กเก็ต โดยมีค่าเป็น 1, 2 และ 3 ซึ่งหมายถึงมีความน่าจะเป็นที่แพ็กเก็ตข้อมูลจะถูกทิ้งต่ำ ปานกลาง และสูง ตามลำดับ ดังข้อมูลในตารางที่ 2.2

ตารางที่ 2.2 แสดงถึงนโยบายการทิ้งแพ็กเก็ตในกรณีที่เกิดความคับคั่งสำหรับ AF

Drop Precedence	AF1	AF2	AF3	AF4
Low	AF11	AF21	AF31	AF41
Medium	AF12	AF22	AF32	AF42
High	AF13	AF23	AF33	AF43

ตารางที่ 2.3 แสดงข้อมูลสำหรับการจับคู่ระหว่าง PHB และ IP Precedence ที่แนะนำโดย IETF

PHB	DSCP (Decimal)	DSCP (Binary)	Precedence Name	Precedence (Binary)	Precedence (Decimal)
CS7	56	111000	Network Control	111	7
CS6	48	110000	Internetwork Control	110	6
CS5	40	101000	Critic/ECP	101	5
CS4	32	100000	Flash Override	100	4
CS3	24	011000	Flash	011	3
CS2	16	010000	Immediate	010	2
CS1	8	001000	Priority	001	1
CS0	0	000000	Routine	000	0

อย่างไรก็ตามด้วยลักษณะการทำงานแบบแต่ละฮอบของ PHB ทำให้อาจจะไม่สามารถรับประกันคุณภาพของการให้บริการในลักษณะ end-to-end ได้ดีนัก โดยเฉพาะอย่างยิ่งในกรณีที่เกิดความคับคั่งในโครงข่าย MPLS ดังนั้นจึงมีการพัฒนาโครงข่าย MPLS ให้สามารถรับประกันคุณภาพของการให้บริการในลักษณะ end-to-end ด้วยกระบวนการวิศวกรรมจราจร (Traffic Engineering)

2.4 MPLS Traffic Engineering (TE)

MPLS TE จะใช้หลักการของ Constraint-based routing เข้ามาช่วย กล่าวคือ LSR (Label Switch Router) ต้นทางสามารถคำนวณเส้นทางเพื่อไปหา LSR ปลายทาง โดยเส้นทางที่คำนวณนั้นสามารถรับประกันคุณภาพของการให้บริการ (เช่น แพ็กเก็ตที่สูญเสีย ความล่าช้าทางเวลา และการแปรผันของความล่าช้าทางเวลา) ได้ โดยอาศัยอัลกอริธึมการหาเส้นทาง (Routing Algorithm)

จากวิธีการหาเส้นทางเดิมที่ใช้งานอยู่ในโครงข่าย เมื่อสามารถหาเส้นทางที่ต้องการได้แล้วระบบจะสร้าง TE LSP (Traffic Engineering Label Switch Path) ตามเส้นทางที่หาได้

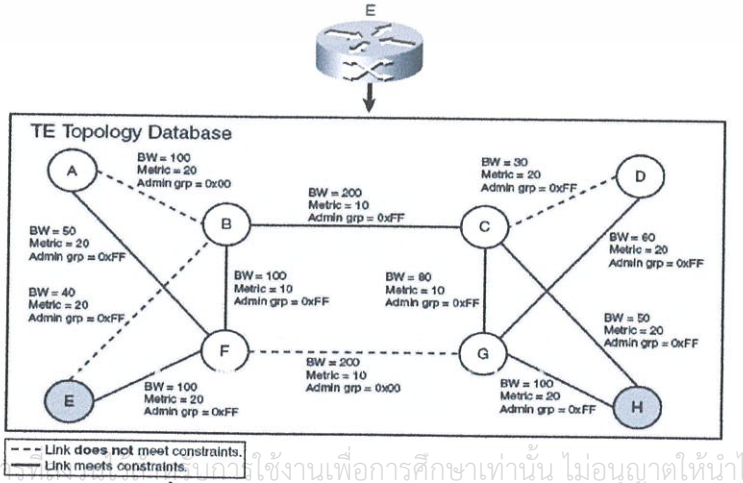
ขั้นตอนการทำงานที่สำคัญของ Constraint-Based Routing จะประกอบไปด้วยขั้นตอนย่อย 2 ขั้นตอน ได้แก่

- ขั้นตอนการแพร่กระจายข้อมูลการเชื่อมต่อ (Link Information Distribution)
- ขั้นตอนการคำนวณหาเส้นทาง (Path Computation)

ในส่วนของขั้นตอนการแพร่กระจายข้อมูลการเชื่อมต่อนั้น LSR จะใช้ข้อมูลการหาเส้นทาง (Flooding Information) ซึ่งใช้ในโปรโตคอลหาเส้นทางแบบ Link State (IS-IS หรือ OSPF) เพื่อสร้างฐานข้อมูล TE Topology ซึ่งฐานข้อมูลนี้จะเป็นคนละส่วนจากฐานข้อมูลที่ใช้ในการหาเส้นทางแบบทีละฮอบ โดยทั่วไป MPLS TE จะใช้ข้อมูลช่องสัญญาณ (Bandwidth), Administrative Group (flag) และ TE Metric ซึ่งเป็นตัวแปรที่เพิ่มขึ้นจากระบบเดิม โดยแต่ละส่วนมีรายละเอียดคร่าว ๆ ดังนี้

- ช่องสัญญาณ มีการแบ่งขนาดช่องสัญญาณออกเป็น 8 ระดับ ตามระดับความสำคัญของ TE LSP
- Administrative Group หรือ Flag เป็นข้อมูลที่ใช้ระบุว่าจะมีการใช้กฎ (Rule) กับการเชื่อมต่อใดบ้าง
- TE Metric เป็นข้อมูลสำหรับการทำ Path Optimization

หลังจากสร้างฐานข้อมูล TE Topology เรียบร้อยแล้วจะสามารถคำนวณหาเส้นทาง (Path Computation) ด้วยวิธีการหาเส้นทางแบบมีข้อจำกัด หรือ Constraint-Based Routing (หลักการทั่วไปคืออาจจะมีการเพิ่มข้อจำกัดในกระบวนการเส้นทาง) โดยจะมีการใช้อัลกอริธึม Shortest Path First (SPF) ที่มีส่วนขยายเพิ่มเติมในการคำนวณ ตัวอัลกอริธึมที่มีส่วนขยายเพิ่มเติมนี้มีอีกชื่อหนึ่งคือ Constraint-Based, Shortest Path First (CSPF) โดยสามารถอธิบายหลักการทำงานคร่าว ๆ ดังรูปที่ 2.11



รูปที่ 2.11 แสดงหลักการทำงานของ CSPF

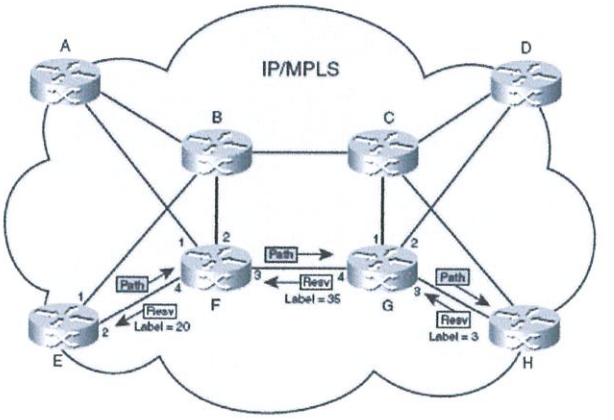
จากรูปที่ 2.11 กำหนดให้ Node E ต้องการส่งข้อมูลไปยัง Node H ด้วยอัลกอริธึมการหาเส้นทางแบบ CSPF โดยมีข้อกำหนดว่าเส้นทางที่ใช้จะต้องมีช่องสัญญาณอย่างน้อย 50 Mbps และอยู่ใน Administrative Group (flag) 0xFF เท่านั้น ภายหลังการคำนวณตาม CSPF จะสามารถหาเส้นทางที่มีคุณสมบัติตรงตามความต้องการได้เส้นทางเป็น {E F B C G H} หรือส่วนที่เป็นเส้นทึบในรูปที่ 2.11 ขั้นตอนหลังจากนี้ Node E จะเริ่มต้นการสร้าง TE LSP โดยใช้ Signaling ซึ่งเป็นส่วนขยายของ ReSource ReserVation Protocol (RSVP)

Signaling ที่ใช้ใน MPLS TE เพื่อสร้าง LSP นั้นหลัก ๆ จะใช้หลักการของ RSVP โดยมีข้อความ (Message) ที่สำคัญดังแสดงในตารางที่ 2.4

ตารางที่ 2.4 แสดงข้อความ (Message) สำหรับการทำ TE โดยหลักการของ RSVP

RSVP Object	RSVP Message	Description
LABEL_REQUEST	Path	Label request to downstream neighbor
LABEL	Resv	MPLS label allocated by downstream neighbor
EXPLICIT_ROUTE	Path	Hop list defining the course of the TE LSP
RECORD_ROUTE	Path, Resv	Hop/label list recorded during TE LSP setup
SESSION_ATTRIBUTE	Path	Requested LSP attributes (priority, protection, affinities)

- LABEL_REQUEST เป็น RSVP Message แบบ Path ซึ่ง Upstream MPLS Router ร้องขอไปยัง Downstream MPLS Router
- LABEL เป็น RSVP Message แบบ Resv ซึ่ง Downstream MPLS Router ได้จอง (Allocate) ไว้ใช้งาน และแจ้งให้ Upstream MPLS Router ทราบ
- EXPLICIT_ROUTE เป็น RSVP Message แบบ Path ซึ่งส่งไปยัง Downstream MPLS Router เพื่อกำหนดเส้นทางการสร้าง LSP ตามที่ผู้ใช้งานต้องการ โดยอาจจะใช้เป็นส่วนหนึ่งของการทำ Path Recovery ซึ่งมีชื่อทางเทคนิคว่า Fast Reroute
- RECORD_ROUTE เป็น RSVP Message แบบ Path หรือ Resv ซึ่งจะบันทึกฮอบหรือลาเบลที่มีการใช้งานในระหว่างที่กำลังสร้าง LSP
- SESSION_ATTRIBUTE เป็น RSVP Message แบบ Path เป็น Attributes ในการสร้าง LSP เช่น จะระบุถึงความสำคัญ หรือการสร้างเส้นทางสำรอง



Node E LFIB			Node F LFIB			Node G LFIB			Node H LFIB		
Input Label	Output Interface	Output Label	Input Label	Output Interface	Output Label	Input Label	Output Interface	Output Label	Input Label	Output Interface	Output Label
—	2	20	20	3	35	35	3	3	3	—	—

รูปที่ 2.12 แสดงขั้นตอนการจองช่องสัญญาณด้วย RSVP ภายหลังการทำ CSPF

จากรูปที่ 2.12 Node E จะส่งข้อความเพื่อร้องขอการสร้าง TE LSP ไปยัง Node H โดยในข้อความจะเป็น MPLS TE (EXPLICIT_ROUTE, LABEL_REQUEST, SESSION_ATTRIBUTE และ RECORD_ROUTE) เพื่อจองทรัพยากรต่าง ๆ ที่ระบุใน SESSION_ATTRIBUTE ตามเส้นทางที่(อาจจะ)มีการระบุไว้ใน EXPLICIT_ROUTE เมื่อข้อความ MPLS TE ดังกล่าวเดินทางถึงปลายทางแล้ว Node H จะส่งข้อความ Resv คือ MPLS TE (LABEL และ RECORD_ROUTE) เพื่อกำหนดลาเบลต่าง ๆ ที่จะใช้ใน LSP รวมถึงการบันทึกข้อมูลต่าง ๆ ด้วย ส่วน node ต่าง ๆ ที่อยู่ระหว่างทางก็จะอัพเดทข้อมูลใน Label Forwarding Information Base (LFIB) ของตนเอง ตามหมายเลขลาเบลที่ได้รับ

ภายหลังการจองช่องสัญญาณด้วย RSVP แล้วก็จะได้ LSP เริ่มตั้งแต่ Node ต้นทางจนถึง Node ปลายทาง พร้อมทั้งข้อมูล Label ที่จะมีการแลกเปลี่ยนกัน จึงทำให้รับประกันควบคุมคุณภาพของการให้บริการแบบ end-to-end ด้วยวิธี DS-TE ในโครงข่าย MPLS ได้ แต่อย่างไรก็ตามก็ต้องแลกกับความซับซ้อนภายในระบบที่เพิ่มมากขึ้น ซึ่งอาจจะทำให้ไม่สามารถใช้งานกับโครงข่ายขนาดใหญ่ ๆ หรือว่ามีทราฟฟิคปริมาณมาก ๆ ได้

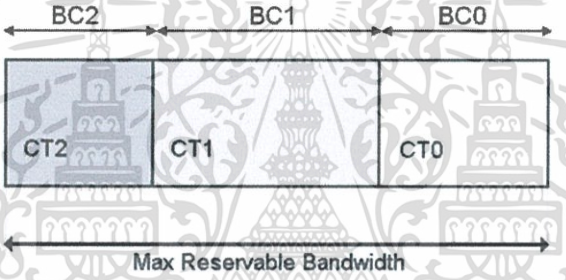
2.5 MPLS DiffServ-aware Traffic Engineering (DS-TE)

MPLS DS-TE จะยังคงใช้หลักการหลัก ๆ ของกระบวนการทำ TE ดังที่กล่าวมาในข้างต้นอยู่ แต่จะเพิ่มในส่วนของการรองรับหลาย ๆ ระดับ (Class) ของข้อมูล และสามารถทำการหาเส้นทางแบบมีข้อจำกัด (Constraint-Based Routing) กับแต่ละระดับของข้อมูลได้ ตามมาตรฐาน RFC4124 โดยข้อแตกต่างหลักของ DS-TE กับ DiffServ คือ DS-TE จะทำงานในส่วนของ Control Plane ใน MPLS Router (ใช้ในการกำหนดนโยบายต่าง ๆ) ในขณะที่ DiffServ จะทำงานในส่วน Forwarding Plane (ใช้รับส่งข้อมูล)

DS-TE ใช้หลักการของ Class Type (CT) ในกระบวนการจัดสรรช่องสัญญาณ การหาเส้นทางแบบมีข้อจำกัด และกระบวนการ Admission Control โดย CT จะมีอยู่ 8 ระดับ (CT0 – CT7) ระดับของ CT จะมีลักษณะคล้ายคลึงกับระดับความสำคัญของข้อมูลใน PHB นอกจาก CT แล้ว DS-TE ยังมีอีกตัวแปรที่สำคัญคือ Bandwidth Constraints (BC) ซึ่งหมายถึงขนาดช่องสัญญาณที่สามารถจัดสรรให้กับแต่ละระดับของบริการ กล่าวคือแต่ละ link ใน DS-TE จะมี BC กำกับอยู่กับแต่ละ CT ดังนั้นโดยทั่วไปแล้ว BC จะมีจำนวนสูงสุดคือ 8 (เพื่อให้สอดคล้องกับระดับ CT) IETF ได้กำหนดมาตรฐานของ BC ออกเป็น 2 แบบคือ

- Maximum Allocation Model (MAM)

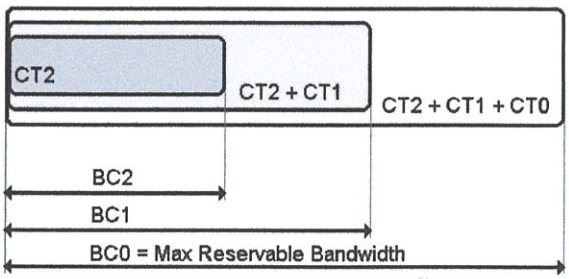
MAM ถูกกำหนดเป็นมาตรฐาน RFC4125 โดย จะมีการกำหนดความสัมพันธ์ระหว่าง CT และ BC เป็นแบบหนึ่งต่อหนึ่ง (นั่นคือแต่ละ CT จะมี BC ของตนเอง) แต่ละ CT ไม่สามารถใช้ช่องสัญญาณที่เหลือจาก CT อื่นได้ (ไม่มีการแบ่งการใช้งานช่องสัญญาณระหว่างแต่ละ CT) ลักษณะความสัมพันธ์ระหว่าง CT และ BC ใน MAM แสดงอยู่ในรูปที่ 2.13



รูปที่ 2.13 แสดงความสัมพันธ์ระหว่าง CT และ BC ใน MAM

- Russian Dolls Model (RDM)

RDM ถูกกำหนดเป็นมาตรฐาน RFC4127 โดยความสัมพันธ์ระหว่าง CT และ BC จะไม่เป็นแบบหนึ่งต่อหนึ่ง ยกตัวอย่างเช่นจากรูปที่ 2.14 จะมีการกำหนด BC อยู่ 3 ระดับคือ BC0 คือค่าจำกัดช่องสัญญาณที่มีค่ามากที่สุด (เท่ากับ Maximum Reservable Bandwidth) จะถูกจับคู่กับทุก CT ในระบบ (CT2 + CT1 + CT0) ในขณะที่ BC1 จะมีขนาดเล็กกว่า BC0 และถูกจับคู่กับ CT2 + CT1 และท้ายสุด BC2 ซึ่งมีขนาดช่องสัญญาณเล็กที่สุดจะถูกจับคู่กับ CT2 นั่นคือสามารถมีการแบ่งปันการใช้งานช่องสัญญาณระหว่าง CT ที่ถูกกำหนดให้อยู่ใน BC ชุดเดียวกัน



รูปที่ 2.14 แสดงความสัมพันธ์ระหว่าง CT และ BC ใน RDM

บทที่ 3
การออกแบบระบบเพื่อทดสอบการรับประกันคุณภาพของการให้บริการด้วยวิธี PHB และ DS-TE

ข้อด้อยของกลไกการควบคุมคุณภาพการให้บริการโดยใช้ Per-Hop Behavior (PHB) คือ การที่ไม่สามารถรับประกันคุณภาพการให้บริการแบบ end-to-end ได้ เนื่องด้วยการทำงานของ PHB จะควบคุมการรับส่งแพ็กเก็ตแบบ Hop by Hop ซึ่งจะสามารถรับประกัน QoS ของ Application ได้เฉพาะฮอบนั้น ๆ แต่ว่าจุดฮอบไป (Next-Hop) จะไม่สามารถรับประกันคุณภาพของการให้บริการได้ ดังนั้นหากเกิดความคับคั่งของในโครงข่าย MPLS ที่ Next-Hop ก็อาจจะทำให้คุณภาพของ Application ดังกล่าวลดลงหรือว่าอาจจะถูกทิ้งแพ็กเก็ตข้อมูลเลย ซึ่งในการส่งข้อมูลในโครงข่าย MPLS จะกำหนดเส้นทาง Label Switch Path (LSP) โดยใช้ Routing Protocols แบบ Interior Gateway Protocol (IGP) คำนวณเส้นทางตาม Routing Table เพื่อหาเส้นทางที่ดีที่สุดหรือสั้นที่สุด Shortest Path First (SPF) เมื่อได้เส้นทางแล้วจึงจะทำการเผยแพร่หมายเลขลาเบล (Label Distribution Protocol) ทำให้เกิด LSP ก่อนที่จะส่งข้อมูล กลไกควบคุมคุณภาพการให้บริการโดยใช้ PHB จะควบคุมการรับส่งข้อมูลแต่ละ Application ที่ส่งตามเส้นทาง โดยการที่ Router ที่อยู่ภายในโครงข่าย MPLS ไม่สามารถทราบถึงการเกิดความคับคั่งของบาง link ซึ่ง link นั้นเป็น Next-Hop ของ SPF ตาม IGP ทำให้ไม่สามารถควบคุมคุณภาพการให้บริการโดยใช้ PHB ตั้งแต่จุดตั้งต้นจนถึงจุดปลายทางได้

การแก้ปัญหาข้างต้นนี้ โดยทั่วไปจะใช้กลไกการควบคุมคุณภาพการให้บริการด้วย DiffServ-aware Traffic Engineering (DS-TE) เพื่อกำหนดเส้นทางในการไหลของทราฟฟิคของแต่ละ Application เพื่อให้สามารถรับประกันคุณภาพการให้บริการแบบ end-to-end ในวิทยานิพนธ์ฉบับนี้จะอาศัยการทำงานของกลไกการควบคุมคุณภาพการให้บริการ โดยใช้ DS-TE สร้างท่อเสมือน (Tunnel) ตั้งแต่ต้นทางถึงปลายทางและภายในแต่ละ Tunnel จะมีการแบ่งลำดับความสำคัญของแต่ละ Application เพื่อควบคุมคุณภาพการให้บริการ

กลไกควบคุมคุณภาพการให้บริการโดยใช้ PHB หรือ DS-TE ที่จะเปรียบเทียบในวิทยานิพนธ์ฉบับนี้ จะเปรียบเทียบกันด้วยพารามิเตอร์หลัก 3 ค่า ได้แก่ค่าแพ็กเก็ตที่สูญเสีย (Packet Loss) ค่าความล่าช้าทางเวลา (Delay หรือ Latency) และค่าแปรผันความล่าช้าทางเวลา (Jitter) ตามข้อตกลงระดับการให้บริการ (Service Level Agreement – SLA) โดยจะมีการกำหนดคุณภาพการให้บริการให้กับข้อมูลที่เป็นภาพเคลื่อนไหว (Video) ซึ่งจะมีการรับส่งข้อมูลภายใต้โครงข่ายทั้งแบบที่ไม่มีความคับคั่งและมีความคับคั่ง เพื่อเปรียบเทียบประสิทธิภาพการรับประกันคุณภาพการให้บริการดังที่ได้กล่าวมาข้างต้น

3.1 แบบจำลองโครงข่าย MPLS

แบบจำลองที่ใช้ในการจำลองเพื่อหาค่าประสิทธิภาพของระบบ กำหนดรูปแบบการเชื่อมต่อ (Topology) แสดงดังรูปที่ 3.1 จากรูปเป็นการออกแบบระบบเครือข่ายเพื่อทำการทดสอบ โดยแบ่งการเชื่อมต่อให้เป็นลำดับชั้นเพื่อลดการทำงานในการประมวลผลของอุปกรณ์เครือข่าย ซึ่งสามารถแบ่งได้ 3 ลำดับชั้นดังนี้

3.1.1 ระดับชั้นแกนกลาง (Core Layer)

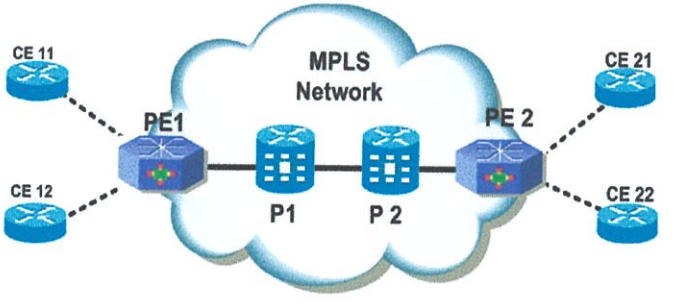
ในลำดับชั้นนี้ถือได้ว่าเป็นชั้นที่สำคัญที่สุด หรือที่เรียกว่าแกนกลางหลัก (Backbone) จะทำงานเป็นหัวใจหลักในโครงข่าย MPLS ทำหน้าที่ส่งข้อมูลด้วยความเร็วสูงและหาเส้นทางซึ่งในแบบจำลองการทดลองรูปที่ 3.1 Core Layer ประกอบด้วย Router P1 และ P2 ซึ่งใช้ Router ยี่ห้อ Cisco รุ่น 7609 Version c7600s72033-adventerprisek9-mz.122-33.SRB2.bin ทำหน้าที่เป็น Provider Router เชื่อมต่อกันด้วย Gigabit Ethernet Interface มีช่องสัญญาณขนาด 1 Gbps.

3.1.2 ระดับชั้นการกระจาย (Distribution Layer)

ระดับชั้นการกระจายเป็นตัวกลางในเครือข่ายเพื่อเชื่อมระหว่างลำดับชั้นแกนกลางและลำดับชั้นการเข้าถึง จะควบคุมการทำงานของอุปกรณ์ในลำดับชั้นการเข้าถึง ควบคุมทราฟฟิกในเครือข่าย ในแบบจำลองการทดลองรูปที่ 3.1 Distribution Layer ประกอบด้วย Router PE1 และ PE2 ใช้ Router ยี่ห้อ Cisco รุ่น 7609 Version c7600s72033-adventerprisek9-mz.122-33.SRB2.bin ทำหน้าที่เป็น Provider Edge Router เชื่อมต่อกับ Core Layer ด้วย Gigabit Ethernet Interface และเชื่อมต่อกับ Access Layer ด้วย Gigabit Ethernet Interface เช่นกัน

3.1.3 ระดับชั้นการเข้าถึง (Access Layer)

ระดับชั้นนี้เป็นการเชื่อมต่อผู้ใช้งานให้สามารถทำการติดต่อกับทรัพยากรที่มีในโครงข่ายได้ ซึ่งในแบบจำลองการทดสอบรูปที่ 3.1 Access Layer จะใช้ Traffic Generator ยี่ห้อ Agilent รุ่น N2X จำลองเป็นอุปกรณ์ CE (Customer Equipment) ทำการส่งข้อมูล Ethernet ขนาด Frame Size 1500 byte โดยเชื่อมต่อกับ Distribution Layer ด้วย Gigabit Ethernet Interface



รูปที่ 3.1 แบบจำลองโครงข่าย MPLS ที่ใช้ทดสอบประสิทธิภาพ

เนื่องจากงานวิจัยนี้มีการใช้อุปกรณ์ของผู้ให้บริการจริง แต่มีการควบคุมปริมาณทราฟฟิคที่ใช้งานผ่าน Router แต่ละตัว จึงเป็นสาเหตุให้ผู้วิจัยไม่สามารถทดสอบระบบกับอุปกรณ์ที่ให้บริการจริงได้ จึงจำเป็นต้องติดตั้งระบบทั้งหมดในห้องทดลอง ทำให้ไม่สามารถจำลองระบบเป็นระบบ WAN (Wide Area Network) ได้ โดยระยะทางระหว่าง Node ต้นทางและ Node ปลายทางยาวประมาณ 100 เมตร ดังนั้นอาจจะมีความแตกต่างจากผลการวัดในวิทยานิพนธ์ฉบับนี้กับระบบที่ใช้งานจริงอยู่บ้าง สืบเนื่องมาจากผลของความล่าช้าทางเวลาเนื่องจากระยะทาง (Propagation Delay)

3.2 พารามิเตอร์ที่ใช้ในการจำลองระบบ

ในส่วนนี้จะแสดงค่าพารามิเตอร์ที่ใช้ในแบบการจำลองการทดสอบระบบ ซึ่งสามารถแบ่งออกได้เป็น 3 ส่วนหลัก ๆ คือ

3.2.1 ค่าพารามิเตอร์ที่ใช้ในการตั้งค่าการใช้งาน MPLS

โครงข่าย MPLS ที่ทดสอบประกอบด้วยการเชื่อมโยงอุปกรณ์ในลำดับชั้นแกนกลาง (Core Layer) มี Router P1 และ P2 ทำหน้าที่เป็น Provider Router เชื่อมต่อกันด้วย 1 Gigabit Ethernet Interface โดยมี PE1 และ PE2 ทำหน้าที่ในการส่งผ่านข้อมูลที่มี Label จาก Provider Edge Router ซึ่งอยู่ในลำดับชั้นการกระจาย (Distribution Layer) โดยข้อมูล IP Packet จะถูกเพิ่มและถอด Label ที่ Provider Edge Router และในส่วน Routing Protocol ที่ใช้กำหนดเส้นทางในการลำเลียง Label จะใช้ IS-IS ซึ่งเป็น Routing Protocol แบบ Interior Gateway Protocol (IGP) การกำหนดค่าพารามิเตอร์สำหรับการใช้งาน MPLS แสดงในตารางที่ 3.1

ตารางที่ 3.1 แสดงการตั้งค่าการใช้งาน MPLS และ TE ในโครงข่าย MPLS

Command	วัตถุประสงค์
mpls traffic-eng tunnels	Enable MPLS รองรับ TE Tunnel
mpls traffic-eng ds-te mode ietf mpls traffic-eng ds-te bc-model mam	เลือกโหมดของ Bandwidth Constraints (BC)
mpls label protocol ldp	ใช้ Protocol ในการกระจาย Label แบบ ldp

ตารางที่ 3.1 (ต่อ)

router isis net49.0001.0020.0200.2002.00 is-type level-2-only metric-style wide nsf ietf passive-interface Loopback0	เป็นการตั้งค่าของ Routing is-is ที่เป็น IGP ของโครงข่าย MPLS
mpls traffic-eng router-id Loopback0	กำหนดให้ IP Loopback 0 เป็น router-id ของ MPLS-TE
mpls traffic-eng level-2	กำหนดให้ MPLS TE ทำงานในชั้น Level 2 ตาม routing IGP

3.2.2 การกำหนดข้อตกลงระดับบริการ (Service Level Agreement) ของช่อง Video

เพื่อทดสอบประสิทธิในด้านการรับประกันคุณภาพของบริการของช่อง Video โดยเฉพาะอย่างยิ่งขณะที่โครงข่าย MPLS เกิดความคับคั่ง จึงได้มีการกำหนดข้อตกลงระดับการให้บริการ (SLA) ของช่อง Video เพื่อทดสอบประสิทธิภาพความน่าเชื่อถือ (Reliability) ของโครงข่าย MPLS ที่มีการใช้กลไกการควบคุมคุณภาพการให้บริการในด้านค่าแพ็กเก็ตสูญเสีย (Packet Loss), ค่าความล่าช้าเวลา (Latency) และค่าแปรผันความล่าช้าทางเวลา (Jitter) ดังข้อมูลในตารางที่ 3.2

ตารางที่ 3.2 แสดงการกำหนดค่า SLA ของช่อง Video ที่ใช้ทดสอบ

SLA ของช่อง Video	คุณภาพการให้บริการที่รับประกัน	ขนาดช่องสัญญาณ
Gold	รับประกัน Bandwidth, มี Packet Loss น้อย, มี Delay ต่ำ และมีค่า Jitter ต่ำ	50 Mbps
Silver	รับประกัน Bandwidth, Packet Loss ปานกลาง , Delay ปานกลาง, Jitter ปานกลาง	30 Mbps
Bronze	ไม่รับประกัน	20 Mbps

3.2.3 แบบจำลองของกลไกการควบคุมคุณภาพการให้บริการโดยใช้ DS-TE

DiffServ-aware Traffic Engineering (TE) จะเป็นการจองช่องสัญญาณ (Bandwidth Allocation), การบังคับเส้นทาง (Constrain-Based Routing) และการควบคุมสิทธิ (Admission Control) ซึ่ง DS-TE เรียกว่า Class-Type (CT) การแบ่งชั้น (Class) ของท่อเสมือน (Tunnel) ตาม

ข้อตกลงระดับบริการ (Service Level Agreement) ในตารางที่ 3.2 เพื่อแบ่งลำดับความสำคัญของแต่ละท่อเสมือนของช่อง Video ในตารางที่ 3.3 ที่อุปกรณ์ Provider Edge (PE1 และ PE2) และในส่วนการกำหนดค่า Bandwidth Constraint (BC) ที่ใช้ในการจองแบนวิดค์ ในการสร้าง Traffic Engineering (TE) ของกลไกการควบคุมคุณภาพการให้บริการโดยใช้ DS-TE จะกำนดค่า Sub-Pool (BC1) เป็น 100 Mbps และค่า Global Pool (BC0) เป็น 150 Mbps โดยวิธีการกำนดค่า BC จะใช้วิธีแบบ Maximum Allocation Model (MAM) การกำหนดค่าพารามิเตอร์ต่าง ๆ รวมถึงการกำนดค่า Sub-Pool แสดงอยู่ในตารางที่ 3.4

ตารางที่ 3.3 แสดงการจัดลำดับความสำคัญของ Tunnel ตาม CT ของแต่ละช่อง Video

Command	วัตถุประสงค์
PE1# interface Tunnel10 description For Traffic Video Chanel 1 load-interval 30	สร้าง Interface Tunnel ตาม CT เพื่อส่งช่อง Video บน PE 1
ip unnumbered Loopback0	กำหนดใช้ IP Loopback 0 ซึ่งไม่ใช่หมายเลขเดียวกับ Router-id
tunnel destination 2.2.2.2	กำหนด IP ปลายทางของ Tunnel
tunnel mode mpls traffic-eng	ให้ Tunnel ถูกห่อหุ้ม (encapsulation) ใน MPLS-TE
tunnel mpls traffic-eng priority 0 0	กำหนดลำดับความสำคัญในการจองสิทธ์ของ Tunnel
tunnel mpls traffic-eng bandwidth 50000 class-type 1	กำหนดแบนด์วิดค์ของ Tunnel ที่แบ่งจาก Sub-Pool
tunnel mpls traffic-eng path-option 10 dynamic	เลือกเส้นทางในการส่งทราฟฟิคของ MPLS-TE
tunnel mpls traffic-eng record-route	แสดงเส้นทางในการส่งทราฟฟิคขอแต่ละ Hop
interface Tunnel20 description For Traffic Video Chanel 2 ip unnumbered Loopback0 load-interval 30 tunnel destination 2.2.2.2 tunnel mode mpls traffic-eng tunnel mpls traffic-eng priority 0 0	ในการสร้าง Interface Tunnel 20 จะเหมือน Interface Tunnel 10 จะกำหนดแบนด์วิดค์ของช่อง Silver

ตารางที่ 3.3 (ต่อ)

tunnel mpls traffic-eng bandwidth 30000 class-type 1 tunnel mpls traffic-eng path-option 10 dynamic tunnel mpls traffic-eng record-route	
interface Tunnel30 description For Traffic Video Chanel 3 ip unnumbered Loopback0 load-interval 30 tunnel destination 2.2.2.2 tunnel mode mpls traffic-eng tunnel mpls traffic-eng priority 0 0 tunnel mpls traffic-eng bandwidth 20000 class-type 1 tunnel mpls traffic-eng path-option 10 dynamic tunnel mpls traffic-eng record-route	ในการสร้าง Interface Tunnel 30 จะเหมือน Interface Tunnel 10 จะกำหนดแบนด์วิดด์ของช่อง Bronze

ตารางที่ 3.4 แสดงการกำหนดค่า Sub-Pool และ Global-Pool ที่ PE1 และ PE2

Command	วัตถุประสงค์
PE1# interface GigabitEthernet3/0/0 description PE1---->P1 mtu 9000 ip address 10.10.10.2 255.255.255.252 ip router isis isis circuit-type level-2-only load-interval 30 negotiation auto	กำหนดให้ Interface ที่ PE1 ใช้ Routing IGP แบบ IS-IS โดยจะทำงานใน Level 2
mpls traffic-eng tunnels	Enable MPLS TE Tunnel ที่ Interface บน PE1
mpls ip	Enable MPLS ที่ Interface บน PE1
ip rsvp bandwidth mam max-reservable-bw	Enable RSVP ที่ Interface เพื่อกำหนดแบนด์-

ตารางที่ 3.4 (ต่อ)

150000 bc0 150000 bc1 100000	วิดด์ โดยใช้วิธีแบ่ง BC (Bandwidth Constraint) แบบ MAM (Maximum Allocation Model) ซึ่งจะมีการกำหนดค่า Global-Pool (BC0) และค่า Sub-Pool (BC1) โดยค่า BC0 จะเป็นค่าแบนด์วิดด์รวมของ Tunnel ทั้งหมดที่ RSVP สามารถจองแบนด์วิดด์ได้
PE2# interface GigabitEthernet3/0/0 description PE2--->P2 mtu 9000 ip address 20.20.20.2 255.255.255.252 ip router isis load-interval 30 negotiation auto mpls traffic-eng tunnels mpls ip cdp enable clns mtu 1497 isis circuit-type level-2-only ip rsvp bandwidth mam max-reservable-bw 150000 bc0 150000 bc1 100000	ในการจองแบนด์วิดด์ Global-Pool และ Sub-Pool ของ PE2 จะมีขั้นตอนเหมือน PE1

3.2.4 แบบจำลองกลไกควบคุม QoS โดยใช้ PHB

คุณสมบัติของ PHB จะรองรับ DiffServ (Different Service) ที่มีการแบ่งกลุ่มของแต่ละ Application โดยใช้ DSCP (DiffServ Code Point) เป็นตัวพิจารณาในการกำหนดนโยบาย (Policy) ในการจัดลำดับ (Priority) ที่จะส่งไปในแต่ละ Hop ซึ่ง PHB จะแสดงถึงรายละเอียดค่า Latency, Jitter หรือการสูญหายของ Packet ที่จะต้องได้รับเมื่อผ่านไปยัง DiffServ Node โดย PHB กลุ่มหนึ่งๆ อาจมี PHBs เกี่ยวข้องจำนวนมาก และอาจดำเนินการทำ PHB พร้อมกันตั้งแต่หนึ่งชุดหรือมากกว่าก็ได้ ใน PHB สามารถแบ่ง DiffServ Specification ออกเป็น การ Expedited Forwarding (EF), Assured Forwarding (AF1, AF2, AF3 และ AF4), Class Selector (CS) และ Default Node

- **Expedited Forwarding (EF)**

EF PHB เป็นค่า Latency, Jitter และการสูญเสีย Packet ขั้นต่ำที่ DiffServ Node ต้องทำให้ได้ PHB ดังกล่าวเป็นเสมือนขอบจำกัดขั้นต่ำของการส่งข้อมูลแบบ Real-Time ผ่าน DiffServ Domain ซึ่ง DiffServ Node จะต้องรักษาการให้บริการ EF ให้มีอัตราเร็วกว่าอัตราที่ EF เข้าถึงอยู่เสมอโดยไม่ขึ้นกับจำนวน Non-EF-Traffic ความแตกต่างระหว่างอัตราการเข้าถึงกับอัตราการให้บริการดังกล่าวทำให้ Packet ทั้งสองไม่ปะทะกันหรือเกิดการคั่งค้าง ส่งผลให้ Latency มีค่าต่ำสุด ทั้งนี้ Latency ประเภทนี้เป็นสาเหตุหลักของการ Latency และ Jitter ของ Packet ระหว่างการปฏิบัติการของ Node การมีความแออัดของคิวต่ำ นอกจากจะทำให้ Latency และ Jitter ต่ำแล้ว ยังทำให้การสูญเสียของ Packet ต่ำลงอีกด้วยเนื่องจาก Packet Buffers ไม่เกิดความคับคั่ง ทั้งนี้ที่จุด DiffServ Node ไม่ควรมีการ Reorder ของ Microflows รายละเอียดของ PHB สามารถอ่านเพิ่มเติมได้จาก RFC 3246 และ RFC 3247

- **Assured Forwarding (AF)**

AF จัดอยู่ในกลุ่มของ PHB มีหน้าที่กำหนดการรับประกัน Forwarding ที่ DiffServ Node จะต้องรองรับ (มี 4 กลุ่ม) กล่าวง่ายๆ คือ เป็นการกำหนดทางเลือก, วิธีการให้ DiffServ Node รับประกันการสูญเสียของ Packet นั่นเอง AF PHB ทั้ง 4 กลุ่มประกอบด้วย AF1, AF2, AF3 และ AF4 โดยในแต่ของกลุ่ม AF ยังแบ่งระดับการทิ้ง Packet (Drop-Precedence) ออกเป็น 3 ระดับ ทั้งนี้หาก Resource (Bandwidth, Buffers) เกิดการล้นหรือรับ Packet ไม่ทัน DiffServ Node จะทิ้ง Packet ที่มีระดับการ Drop ต่ำก่อน

ระดับการ Drop ทั้ง 12 ระดับของ AF PHB แสดงอยู่ดังตารางที่ 3.5 รายละเอียดการกำหนดเซต PHB เหล่านี้สามารถอ่านเพิ่มเติมได้จาก RFC 2597

AF PHB ทั้ง 4 กลุ่มทำงานเป็นอิสระต่อกัน โดยไม่มีผลต่อการ Forwarding Guarantee ของอีกกลุ่ม และไม่มีผลต่อค่า Latency หรือ Jitter ทั้งนี้การ Guarantee ของแต่ละกลุ่มจะขึ้นอยู่กับ Forwarding Resource ของ Node, จำนวนการจราจรที่เข้าถึง Node และผลสืบเนื่องที่จะเกิดจากการ Drop ของ Packet โดยพิจารณาจาก Bandwidth หรือพื้นที่ของ Buffer เป็นหลัก และกำหนดให้ Node ทำการ Forward ในอัตราสูงที่สุดเท่าที่จะทำได้เพื่อให้ระดับการ Drop Packet ต่ำ และไม่มีการ Reorder Packet ของ Microflows ที่ถูก Drop ไปแล้วอีก

ตารางที่ 3.5 แสดงระดับการ Drop ของ AF PHBs

Drop Precedence	AF1	AF2	AF3	AF4
Low	AF11	AF21	AF31	AF41
Medium	AF12	AF22	AF32	AF42
High	AF13	AF23	AF33	AF43

- **Class selectors (CS)**

DiffServ กำหนด CS PHBs ขึ้นเพื่อให้สามารถ Backward โดยใช้ IP Precedence ใน IPv4 TOS Octet ได้ Class Selector ทำหน้าที่รักษา Relative Ordering ของ IP Precedence ให้คงที่ (ค่ามากกว่าหมายถึง Relative Order สูงกว่า) โดย Node จะต้องทำการ Forwarding ไปยัง CSs ด้วยอัตราสูงสุดเท่าที่จะทำได้ เพื่อป้องกันไม่ให้ Latency, Jitter หรือการสูญเสีย Packet มีค่าเกินกว่าที่กำหนด ตารางที่ 3.6 แสดงการ Mapping ระหว่าง CSs กับ IP Precedence

ตารางที่ 3.6 แสดงการ Mapping ระหว่าง CSs กับ IP Precedence

PHB	DSCP (Decimal)	DSCP (Binary)	Precedence Name	Precedence (Binary)	Precedence (Decimal)
CS7	56	111000	Network Control	111	7
CS6	48	110000	Internetwork Control	110	6
CS5	40	101000	Critic/ECP	101	5
CS4	32	100000	Flash Override	100	4
CS3	24	011000	Flash	011	3
CS2	16	010000	Immediate	010	2
CS1	8	001000	Priority	001	1
CS0	0	000000	Routine	000	0

Default PHB

DiffServ Domain กำหนด Default PHB ขึ้นเพื่อรองรับบริการ Best-Effort Service กล่าวคือ สถาปัตยกรรมกำหนด Default PHB ขึ้นเพื่อให้เป็นไปตาม Best-Effort Service ที่ RFC 1812 ระบุ ซึ่งหมายความว่า DiffServ Domain จะต้องทำการ Forward จำนวน Packet ให้มากที่สุดเท่าที่จะทำได้ โดยไม่เกิด Latency, Jitter และการสูญเสีย Packet มากเกินกว่าที่กำหนด ทั้งนี้การทำ PHBs ก็อยู่ภายใต้ Best-Effort Service นี้เช่นกัน

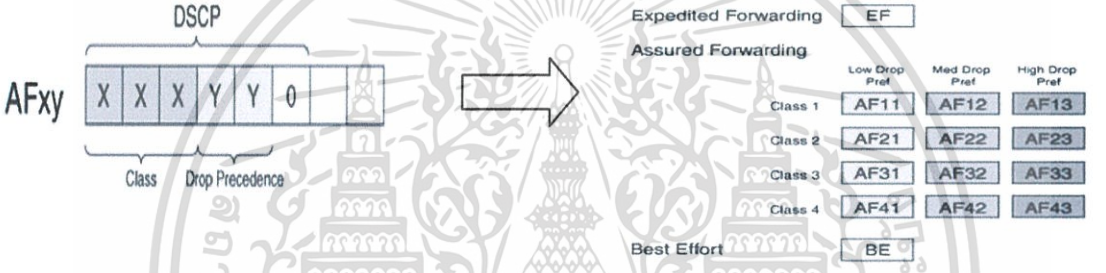
3.3 การกำหนดค่านโยบาย (Policy) ของกลไกการควบคุมคุณภาพการให้บริการที่อุปกรณ์ในระดับชั้นกระจายข้อมูล (Distribution Layer)

ค่าพารามิเตอร์ในการกำหนดเงื่อนไข เพื่อกำหนดความสำคัญของ Application ที่ใช้ทดสอบ โดยจะมีขั้นตอนของแต่ละกลไกดังนี้

3.3.1 การคัดเลือกและกำหนดค่าลำดับความสำคัญ (Classification and Marking)

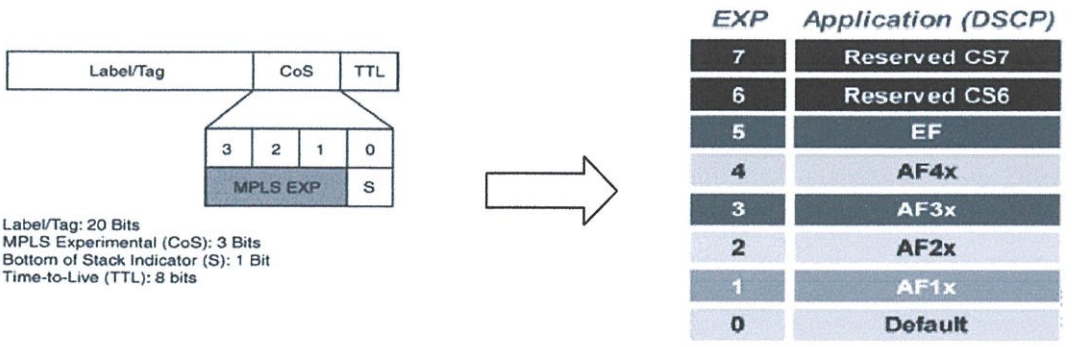
ในการคัดแยก (Classification) และการกำหนดค่าเพื่อจัดลำดับความสำคัญ (Marking) ของแต่ละ Application ซึ่งกลไกการควบคุมคุณภาพการให้บริการทั้ง 2 วิธีจะมีการคัด

แยก (Classification) และการกำหนดเพื่อจัดลำดับความสำคัญ (Marking) ดังนี้ กลไกควบคุมคุณภาพการให้บริการโดยใช้ PHB จะใช้ค่า DSCP ซึ่งเป็นค่าที่ใช้ในการกำหนดชนิดของการให้บริการ โดย จะใช้ 3 บิตของค่า DSCP เพื่อแบ่งชนิดของบริการและกำหนดค่าเป็น 4 ประเภท คือ แบบส่งรวดเร็ว (Expedite Forwarding) กำหนดค่า DSCP = EF, แบบรับประกันการส่ง (Assured Forwarding) กำหนดค่า DSCP = AFxy และแบบพยายามที่สุด (Best Effort) กำหนดค่า DSCP = BE โดย Application ประเภท Video ที่ใช้ในการทดสอบจะถูกจัดอยู่ในประเภท AFxy ซึ่งค่า x จะเป็นชนิดของบริการ ส่วน y จะเป็นลำดับความสำคัญของบริการนั้น โดยช่อง Video ที่ใช้ในการทดสอบจะถูกกำหนดค่าเป็น ช่อง Gold (AF31), ช่อง Silver (AF32), ช่อง Bronze (AF33) และ ทราฟฟิคที่เป็นข้อมูลคอมพิวเตอร์จะไม่มีการรับประกันคุณภาพการให้บริการ โดยจะถูกจัดให้เป็นข้อมูลประเภท BE วิธีการแบ่งบริการและจัดลำดับความสำคัญแสดงในรูปที่ 3.2



รูปที่ 3.2 แสดงการแบ่งชนิดบริการและการจัดลำดับความสำคัญใน PHB

กลไกการควบคุมคุณภาพการให้บริการโดยใช้ DS-TE จะใช้ค่า EXPerimental Bit (EXP) ซึ่งเป็นฟิลด์ที่อยู่ใน MPLS Label เป็นตัวกำหนดชนิดของบริการและบอกถึงความสำคัญของแพ็กเก็ต ซึ่งจำนวณบิตของ EXP มีค่าเป็น 3 บิต ดังแสดงในรูปที่ 3.3 ทำให้สามารถแบ่งประเภทบริการและจัดลำดับความสำคัญได้ถึง 8 (2^3) ประเภท ในการทดสอบช่อง Video แต่ละช่องจะคัดเลือกและกำหนดค่า EXP ของช่อง Gold = 5, ช่อง Silver = 4, ช่อง Bronze = 3 และ ทราฟฟิคไม่รับประกัน QoS จะมีค่า EXP = 0 ตามลำดับ



รูปที่ 3.3 แสดงถึงประเภทของบริการที่ถูกกำหนดโดยบิต EXP

3.3.2 การจัดการความคับคั่ง (Congestion Management)

ในระดับชั้น Layer 3 ของ OSI จะเป็นชั้นของ IP Packet จะอาศัยการจัดคิว (Queuing) ขาเข้า (In Bound) ของระดับชั้นการกระจาย (Distribution Layer) PE1 เพื่อจัดแถวของ IP Packet แล้วส่งไปยังระดับชั้นแกนกลาง (Core Layer) ตามลำดับความสำคัญดังแสดงในรูปที่ 3.4

รูปที่ 3.4 แสดงการจัดการคิวข้อมูลด้านขาเข้า

Application ประเภท Real-Time จะใช้การจัดคิวแบบการจัดลำดับความสำคัญเฉพาะ (Strict Priority หรือ Priority Queuing) ซึ่งเน้นเรื่องการรับประกันขนาดช่องสัญญาณ (Bandwidth Guarantee) และรับประกันค่าความล่าช้าทางเวลา (Latency Guarantee) โดยกลไกควบคุมคุณภาพการให้บริการโดยใช้ PHB จะใช้การจัดการคิวข้อมูลแบบ Class-Based Weighted Fair Queuing (CBWFQ) ซึ่ง CBWFQ จะสัมพันธ์กับความน่าจะเป็นในการ Drop (Probability Drop) ที่พิจารณาค่า DSCP ของ IP Packet ส่วนกลไกควบคุมคุณภาพการให้บริการโดยใช้ DS-TE จะใช้ Priority Queuing (PQ) เป็นตัวจัดแถวของแพ็กเก็ต ซึ่งจะพิจารณาจากค่า MPLS EXP ของทราฟฟิคขาเข้า วิธีการจัดแถวของทั้ง 2 กลไกการควบคุมคุณภาพการให้บริการแสดงอยู่ในตารางที่ 3.7 โดยจะถูกนำไปใช้ที่ Interface Gi3/0/0 ของ PE1 ซึ่งจะเชื่อมต่อเข้าระดับชั้นแกนกลาง (Core Layer) P1 ที่ Interface Gi1/0/0

ตารางที่ 3.7 แสดงการกำหนดนโยบายการจัดการความคับคั่ง (Congestion Management)

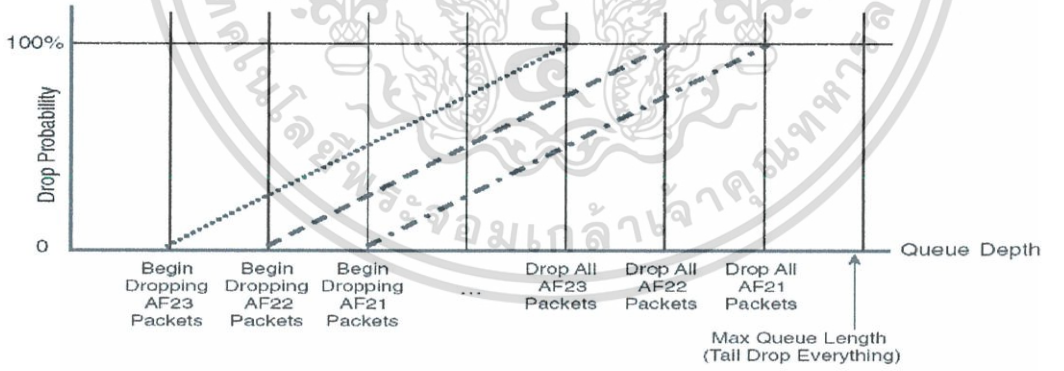
กลไกการควบคุมคุณภาพการให้บริการโดยใช้ PHB	กลไกการควบคุมคุณภาพการให้บริการโดยใช้ DS-TE
policy-map video	policy-map out-exp
class video-ch1	class exp-5-traffic
bandwidth 50000	priority 50000
class video-ch2	class exp-3-traffic
bandwidth 30000	priority 30000
class video-ch3	class exp-2-traffic
bandwidth 20000	priority 20000

ในการจัดการความคับคั่ง (Congestion Management) กลไกควบคุม QoS จะต้องกำหนดค่าให้สัมพันธ์กับการหลีกเลี่ยงการเกิดความคับคั่ง (Congestion Avoidance) ที่มีการกำหนดค่านโยบายในการสุ่ม Drop โดยกลไกควบคุม QoS โดยใช้ PHB จะพิจารณาค่าแบนด์วิดของแต่ละช่อง Video ที่ผ่านการสุ่ม Drop ตามการกำหนดค่านโยบาย (Policy) แบบ WRED และทำการส่งผ่านทราฟฟิคของช่อง Video ตามลำดับความสำคัญตามค่า PHB DSCP (AFxy) ของแต่ละช่อง Video

ส่วนกลไกควบคุม QoS โดยใช้ DS-TE จะพิจารณาค่า MPLS-EXP ซึ่งจะถูกกำหนดจากการกำหนดค่านโยบาย (Policy) ในการสุ่ม Drop ของ DS-TE ในวิธีการของ WRED โดยจะมีการจัดลำดับความสำคัญ (Priority) ของแต่ละช่อง Video

3.3.3 การหลีกเลี่ยงการเกิดความคับคั่ง (Congestion Avoidance)

เมื่อโครงข่าย MPLS เกิดความคับคั่งขึ้น การหลีกเลี่ยงเพื่อไม่ให้เกิดความคับคั่งที่ดีที่สุดคือ การสุ่มเพื่อทิ้ง IP แพ็กเก็ต (Random Drop) ที่ขาเข้าของระดับชั้นกระจาย (Distribution Layer) ที่เชื่อมต่อกับระดับชั้นการเข้าถึง (Access Layer) เทคนิคในการสุ่ม Drop ของกลไกควบคุม QoS โดยใช้ PHB และกลไกควบคุม QoS โดยใช้ DS-TE จะใช้วิธี Weighted Random Early Detection (WRED) ซึ่งจะมีการกำหนดค่า Threshold ต่ำสุดในการเริ่มต้นในการสุ่ม Drop Packet จนถึงระดับค่า Threshold สูงสุดในการสุ่ม Drop Packet ดังแสดงในรูปที่ 3.5



รูปที่ 3.5 แสดงความน่าจะเป็นในการทิ้งแพ็กเก็ตของ AF แบบต่าง ๆ

โดยจะนำไปใช้งานที่ระดับกระจาย (Distribution Layer) PE1 โดยใช้ที่ Interface Gi3/0/4 ซึ่งทำหน้าที่รับทราฟฟิคของช่อง Video ทั้ง 3 ช่อง ที่ใช้ทดสอบ โดยจะรับทราฟฟิคจาก IP Traffic Generator ที่ส่งเข้ามา จะกำหนดค่านโยบายของ WRED ของกลไกควบคุม QoS ทั้ง 2 วิธี ตามตารางที่ 3.8

ตารางที่ 3.8 แสดงการกำหนดค่าในการสุ่ม Drop โดยใช้ WRED

PHB	policy-map video-in class video-ch1 police 50000000 conform-action transmit exceed-action drop class video-ch2 police 30000000 conform-action transmit exceed-action drop class video-ch3 police 20000000 conform-action transmit exceed-action drop
DS-TE	policy-map sla-input class sla-1-class police 50000000 conform-action set-mpls-exp-transmit 5 exceed-action drop class sla-2-class police 30000000 conform-action set-mpls-exp-transmit 3 exceed-action drop class sla-3-class police 20000000 conform-action set-mpls-exp-transmit 2 exceed-action drop

จากตารางที่ 3.8 ในการกำหนดค่านโยบาย (Policy) ในการสุ่ม Drop ตามวิธีการทำงานของ WRED ในกลไกควบคุม QoS โดยใช้ PHB จะกำหนดค่านโยบายในการ Drop จะจำกัดแบนด์วิดท์ของแต่ละช่อง Video ตาม SLA ในตารางที่ 3.2 ตามเงื่อนไขในการพิจารณา Drop ทราฟฟิคของแต่ละช่อง Video ในการทดสอบจะใช้ช่อง Gold ทดสอบ ถ้าทราฟฟิคของช่อง Gold เข้ามาปรกติก็จะปล่อยผ่าน แต่ถ้าทราฟฟิคของช่อง Gold เกินจากค่า SLA ในส่วนทราฟฟิคที่เกินก็จะถูก Drop

ในส่วนกลไกควบคุม QoS โดยใช้ DS-TE ในการกำหนดค่านโยบาย (Policy) ในการสุ่ม Drop จะคล้ายกับกลไกควบคุม QoS โดยใช้ PHB แต่จะเพิ่มการใส่ค่า MPLS-EXP เพื่อแบ่งระดับความสำคัญของแต่ละช่อง และให้สัมพันธ์ในการจัดลำดับ (Priority) ในการส่งทราฟฟิคในการจัดการความคับคั่ง (Congestion Management)

3.4 การกำนดค่าตัวแปรที่ใช้ในการประเมินคุณภาพของการให้บริการ

Application แบบ Real-Time ประเภท Video ที่ทดสอบในวิทยานิพนธ์ฉบับนี้ ต้องการคุณภาพของบริการ ดังนี้

- มีค่าแพ็กเก็ตสูญเสียไม่เกิน 1% ของแบนด์วิดท์ที่ใช้งาน
- มีค่าความล่าช้าทางเวลาทางเดียว (One-way Latency) ไม่เกิน 150 ms
- มีค่าแปรผันความล่าช้าทางเวลา (Jitter) ไม่เกิน 30 ms

ในวิทยานิพนธ์นี้ จะทำการทดสอบเพื่อประเมินวิธีการควบคุมคุณภาพการให้บริการแบบ PHB และ DS-TE เทียบกับแบบ BE โดยจะเปรียบเทียบจากพารามิเตอร์ดังนี้

- ค่าแพ็กเก็ตสูญเสีย (Packet Loss)
- ค่าความล่าช้าทางเวลาทางเดียว (One-way Latency)
- ค่าแปรผันความล่าช้าทางเวลา (Jitter)

โดยผลทั้งหมดจะถูกอ่านจากเครื่องมือวัด ยี่ห้อ Agilent รุ่น N2X ซึ่งถูกติดตั้งอยู่ที่ปลายทาง (ทำหน้าที่แทน CE21) โดยระหว่างที่ทดสอบจะจำลองข้อมูลประเภทที่เป็น BE เข้ามาในระบบ และเพิ่มอัตราการส่งข้อมูลจนกระทั่งเกิดความคับคั่งขึ้นในโครงข่าย นั่นคือจำเป็นต้องมีการทิ้งแพ็กเก็ตข้อมูลที่อยู่ภายในระบบ

บทที่ 4
ผลการทดสอบและการวิจารณ์ผล

เนื่องจากในวิทยานิพนธ์ฉบับนี้ใช้เครื่องมือวัดในการจำลองข้อมูลที่เป็นช่อง Video และข้อมูล ซึ่งได้ใช้เครื่องมือวัด Agilent รุ่น N2X นั้นไม่สามารถจำลองข้อมูลช่อง Video ที่ควบคุมคุณภาพการให้บริการด้วยวิธี DS-TE และ PHB ได้พร้อมกัน ดังนั้นจึงได้แบ่งการทดสอบออกเป็น 4 กรณี ดังนี้

กรณีที่ 1 ช่อง Video ประเภท Gold ที่มีการควบคุมคุณภาพการให้บริการด้วยวิธี PHB และช่อง Video ประเภท Bronze ซึ่งเป็น BE

กรณีที่ 2 ช่อง Video ประเภท Gold ที่มีการควบคุมคุณภาพการให้บริการด้วยวิธี DS-TE และช่อง Video ประเภท Bronze ซึ่งเป็น BE

กรณีที่ 3 ช่อง Video ประเภท Silver ที่มีการควบคุมคุณภาพการให้บริการด้วยวิธี PHB และช่อง Video ประเภท Bronze ซึ่งเป็น BE

กรณีที่ 4 ช่อง Video ประเภท Silver ที่มีการควบคุมคุณภาพการให้บริการด้วยวิธี DS-TE และช่อง Video ประเภท Bronze ซึ่งเป็น BE

โดยในทุกกรณีจะมีการใช้ IP Traffic Generator สร้างทราฟฟิคประเภท BE โดยมีปริมาณทราฟฟิคขึ้นกับช่วงเวลา โดยมี 3 ช่วงเวลาได้แก่ ช่วงเวลา 0-60 วินาทีแรกจะส่งทราฟฟิคด้วยอัตรา 200 Mbps ช่วงเวลา 61-130 วินาที ส่งทราฟฟิคด้วยอัตรา 500 Mbps และท้ายสุดระหว่างเวลา 131-190 วินาที ส่งทราฟฟิคด้วยอัตรา 980 Mbps

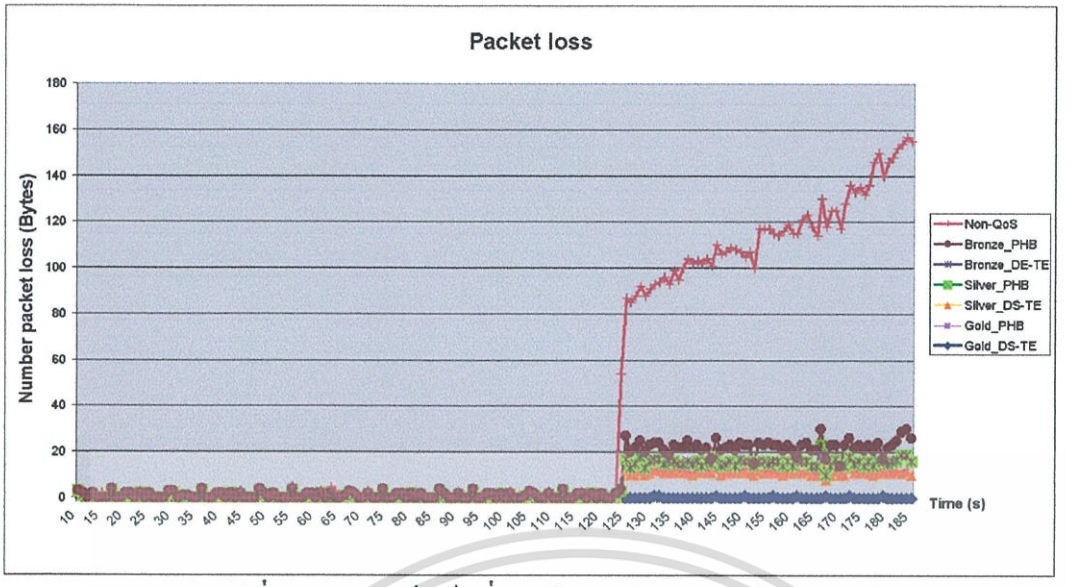
ดังนั้นในทุกกรณีช่วงเวลาที่ระบบจะเกิดความคับคั่ง คือช่วงระหว่างเวลา 131-190 วินาที เนื่องจากทราฟฟิคที่เข้าในโครงข่ายมีปริมาณทั้งสิ้น 50 + 15 + 980 = 1,045 Mbps ในขณะที่ระบบมีขนาดช่องสัญญาณเพียง 1,000 Mbps ดังนั้นในระบบที่ทดสอบช่วงเวลานี้จึงเหมาะสมที่สุดที่จะใช้เปรียบเทียบประสิทธิภาพการทำงานของวิธีควบคุมคุณภาพการให้บริการ

4.1 ผลการทดสอบ

เพื่อความชัดเจนในการเปรียบเทียบประสิทธิภาพการทำงานของวิธีควบคุมคุณภาพการให้บริการ กราฟในแต่ละกรณีต่อไปนี้จึงจะขอแสดงผลของในทุกกรณีในกราฟเดียวกัน

4.1.1 แพ็กเก็ตที่สูญเสีย

ผลการทดสอบแสดงอยู่ในรูปที่ 4.1



รูปที่ 4.1 แสดงแพ็กเก็ตที่สูญเสียของช่อง Video ในทุกกรณี

เพื่อความชัดเจนในการเปรียบเทียบ ตารางที่ 4.1 แสดงแพ็กเก็ตที่สูญเสียของช่อง Video ประเภท Gold

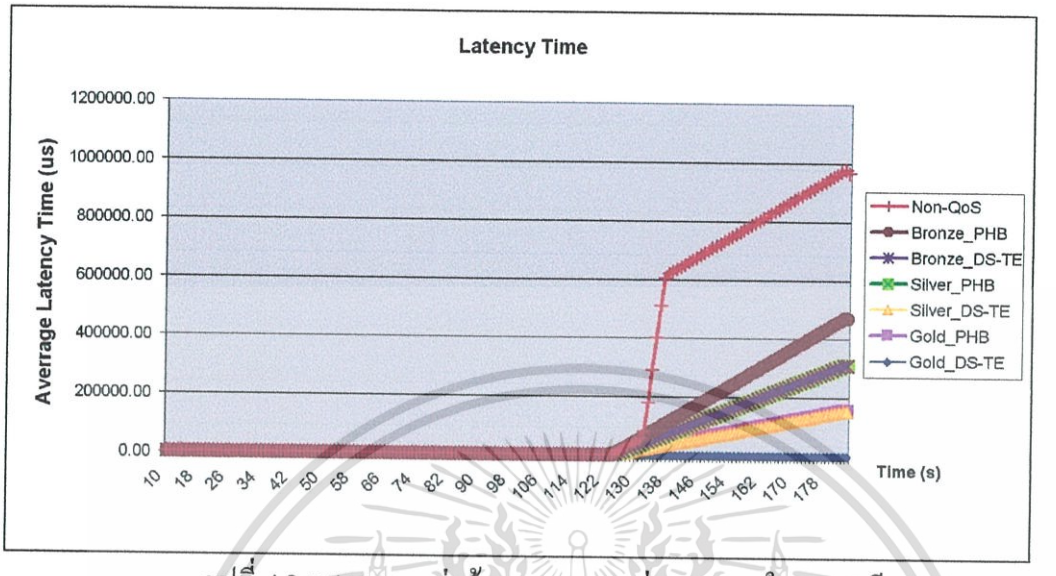
ตารางที่ 4.1 แสดงแพ็กเก็ตที่สูญเสียของช่อง Video ประเภท Gold

Mechanism	Tx Packet	Rx Packet	Packet Loss	%Packet Loss
PHB	50 Mbps	49.85 Mbps	0.15 Mbps	0.3 %
DS-TE	50 Mbps	49.98 Mbps	0.02 Mbps	0.04 %

จากรูปที่ 4.1 พบว่าช่วงเวลาที่ระบบไม่ได้เกิดความคับคั่ง (ช่วง 0-130 วินาทีแรก) นั้น ช่อง Video ทั้ง 3 ประเภท (Gold, Silver และ Bronze) รวมถึงข้อมูลประเภท BE จะมีการสูญเสียแพ็กเก็ตข้อมูลน้อย หรือแทบจะไม่มีเลย ระบบเริ่มจะมีการทิ้งแพ็กเก็ตเมื่อเกิดความคับคั่ง (ภายหลักวินาทีที่ 130) โดยจะเห็นได้ว่าแพ็กเก็ตข้อมูลที่เป็น BE จะถูกทิ้งมากที่สุด และเพิ่มขึ้นตามเวลา ในขณะที่แพ็กเก็ตของช่อง Video ทั้งสามก็มีจำนวนที่ถูกทิ้งมากขึ้น แต่ว่ายังสามารถควบคุมให้ค่อนข้างคงที่ได้ โดยช่อง Video ประเภท Gold จะมีการสูญเสียน้อยที่สุด รองลงมาคือประเภท Silver และ Bronze ตามลำดับ ในขณะที่ถ้าเปรียบเทียบกับช่อง Video ประเภทเดียวกัน วิธีควบคุมคุณภาพการให้บริการแบบ DS-TE จะมีการทิ้งแพ็กเก็ตในจำนวนที่น้อยกว่าแบบ PHB โดยเพื่อความชัดเจนผู้วิจัยได้เก็บและนำเสนอข้อมูลแพ็กเก็ตที่สูญเสียสำหรับ Video ประเภท Gold ทั้งวิธีควบคุมคุณภาพการให้บริการแบบ DS-TE และ PHB ในตารางที่ 4.1 ซึ่งแสดงให้เห็นว่าวิธี DS-TE สามารถรับประกันในประเด็นจำนวนแพ็กเก็ตที่สูญเสียได้ดีกว่าแบบ PHB เนื่องมาจากวิธี DS-TE นั้นสามารถรองรับการประกันคุณภาพการให้บริการแบบ end-to-end ได้ ในขณะที่วิธี PHB นั้นจะสามารถรับประกันคุณภาพการให้บริการได้เฉพาะแบบ Hop by Hop เท่านั้น

4.1.2 ค่าความล่าช้าทางเวลา

ผลการทดสอบแสดงอยู่ในรูปที่ 4.2

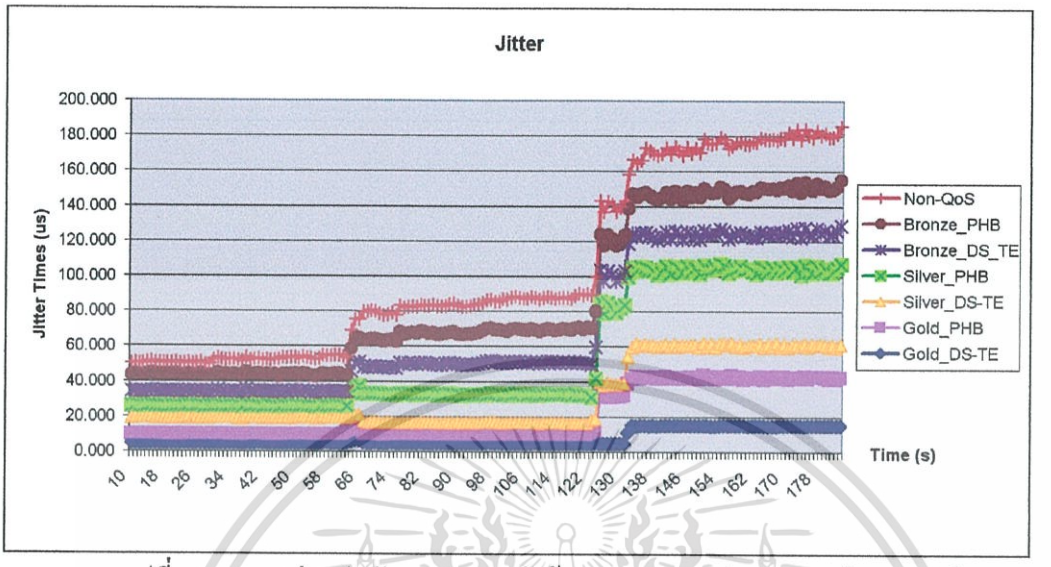


รูปที่ 4.2 แสดงความล่าช้าทางเวลาของช่อง Video ในทุกกรณี

จากรูปที่ 4.2 พบว่าช่วงเวลาที่ระบบไม่ได้เกิดความคับคั่ง (ช่วง 0-130 วินาทีแรก) นั้น ช่อง Video ทั้ง 3 ประเภท (Gold, Silver และ Bronze) รวมถึงข้อมูลประเภท BE จะมีค่าความล่าช้าทางเวลาน้อยมาก หรือแทบจะไม่มีเลย ระบบเริ่มจะมีการทิ้งแพ็กเก็ตเมื่อเกิดความคับคั่ง (ภายหลังวินาทีที่ 130) โดยจะเห็นได้ว่าแพ็กเก็ตข้อมูลที่เป็น BE จะมีความล่าช้าทางเวลามากที่สุด และเพิ่มขึ้นตามเวลา จนกระทั่งถึงวินาทีที่ 140 โดยประมาณค่าความล่าช้าทางเวลาของข้อมูล BE จะเพิ่มขึ้นในอัตราที่น้อยลง (สังเกตุจากความชันของกราฟที่น้อยลง) เหตุผลเนื่องมาจากมีการละทิ้งแพ็กเก็ตข้อมูลจำนวนมากของข้อมูล BE ทำให้จำนวนข้อมูลในบัฟเฟอร์น้อยลง ส่งผลให้ค่าความล่าช้าทางเวลาน้อยลง แพ็กเก็ตของช่อง Video ทั้งสาม (Gold แบบ PHB, Silver และ Bronze ทั้งแบบ DS-TE และ PHB) จะมีค่าความล่าช้าทางเวลามากขึ้น จนกระทั่งมากกว่าค่า 150 msec ที่เป็นข้อกำหนดใน SLA โดยมีข้อสังเกตุว่าการเพิ่มขึ้นของค่าความล่าช้าทางเวลาของวิธีควบคุมความคับคั่งประเภทเดียวกัน ช่องสัญญาณ Gold จะมีอัตราการเพิ่มของค่าความล่าช้าทางเวลาน้อยกว่าช่องสัญญาณ Silver และ Bronze ตามลำดับ จะมีเพียงแต่ช่อง Video ประเภท Gold แบบ DS-TE เท่านั้นที่สามารถควบคุมค่าความล่าช้าทางเวลาได้ เนื่องมาจากวิธี DS-TE นั้นสามารถรองรับการประกันคุณภาพการให้บริการแบบ end-to-end ได้ ในขณะที่วิธี PHB นั้นจะสามารถรับประกันคุณภาพการให้บริการได้เฉพาะแบบ Hop by Hop เท่านั้น

4.1.3 ค่าความแปรผันของค่าความล่าช้าทางเวลา

ผลการทดสอบแสดงอยู่ในรูปที่ 4.3



รูปที่ 4.3 แสดงค่าแปรผันของความล่าช้าทางเวลาของช่อง Video ในทุกกรณี

จากรูปที่ 4.3 พบว่าไม่ว่าในช่วงเวลาที่ระบบมีหรือไม่มีความคับคั่ง ค่าแปรผันของความล่าช้าทางเวลาของช่อง Video ทุกประเภท รวมถึงข้อมูลประเภท BE ต่างก็มีค่าต่ำกว่าค่าเป้าหมาย (30 msec) ทั้งสิ้น โดยสำหรับช่อง Video ในทุกประเภท (Gold, Silver และ Bronze) การควบคุมคุณภาพบริการด้วยวิธี DS-TE จะให้ค่าแปรผันความล่าช้าทางเวลาต่ำกว่าวิธี PHB เสมอ โดยทุก ๆ ครั้งที่ระบบมีปริมาณทราฟฟิคเพิ่มมากขึ้น (ที่เวลา 61 และ 131 วินาที) ทุก ๆ ช่อง Video และข้อมูลจะมีค่าแปรผันความล่าช้าทางเวลาเพิ่มขึ้นเล็กน้อยในทุกกรณี และจะมีค่าคงที่เพื่อปริมาณทราฟฟิคไม่เปลี่ยนแปลง

อย่างไรก็ตามในทางปฏิบัติในระบบจริง อัตราการส่งข้อมูลของข้อมูล BE จะมีอัตราไม่คงที่ รวมถึงอัลกอริธึมการเข้ารหัส (Encode) ข้อมูลภาพปัจจุบัน (เช่น MPEG4 หรือ H.264) เอง ก็จะให้อัตราการส่งข้อมูลที่ไม่คงที่เช่นเดียวกัน ดังนั้นในระบบใช้งานจริง ค่าแปรผันความล่าช้าทางเวลาโดยส่วนใหญ่จะมีค่าไม่คงที่ตลอดเวลา

4.2 วิจารณ์ผลการทดสอบระบบ

จากข้อมูลผลการทดสอบระบบในหัวข้อ 4.1 สามารถสรุปได้ดังนี้

4.2.1 การควบคุมคุณภาพการให้บริการสำหรับช่อง Video ทั้งแบบ DS-TE และ PHB ในโครงข่าย MPLS จะให้ผลที่ดีกว่า BE ทั้งในประเด็นของแพ็กเก็ตที่สูญหาย ค่าความล่าช้าทางเวลา และค่าแปรผันความล่าช้าทางเวลา

4.2.2 สำหรับช่อง Video ประเภทเดียวกัน การควบคุมคุณภาพการให้บริการด้วยวิธี DS-TE จะให้ผลลัพธ์ดีกว่าแบบ PHB เนื่องจาก DS-TE มีการจองขนาดช่องสัญญาณแบบ end-to-end ด้วยโปรโตคอล RSVP ในขณะที่ PHB นั้นจะรับประกันคุณภาพการให้บริการแบบ Hop by Hop เท่านั้น ดังนั้นอาจจะทำให้ไม่สามารถรับประกันคุณภาพการให้บริการในภาพรวมจากต้นทางถึงปลายทางได้

4.2.3 ในระบบที่ทดสอบ พารามิเตอร์ความแตกต่างจุดหนึ่งระหว่าง DS-TE และ PHB คือ นโยบายการส่งข้อมูลจากคิวข้อมูล (Queuing Policy) โดย Priority Queuing ซึ่งใช้ใน DS-TE จะให้ประสิทธิภาพที่ดีกว่าแบบ Class-Based Wight Fair Queuing (CBFWQ)

4.2.4 อย่างไรก็ตามกระบวนการ DS-TE และนโยบายการส่งข้อมูลจากคิวข้อมูลแบบ Priority Queuing มีความซับซ้อนในการใช้งานในทางปฏิบัติมากกว่าวิธีอื่น ๆ ทำให้ในบางกรณีอาจจะไม่สามารถใช้งานกับระบบใหญ่ ๆ หรือมีปริมาณทราฟฟิคปริมาณมาก ๆ ได้

บทที่ 5
สรุปผลและข้อเสนอเสนอแนะ

5.1 สรุปผล

จากการออกแบบ ติดตั้ง และตรวจวัดค่าคุณภาพการให้บริการของบริการ Video ซึ่งมีการควบคุมคุณภาพการให้บริการด้วยวิธี PHB และ DS-TE เมื่อเปรียบเทียบกับแบบ BE ในโครงข่าย MPLS แล้วพบว่า

- ในกรณีที่โครงข่ายไม่เกิดความคับคั่ง วิธี PHB, DS-TE และ BE ต่างก็สามารถควบคุมความล่าช้าทางเวลา ค่าแปรผันความล่าช้าทางเวลา และแพ็กเก็ตที่ถูกสูญเสีย ได้ตามที่กำหนดไว้ใน SLA (Service Level Agreement)
- ในกรณีที่โครงข่ายเกิดความคับคั่ง เฉพาะวิธี DS-TE เท่านั้นที่สามารถควบคุมแพ็กเก็ตที่ถูกทิ้ง ความล่าช้าทางเวลา และค่าแปรผันความล่าช้าทางเวลาได้ตามที่กำหนดใน SLA ในขณะที่วิธี PHB นั้นค่าแพ็กเก็ตที่สูญเสีย และค่าแปรผันความล่าช้าทางเวลาจะมีค่ามากขึ้น (เทียบกับกรณีที่ไม่เกิดความคับคั่งในโครงข่าย) แต่ว่าระบบยังคงสามารถควบคุมได้อยู่ ในขณะที่ค่าความล่าช้าทางเวลานั้นจะมีค่าเพิ่มขึ้นตลอดเวลา ไม่สามารถควบคุมได้ โดยเกิดจากความล่าช้าทางเวลาที่เกิดจากคิวข้อมูล และความล่าช้าทางเวลาที่เกิดจากการประมวลผลข้อมูลเป็นหลัก ส่วนของ BE นั้นค่าความล่าช้าทางเวลาจะเพิ่มขึ้นอย่างมาก ในขณะที่ค่าความแพ็กเก็ตที่สูญเสีย และค่าแปรผันความล่าช้าทางเวลาก็เพิ่มขึ้นจนถึงค่าหนึ่งก่อนที่จะคงที่
- การจัดการคิวข้อมูลแบบ Priority Queuing (PQ) มีผลต่อประสิทธิภาพการทำงานของระบบโดยรวม โดย PQ จะสามารถควบคุมคุณภาพการให้บริการ (แพ็กเก็ตที่สูญเสีย ความล่าช้าทางเวลา และค่าแปรผันความล่าช้าทางเวลา) ได้มีประสิทธิภาพมากกว่าการจัดการคิวข้อมูลด้วยวิธี Class-Based Weight Fair Queue (CBWFQ)

5.2 ข้อจำกัดของงานวิจัย

อย่างไรก็ตามวิทยานิพนธ์ฉบับนี้ยังมีข้อจำกัดอยู่บ้าง ได้แก่

5.2.1 ผลการทดสอบทั้งหมดทำในระบบ LAN แต่การใช้งานจริงระบบส่วนใหญ่จะเป็น WAN ซึ่งอาจจะทำให้ผลการใช้งานในโครงข่ายจริงแตกต่างจากผลการทดสอบในวิทยานิพนธ์ฉบับนี้บ้าง โดยสิ่งที่คาดการณ์ไว้คือส่วนของความล่าช้าทางเวลาและแพ็กเก็ตที่ถูกทิ้งในระบบอาจจะมีค่ามากกว่าผลการทดสอบอยู่บ้าง อันเนื่องมาจากผลของความล่าช้าทางเวลาเนื่องมาจากระยะทาง อย่างไรก็ตามสามารถที่จะนำข้อสรุปจากวิทยานิพนธ์นี้ไปเป็นแนวทางในการใช้งานจริงได้

5.2.2 ยังขาดการศึกษาถึงผลของตัวแปรบางตัวต่อประสิทธิภาพของระบบ เช่น

- นโยบายการทิ้งแพ็กเก็ต (Dropping Policy) ในกรณีที่เกิดความคับคั่ง
- ขนาดของ Global-Pool และ Sub-Pool ในกระบวนการ DS-TE
- ผลของอัลกอริธึม MAM และ RDM ใน DS-TE เป็นต้น

5.3 ข้อเสนอแนะสำหรับงานวิจัยในอนาคต

ข้อเสนอแนะสำหรับงานวิจัยในอนาคตที่เกี่ยวข้องกับการศึกษาเรื่องการรับประกันคุณภาพการให้บริการในโครงข่าย MPLS มีดังนี้

5.3.1 ควรจะทดสอบการทำงานของระบบที่เป็น WAN เพื่อให้สามารถประเมินประสิทธิภาพของวิธีการควบคุมคุณภาพการให้บริการในโครงข่ายที่มีลักษณะใกล้เคียงกับการใช้งานจริงมากที่สุด

5.3.2 ควรจะมีการศึกษาผลกระทบของตัวแปรอื่นที่อาจจะมีผลกระทบต่อประสิทธิภาพการทำงานของระบบ เช่น นโยบายการทิ้งแพ็กเก็ต ขนาดของ Global-Pool และ Sub-Pool ใน DS-TE และผลของอัลกอริธึม MAM และ RDM ใน DE-TE เป็นต้น

บรรณานุกรม

[1] T. Szigeti and C. Hattingh, "**End-to-End QoS Network Design**," Indianapolis, Indiana: Cisco Press, 2005.

[2] S. Alvarez, "**QoS for IP/MPLS Networks**," Indianapolis, Indiana : Cisco Press, 2006.

[3] E. Osborne and A. J. Simha, "**Traffic Engineering with MPLS**," Indianapolis, Indiana: Cisco Press, 2002.

[4] Student Guide "**Implementing Cisco Quality of Service (QoS)**," Indianapolis, Indiana: Cisco Press, 2004.

[5] D.L. Zhang and D. Inescu, "**QoS Performance Analysis in Deployment of DiffServ-aware MPLS Traffic Engineering**," IEE Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eight ACIS International Conference, July 30 2007-Aug. 1 2007

[6] F. L. Faucheur and W. Lai, "**Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering**," RFC 3564, July 2003.

[7] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski, "**Assured Forwarding PHB Group**," RFC 2597 (Proposed Standard), June 1999, updated by RFC 3260.

ภาคผนวก

ภาคผนวก ก.

คำสั่งที่ใช้ในการจัดสร้างโครงข่าย MPLS ใช้ในการทดสอบ

```
+************************************************************************
+       Implement configure for MPLS Network
+************************************************************************

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
                        Provider Edge (PE1)
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service counters max age 10
!
hostname PE1
!
boot-start-marker
boot system disk0:c7600s72033-adventerprisek9-mz.122-33.SRB2.bin
boot-end-marker
!
enable password cisco
!
no aaa new-model
ip subnet-zero
!
!
!
!

vtp mode transparent

interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
!

interface GigabitEthernet1/1
 mtu 1526
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet1/2
 ip address 10.5.3.111 255.255.255.0
 media-type rj45
!
interface GigabitEthernet3/0/0
 description PE1---->P1
 mtu 9000
 ip address 10.10.10.2 255.255.255.252
 ip router isis
 load-interval 30
```

```
 negotiation auto
 mpls traffic-eng tunnels
 mpls ip
 cdp enable
 clns mtu 1497
 isis circuit-type level-2-only
 service-policy output out-exp
 ip rsvp bandwidth mam max-reservable-bw 150000 bc0 100000 bc1 50000
!
interface GigabitEthernet3/0/1
 mtu 9000
 ip address 13.13.13.1 255.255.255.252
 ip router isis
 load-interval 30
 negotiation auto
 mpls ip
 cdp enable
 clns mtu 1497
 isis circuit-type level-2-only
!
interface GigabitEthernet3/0/2
 mtu 9000
 no ip address
 load-interval 30
 shutdown
 negotiation auto
 mpls ip
 cdp enable
 clns mtu 1497
 isis circuit-type level-2-only
!
interface GigabitEthernet3/0/3
 mtu 9000
 ip address 32.32.32.1 255.255.255.0
 ip router isis
 load-interval 30
 negotiation auto
!
interface GigabitEthernet3/0/4
 description *** Traffic from CE(Tester) ****
 ip address 111.111.111.1 255.255.255.252
 ip policy route-map ds-te
 load-interval 30
 negotiation auto
 service-policy input sla-input
!

!
interface Vlan1
 no ip address
 shutdown
!
```

```
router isis
 net 49.0001.0010.0100.1001.00
 is-type level-2-only
 metric-style wide
 nsf ietf
 passive-interface Loopback0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!

ip classless

mpls ldp router-id Loopback0
!
control-plane
!
!
line con 0
line vty 0 4
 session-timeout 120
 privilege level 15
 password cisco
 no login
!
!


%%% Classification and Marking Traffic %%%%

class-map match-all video-ch1
  match ip dscp af31
class-map match-all video-ch2
  match ip dscp af32
class-map match-all video-ch3
  match ip dscp af33


class-map match-all sla-1-class
  match access-group 110
class-map match-all sla-2-class
  match access-group 120
class-map match-all sla-3-class
  match access-group 130
class-map match-all video-ch1-class


access-list 110 permit ip host 10.10.10.2 host 42.42.42.2
access-list 120 permit ip host 20.20.20.2 host 42.42.42.2
access-llst 130 permit ip host 30.30.30.2 host 42.42.42.2

route-map VIDEO-CH3 permit 10
 match ip address 30
 set interface Tunnel30
```

```
!
route-map VIDEO-CH2 permit 10
 match ip address 20
 set interface Tunnel20
!
route-map VIDEO-CH1 permit 10
 match ip address 10
 set interface Tunnel10

!==========================================================
        Setup Policy for WRED (Congestion Avoidance)
!==========================================================

policy-map video-in
  class video-ch1
   police 50000000    conform-action transmit    exceed-action drop
  class video-ch2
   police 30000000    conform-action transmit    exceed-action drop
  class video-ch3
   police 20000000    conform-action transmit    exceed-action drop


policy-map sla-input
  class sla-1-class
   police 50000000    conform-action set-mpls-exp-transmit 5    exceed-action
drop
  class sla-2-class
   police 30000000    conform-action set-mpls-exp-transmit 3    exceed-action
drop
  class sla-3-class
   police 20000000    conform-action set-mpls-exp-transmit 2    exceed-action
drop


!==========================================================
         Setup Policy for CBWFQ (Congestion Management)
!==========================================================

  policy-map video
  class video-ch1
    bandwidth 50000
  class video-ch2
    bandwidth 30000
  class video-ch3
    bandwidth 20000

policy-map out-exp
  class exp-5-traffic
    priority 50000
  class exp-3-traffic
    priority 30000
  class exp-2-traffic
```

```
   priority 20000
!=============================================================
      Setup Tunnel for DS-TE
!=============================================================
interface Tunnel10
 description #### For Traffic Video Chanel 1 #####
 ip unnumbered Loopback0
 load-interval 30
 tunnel destination 2.2.2.2
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 50000 class-type 0
 tunnel mpls traffic-eng path-option 10 dynamic
 tunnel mpls traffic-eng record-route
!
interface Tunnel11
 description *** Test QoS PE1-->PE2
 ip unnumbered Loopback0
 shutdown
 tunnel destination 2.2.2.2
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 100000 class-type 1
 tunnel mpls traffic-eng path-option 10 dynamic
 tunnel mpls traffic-eng record-route
!
interface Tunnel20
 description #### For Traffic Video Chanel 2 #####
 ip unnumbered Loopback0
 load-interval 30
 tunnel destination 2.2.2.2
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 30000 class-type 1
 tunnel mpls traffic-eng path-option 10 dynamic
 tunnel mpls traffic-eng record-route
!
interface Tunnel30
 description #### For Traffic Video Chanel 3 #####
 ip unnumbered Loopback0
 load-interval 30
 tunnel destination 2.2.2.2
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 20000 class-type 1
 tunnel mpls traffic-eng path-option 10 dynamic
 tunnel mpls traffic-eng record-route
!
```

```
%%#################################################################
```

Provider (P1)

```
%%#################################################################
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service counters max age 10
!
hostname P1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
!
!
vtp mode transparent
mls ip multicast flow-stat-timer 9
mls flow ip interface-full
no mls flow ipv6
no mls acl tcam share-global
mls cef error action reset
mpls traffic-eng tunnels
mpls traffic-eng ds-te mode ietf
mpls traffic-eng ds-te bc-model mam
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
no mpls ip propagate-ttl forwarded
mpls label protocol ldp
!
!
spanning-tree mode pvst
spanning-tree extend system-id
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 101
```

```
!
!
!
!
!
!
interface Loopback0
 ip address 11.11.11.11 255.255.255.255
!
interface GigabitEthernet1/0/0
 description P1----->P2
 mtu 9000
 ip address 12.12.12.1 255.255.255.252
 ip router isis
 load-interval 30
 negotiation auto
 mpls traffic-eng tunnels
 mpls ip
 cdp enable
 clns mtu 1497
 isis circuit-type level-2-only
 ip rsvp bandwidth mam max-reservable-bw 150000 bc0 100000 bc1 50000
!
interface GigabitEthernet1/0/1
 description P1---->PE1
 mtu 9000
 ip address 10.10.10.1 255.255.255.252
 ip router isis
 load-interval 30
 negotiation auto
 mpls traffic-eng tunnels
 mpls ip
 cdp enable
 clns mtu 1497
 isis circuit-type level-2-only
 ip rsvp bandwidth mam max-reservable-bw 150000 bc0 100000 bc1 50000
!
interface GigabitEthernet1/0/2
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet1/0/3
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet1/0/4
 mtu 9000
 no ip address
 load-interval 30
 shutdown
```

```
 negotiation auto
 cdp enable
!
interface GigabitEthernet6/1
 no ip address
 shutdown
!
interface GigabitEthernet6/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router isis
 net 49.0001.0110.1101.1011.00
 is-type level-2-only
 metric-style wide
 nsf ietf
 passive-interface Loopback0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
ip classless
!
!
no ip http server
no ip http secure-server
!
!
!
mpls ldp router-id Loopback0
!
control-plane
!
!
line con 0
line vty 0 4
 privilege level 15
 password cisco
 login
!
exception crashinfo buffersize 80
!
end
```

%%###

Provider (P2)

%%###

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service counters max age 10
!
hostname P2
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
clock timezone BKK 7
logging event link-status default
ip subnet-zero
!
!

P2#sh run
Building configuration...

Current configuration : 2969 bytes
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service counters max age 10
!
hostname P2
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
clock timezone BKK 7
logging event link-status default
ip subnet-zero
!
!
!
!
vtp mode transparent
```

```
mls ip multicast flow-stat-timer 9
mls flow ip interface-full
no mls flow ipv6
no mls acl tcam share-global
mls cef error action reset
mpls traffic-eng tunnels
mpls traffic-eng ds-te mode ietf
mpls traffic-eng ds-te bc-model mam
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
no mpls ip propagate-ttl forwarded
mpls label protocol ldp
!
!
spanning-tree mode pvst
spanning-tree extend system-id
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 101,199
!
!
!
!
!
!
interface Loopback0
 ip address 22.22.22.22 255.255.255.255
!
interface GigabitEthernet1/0/0
 description P2---->P1
 mtu 9000
 ip address 12.12.12.2 255.255.255.252
 ip router isis
 load-interval 30
 negotiation auto
 mpls traffic-eng tunnels
 mpls ip
 cdp enable
 clns mtu 1497
 isis circuit-type level-2-only
 ip rsvp bandwidth mam max-reservable-bw 150000 bc0 100000 bc1 50000
!
```

```
interface GigabitEthernet1/0/1
 description P2---->PE2
 mtu 9000
 ip address 20.20.20.1 255.255.255.252
 ip router isis
 load-interval 30
 negotiation auto
 mpls traffic-eng tunnels
 mpls ip
 cdp enable
 clns mtu 1497
 isis circuit-type level-2-only
 ip rsvp bandwidth mam max-reservable-bw 150000 bc0 100000 bc1 50000
!
interface GigabitEthernet1/0/2
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet1/0/3
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet1/0/4
 no ip address
 shutdown
 negotiation auto
!
interface TenGigabitEthernet2/1
 switchport
 switchport access vlan 101
 switchport mode access
 load-interval 30
!
interface TenGigabitEthernet2/2
 no ip address
 shutdown
!
interface TenGigabitEthernet2/3
 switchport
 switchport access vlan 101
 switchport mode access
 load-interval 30
!
interface TenGigabitEthernet2/4
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
```

```
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router isis
 net 49.0001.0220.2202.2022.00
 is-type level-2-only
 metric-style wide
 nsf ietf
 passive-interface Loopback0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
ip classless
!
!
no ip http server
no ip http secure-server
!
!
!
mpls ldp router-id Loopback0
!
control-plane
!
!
line con 0
 logging synchronous
line vty 0 4
 privilege level 15
 password cisco
 login
!
exception crashinfo buffersize 80
!
End
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Provider Edge (PE2)

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service counters max age 10
!
hostname PE2
!
boot-start-marker
boot system flash disk0:c7600s72033-adventerprisek9-mz.122-33.SRB2.bin
boot-end-marker
!
enable secret 5 $1$.PSP$uTXpSUd1ATt7IA.VvwoHp/
enable password cisco
!
no aaa new-model
ip subnet-zero
!
!
!
!
vtp domain pe2.gigabit
vtp mode transparent
!
class-map match-all EF-OUT
  match ip dscp cs4  af41  ef  cs6  cs7
class-map match-all wuttest
 class-map match-all AF31-OUT
  match ip dscp cs3  af31
!
policy-map OUT
  class EF-OUT
    priority 50000
  class AF31-OUT
    bandwidth 35000
  class class-default
    bandwidth 15000
!
mls ip multicast flow-stat-timer 9
mls flow ip interface-full
no mls flow ipv6
mls qos
no mls acl tcam share-global
mls cef error action reset
mpls traffic-eng tunnels
mpls traffic-eng ds-te mode ietf
mpls traffic-eng ds-te bc-model mam
mpls ldp discovery targeted-hello accept
```

```
 no mpls ip propagate-ttl forwarded
 mpls label protocol ldp
 !
 !
 spanning-tree mode pvst
 no spanning-tree optimize bpdu transmission
 spanning-tree extend system-id
 diagnostic cns publish cisco.cns.device.diag_results
 diagnostic cns subscribe cisco.cns.device.diag_commands
 username cisco secret 5 $1$vIFP$19M.c84mHw.nXUPLLapqZ1
 !
 !
 redundancy
  mode sso
  main-cpu
   auto-sync running-config
 !
 vlan internal allocation policy ascending
 vlan access-log ratelimit 2000
 !
 vlan 9
 !
 vlan 100
  name vlan100
 !
 !
 !
 !
 !
 !
 !
 !
 interface Loopback0
  ip address 2.2.2.2 255.255.255.255
 !
 interface Loopback40
  ip address 40.40.40.40 255.255.255.255
 !
 interface GigabitEthernet1/1
  mtu 1526
  no ip address
  load-interval 30
  no cdp enable
 !
 interface GigabitEthernet1/2
  no ip address
  media-type rj45
 !
 interface GigabitEthernet3/0/0
  description PE2--->P2
  mtu 9000
  ip address 20.20.20.2 255.255.255.252
```

```
 ip router isis
 load-interval 30
 negotiation auto
 mpls traffic-eng tunnels
 mpls ip
 cdp enable
 clns mtu 1497
 isis circuit-type level-2-only
 ip rsvp bandwidth mam max-reservable-bw 150000 bc0 100000 bc1 50000
!
interface GigabitEthernet3/0/1
 mtu 9000
 ip address 13.13.13.2 255.255.255.252
 ip router isis
 load-interval 30
 shutdown
 negotiation auto
 mpls ip
 cdp enable
 clns mtu 1497
 isis circuit-type level-2-only
!
interface GigabitEthernet3/0/2
 mtu 9000
 no ip address
 load-interval 30
 shutdown
 negotiation auto
 cdp enable
!
interface GigabitEthernet3/0/3
 mtu 9000
 ip address 192.168.2.10 255.255.255.0
 ip router isis
 load-interval 30
 negotiation auto
!
interface GigabitEthernet3/0/4
 ip address 42.42.42.1 255.255.255.0
 ip router isis
 load-interval 30
 negotiation auto
!
interface Vlan1
 no ip address
 shutdown
!
router isis
 net 49.0001.0020.0200.2002.00
 is-type level-2-only
 metric-style wide
 nsf ietf
```

```
 passive-interface Loopback0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
ip classless
!
!
no ip http server
no ip http secure-server
!
!
!
mpls ldp router-id Loopback0
!
control-plane
!
!
line con 0
line vty 0 4
 session-timeout 120
 privilege level 15
 password cisco
 no login
!
!
end
```

ภาคผนวก ข.

ผลงานวิจัยที่ได้รับการตีพิมพ์เผยแพร่

1. วิรัช ชัยขุนพล , **"กลไกควบคุมคุณภาพการให้บริการ โดยใช้ DiffServ-aware Traffic Engineering,"** วิศวกรรมสารลาดกระบัง, ปีที่ 26, ฉบับที่ 3, กันยายน, 2552.

วิศวสารลาดกระบัง
Ladkrabang Engineering Journal
คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ 10520
Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang,Bangkok 10520

วันที่ 14 กันยายน 2552

เลขที่อ้างอิง 1314

เรื่อง การตอบรับบทความ

เรียน คุณวิรัช ชัยขุนพล คณบดี เดชหาญ

ตามที่ท่านได้ส่งบทความเรื่อง กลไกควบคุมคุณภาพการให้บริการ โดยใช้ DiffServ-aware Traffic Engineering (Mechanism Control QoS Using DiffServ-aware Traffic Engineering) มาให้พิจารณาเพื่อลงตีพิมพ์ในวารสารวิศวสารลาดกระบัง บัดนี้ ผู้ทรงคุณวุฒิได้ทำการพิจารณาแล้วเห็นว่ายอมรับตีพิมพ์ได้ โดยจะตีพิมพ์ในปีที่ 26 ฉบับที่ 3 เดือนกันยายน 2552

จึงเรียนมาเพื่อทราบ

(รศ.ดร.อิสระชัย งามหรู)
หัวหน้ากองบรรณาธิการ

กลไกควบคุมคุณภาพการให้บริการ โดยใช้ DiffServ-aware Traffic Engineering

Mechanism Control QoS Using DiffServ-aware Traffic Engineering.

วิรัช ชัยขุนพล กอบชัย เดชหาญ

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

บทคัดย่อ

บทความนี้ได้ทำการศึกษาและทดสอบประสิทธิภาพคุณภาพของบริการ (Quality of Service) ในด้านการรันตีคุณภาพของบริการตามข้อตกลงของระดับการให้บริการ (Service Level Agreement) โดยทำการทดสอบบริการแบบ Video ที่จำลอง Traffic Video ขณะที่เกิดความคับคั่งบนโครงข่าย MPLS บทความนี้นำเสนอกลไกควบคุม QoS ในด้าน ค่า Packet loss, ค่าหน่วงเวลา (Latency) และค่าหน่วงเวลาแปรผัน (Jitter) โดยใช้ DiffServ-aware Traffic Engineering (DS-TE)

คำสำคัญ: MPLS, QoS, SLA, DiffServ-aware Traffic Engineering

Abstract

This paper concerns about the studying and testing performance of QoS with guarantee service according to SLA, also and test of video service by using video traffic simulation within MPLS network when congested. This paper propose QoS control mechanism in term of packet loss, latency and Jitter by using DiffServ-aware Traffic Engineering.

Key words: MPLS , QoS, SLA, DiffServ-aware Traffic Engineering

1. บทนำ

MPLS Network เป็น โครงข่าย ที่รองรับ ความหลากหลายของบริการ ในการถ่ายโอนข้อมูลบน โครงข่ายเดียวกัน ซึ่งโครงข่ายดังกล่าว ควรต้องมีการจัดการความแตกต่างของ Quality of Service (QoS) เพื่อรองรับบริการที่แตกต่าง ตาม ข้อตกลง ระดับ บริการ (Service Level Agreement) ในด้านการควบ คุมค่า Packet loss ค่าหน่วงเวลา (Latency) ค่าแปรผันหน่วงเวลา (Jitter) วัตถุประสงค์หลักของ QoS คือการจัดการข้อมูลที่รับประกัน [1,2,4] คุณภาพ ที่มีประเภทที่แตกต่างและความต้องการลำดับความสำคัญของข้อมูลแต่ละประเภท เช่น เสียง (Voice) ที่มีการควบคุมและรับประกันค่า Packet loss, Latency และ Jitter เช่นเดียวกับข้อมูลประเภทภาพ (Video) ส่วนข้อมูลทั่วๆไป อาจไม่ต้องเน้นการรับประกันข้อมูล ในขณะที่เกิดความ คับคั่ง ในโครงข่าย สิ่งสำคัญที่กลไก Qos คือ ไม่สามารถ เพิ่มความจุ แต่รับรองการไหลของข้อมูล และจัดสรรความจุภายในได้ หรือการลดอัตราคับคั่งให้ลดลง

ทำผู้ให้บริการ (Service Provider) มีการเพิ่มความสามารถในโครงข่ายให้รองรับกับหลายๆ บริการ (diff-serv)

การรับประกันคุณภาพของข้อมูล (Assured Forwarding) แต่ละประเภทจะอาศัยการผสมผสานระหว่าง MPLS DiffServ กับ MPLS Traffic engineering (MPLS-TE) คือการรวมเอาข้อดีของสองเทคโนโลยี เป็น กลไก QoS เพื่อให้สามารถการันตีบริการแบบ end-to-end และสามารถกำหนด SLA บนโครงข่าย MPLS ได้ เรียกวิธีการนี้ว่า DiffServ-aware Traffic Engineering (DS-TE) จะทำหน้าที่เป็นตัวสร้างท่อเสมือน (Tunnel) ที่มีการแบ่งชั้น (Class) ของแต่ละบริการให้วิ่งผ่านแต่ละ Tunnel และยังมีการจัดลำดับความสำคัญของแต่ละ Tunnel ตามลำดับความสำคัญของบริการ ทำให้สามารถรับประกันคุณภาพของบริการ ในขณะมีการคับคั่งในโครงข่ายเกิดขึ้น [1-7]

2. ทฤษฎีที่ใช้ในการทดสอบ

2.1. QoS

Quality of Service (QoS) เป็นการจัดลำดับความสำคัญของข้อมูล Application โดยการทำงานของเทคโนโลยี Quality of Service (QoS) จะเป็นการจัดแบ่งประเภทของข้อมูล Application ออกเป็นหมวดหมู่ และมีการจัดลำดับความสำคัญของข้อมูลในแต่ละหมวดหมู่นั้นๆ ซึ่งทำให้สามารถควบคุม Bandwidth ในระบบเครือข่ายของให้ใช้ประโยชน์ได้สูงสุดตาม วัตถุประสงค์พื้นฐานของกลไก Qos คือ การการันตีแพ็คเก็ตที่จะไม่เกิดการคับคั่งมากเกินไปแน่นอน การแบ่งแยกระบบ QoS ที่ใช้งานจึงแบ่งแยกออกเป็น Best-Effort (BE), IntServ: Integrated Service และ DiffServ : Differentiated Service

Best-Effort (BE) จะเป็นการไม่ใช้งาน QoS ในโครงข่าย เมื่อโครงข่ายเกิดความคับคั่ง บริการต่างๆ ที่ส่งผ่านในโครงข่าย อาจจะมีการเสียหายหรือคุณภาพแย่ได้

Integrate Service เป็นขบวนการทำงานที่ได้รับการนำมาประยุกต์ใช้ตั้งแต่เริ่มต้น โดยการแบ่งการเชื่อมโยงหรือการไหลเป็นลำดับชั้น และแบ่งแยกตามลาดับการให้บริการในระบบนี้ จะใช้ โปรโตคอล ReSource reserVation Protocol (RSVP) ในการควบคุม QoS

Difference Service คือ การแบ่งแยกรูปแบบของข้อมูลออกจากกันให้บริการ โดยการเพิ่มแท็ก (tag) ในแต่ละแพ็กเก็ตเพื่อแบ่งแยกระดับการให้บริการ [4,5,6]

2.2 MPLS Support DiffServ

MPLS Support DiffServ โครงข่าย MPLS ที่ต้องรองรับความต้องการของ คุณภาพการให้บริการ หลายๆ รูปแบบ โดยโครงข่ายควรจะพิจารณาเฉพาะค่า Per-Hop Behavior (PHB) ซึ่งจะเป็นกำหนดความต้องการของคุณภาพการให้บริการได้ [6]

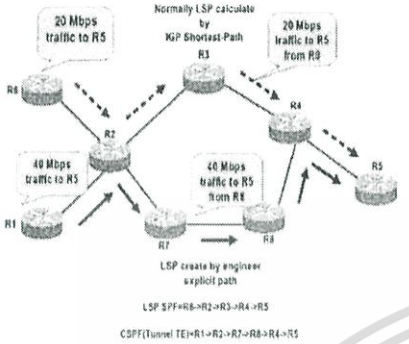
MPLS ที่รองรับบริการที่แตกต่างกัน จะใช้ Label Switch Path (LSP) ที่พิจารณา คุณลักษณะและการทำงานอยู่ 2 แบบคือ แบบที่ 1 EXP-inferred-class LSP (E-LSP) จะลำเลียงข้อมูลหลายๆชั้นได้ ส่วนแบบที่ 2 Label-inferred-class LSP (L-LSP) จะลำเลียงข้อมูลได้ชั้นเดียว [5]

2.3 MPLS Traffic Engineering (TE)

Traffic Engineering เป็นการควบคุมการไหลของข้อมูลผ่านโครงข่าย MPLS ตามอัตราส่วนที่เหมาะสมของทรัพยากรโครงข่าย โดยการสร้างเส้นทาง Label Switch Path (LSP) ของ MPLS TE จะกำหนดเส้นทางเอง ปกติการสร้างเส้นทางของ Packet IP จะสร้างตาม Routing Protocol แบบ Interior Gateway Protocol (IGP) ซึ่งจะคำนวณเส้นทางที่ดีที่สุดตาม Shortest Path First (SPF) ตาม routing table ของ edge router ส่วน MPLS TE จะคำนึงข้อจำกัด เช่น BW และการจำกัดข้อมูลให้เหมาะสม เมื่อคำนวณเส้นทางได้แล้วจะทำการเปลี่ยน SPF และใช้เส้นทางใหม่ Constrained SPF (CSPF) ซึ่งวิธีการสร้าง CSPF จะใช้โปรโตคอลที่ใช้คำนวณเส้นทางใหม่โดยใช้ RSVP เป็นโปรโตรคอลส่ง Label ตั้งแต่การไหลตาม LSP และจอง BW ตลอดทั้งเส้นทาง ดังแสดงในรูปที่ 2 [3]

กลไกการทำงานของ QoS ภายในโครงข่าย MPLS ที่อุปกรณ์ Provider Edge (PE) จะทำการ คัดแยกประเภทข้อมูล (Classification), กำหนดประเภท (Marking), การจัดการความคับคั่ง (Congestion Management), แก้ไขความคับคั่ง (Congestion Avoidance) และควบคุมการไหลของข้อมูล (Policing and Shaping) ดังแสดงในรูปที่ 4 โดยการคัดแยกประเภทข้อมูลและกำหนดประเภทข้อมูล

(Classification and Marking) ที่อุปกรณ์ PE จะคัดแยกตามค่า DiffServ Code Point (DSCP) หรือค่า IP Precedence ซึ่งค่าดังกล่าวจะถูกกำหนดจากอุปกรณ์ลูกค้า Customer Edge (CE) ที่แยกประเภทแต่ละ Application [2,4]



รูปที่ 2 การสร้าง TE Tunnel ของ Traffic Engineering

2.4. DIFFSERV-AWARE TRAFFIC ENGINEERING

DiffServ-aware Traffic Engineering (DS-TE) คือ การควบคุมและการันตี traffic เพื่อสามารถจัดสรรแบนวิดสำหรับ traffic ที่ต่างชนิดกัน ในการจำกัด BW ของแต่ละ traffic จะเรียกว่า sub-pool และมี global pool เป็น BW รวมของ TE tunnel โดย sub-pool จะเป็นการจัดลำดับความสำคัญของ traffic แต่ละประเภทให้มีการส่งข้อมูลบนคลาสที่เหมาะสม

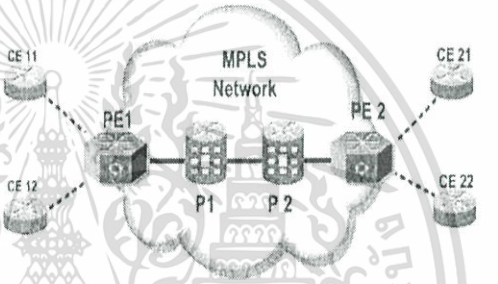
การแบ่งคลาส Class Type (CT) คือ การ จัดลำดับความสำคัญของ traffic ของ sub-pool ที่ส่งผ่านในท่อเสมือน (Tunnel) เพื่อจัดสรรแบนวิดภายใน tunnel ที่จำกัดบนเส้นทางที่กำหนด ส่วนหนึ่งของ CT ที่จำกัด BW ในการแบ่งของ CT จะมีการแบ่งตั้งแต่ CT0 ถึง CT7 ลักษณะที่สำคัญที่สุดของการคำนวณแบนวิดที่เหมาะสม การแบ่งของแบนวิดระหว่าง CT เรียกว่า Bandwidth Constraint (BC) มี 2 BC อยู่ 2 แบบ คือ

- Maximum Allocation Model (MAM) แต่ละคลาสทำหน้าที่เฉพาะปริมาณของแบนวิดและคลาสอื่นไม่สามารถได้ประโยชน์จากการไม่ใช้แบนวิด

- Russian Dolls Model (RDM) แต่ละคลาสรับปริมาณของแบนวิดแต่สิทธิต่ำกว่าคลาสสามารถใช้แบนวิดของสิทธิที่สูงกว่าคลาส เมื่อ แบนวิดเหมาะสม [5,6]

3. การทดสอบการทำงาน

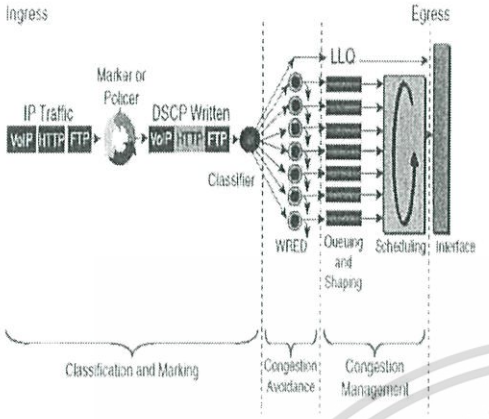
บทความนี้ จะทดสอบประสิทธิภาพของการทำงาน บนโครงข่าย MPLS ที่ใช้กลไกควบคุมคุณภาพของบริการ (QoS) ที่มีวิธีการทำงาน ของกลไกควบคุม QoS ที่แตกต่างกัน ทำการทดสอบการให้บริการข้อมูลประเภท video ซึ่งทดสอบประสิทธิภาพการทำงานของ QoS ขณะโครงข่าย MPLS เกิดความคับคั่ง โดยใช้ IP Traffic Generator ทำให้เกิดความคับคั่ง



รูปที่ 3 แบบจำลองโครงข่าย MPLS ที่ใช้ทดสอบ

จากรูปที่ 3 แสดงแบบจำลองโครงข่าย MPLS ที่ใช้ในการทดสอบ ประกอบไปด้วย P Router (P1, P2) และ Provider Edge Router (PE1, PE2) เชื่อมต่อด้วยความเร็ว 1 Gigabit Ethernet Interface อุปกรณ์ router ทั้งหมด ถูก configure เป็น MPLS เพื่อจัดสร้างเป็นโครงข่าย MPLS และมีการสร้างกลไกควบคุม QoS แบบ Per-Hop Behavior (PHB), Traffic Engineering (TE) และ DiffServ-aware Traffic Engineering (DS-TE) ในการทดสอบบริการ video ได้มีการกำหนดค่า Service Level Agreement (SLA) ของบริการ video แบ่งออกเป็น 3 ช่อง คือ Gold, Silver และ Bronze การออกแบบการทำงานของ กลไกควบคุม QoS แบบ PHB และแบบ DS-TE จะคำนึงถึงคุณภาพของบริการประเภท Video คือ ค่า Packet loss ไม่เกิน 5 % ค่าหน่วงเวลา (Latency) ไม่เกิน 150 ms ค่าแปรผันหน่วงเวลา (Jitter) ไม่เกิน 30 ms ในส่วน Video Stream สามารถ Burst

Bandwidth 20 % โดยการทำงานของกลไกควบคุม QoS ทั้งสองรูปแบบจะมีการทำงานดังรูปที่ 4



รูปที่ 4 ลำดับการทำงานกลไกควบคุม QoS ทั้งสองรูปแบบ

การกำหนดนโยบาย (Policy) ของ PHB จะแบ่งประเภทข้อมูล โดยใช้ค่า Diff-Serv Code Point (DSCP) ที่กำหนดมาจากอุปกรณ์ลูกค้า Customer Edge (CE) มาเข้าเงื่อนไขของ PHB ซึ่งใช้แบบ การส่งที่มีการการันตี (Assured Forwarding PHB) ในการการันตี bandwidth จะใช้บิท 5-7 ของค่า DSCP จัดลำดับความสำคัญของช่อง Video คือ 001 (มาก), 010 (ปานกลาง), 011 (น้อย) โดยจะกำหนดค่า DSCP ของแต่ละช่องเป็น Gold (AF31), Silver (AF32) และ Bronze (AF33) โดยแบ่งตามการกำหนดค่า SLA ตามตารางที่ 1

การสร้าง Tunnel ใน DS-TE จะมีการกำหนดค่า sub-pool เป็น 150 Mbps และค่า global pool เป็น 400 Mbps ที่ Interface Output ของอุปกรณ์ PE1, P1, P2 และ PE2 ในการแบ่ง CT จะใช้วิธีแบ่งแบบ MAM และมีการสร้าง tunnel สำหรับ traffic ของแต่ละช่อง Video คือ ช่อง Gold (Tun10), ช่อง Silver (Tun20) และช่อง Bronze (Tun30) ซึ่งถูกจัดลำดับความสำคัญของแต่ละช่อง Video จากค่า Experimental (exp) ดังแสดงในตารางที่ 2 ในการจำลองอุปกรณ์ CE11 ที่ใช้จำลอง Traffic ประเภท Video จะใช้ IP Traffic Generator ส่ง Traffic 100 Mbps ของอุปกรณ์ CE11 โดยจะจำลองเป็นช่อง Video 3 ช่อง

Chanel Video	Guarantees	BW
Gold	Bandwidth, packet loss น้อย, Delay ต่ำ,Jitter ต่ำ	50M
Silver	Bandwidth, packet loss ปานกลาง Delay ปานกลาง, Jitter ปานกลาง	35M
Bronze	ไม่รับประกัน	15M

ตารางที่ 1 กำหนดค่า SLA ของแต่ละช่อง Video ของ CE11

ในการทดสอบการทำงานของ กลไกควบคุม QoS แบบ PHB และแบบ DS-TE จะใช้เส้นทางในการส่งข้อมูลเส้นทางเดียวกันคือ PE1->P1->P2->PE2 ส่วนการทดสอบประสิทธิภาพของการควบคุมคุณภาพของบริการ แบบ PHB และแบบ DS-TE ทำการทดสอบ ที่ช่อง Gold ของบริการประเภท Video เพื่อแสดงประสิทธิภาพความสามารถในการการันตีบริการตาม SLA ในเรื่องค่า Packet loss ค่า Latency และค่า Jitter โดยมีการกำหนดนโยบาย ของช่อง Gold ในการ Classify และ Marking ทั้งสองแบบ จะใช้วิธีการเดียวกัน ส่วน Congestion Avoidance จะใช้ Weighted Random Early Detection (WRED) ในการจำกัด BW แต่ละบริการตามการคัดเลือกข้อมูล ของช่องขาเข้าของอุปกรณ์ PE1 คือInterface Gi3/0/4 มีรายละเอียดการกำหนด Policy ตาม ตารางที่ 2

Mechanism	Policy Conditions
PHB	Class video-gold police cir 50000000 bc 1562500 conform-action transmit exceed-action drop
DS-TE	Class sla-1-class police cir 50000000 bc 1562500 conform-action set-mpls-exp-transmit 5 exceed-action drop

ตารางที่ 2 การกำหนด Policy ขาเข้าของช่อง Gold

การกำหนดนโยบายของ Congestion Management PHB จะใช้แบบ Class-Based Weight Fair Queuing (CBWFQ) ส่วน DS-TE จะใช้แบบ Priority Queuing (PQ) นำมาใช้กับขาออกของอุปกรณ์ PE1 ที่ Interface Gi3/0/0

3.1 ทดสอบประสิทธิภาพ ความน่าเชื่อถือของบริการ (Reliability of Service)

การทดสอบประสิทธิภาพด้านคุณภาพการบริการ (Quality of Service) เป็นการทดสอบความสามารถในการให้บริการข้อมูลประเภท Video บนโครงข่าย MPLS โดยจัดลำดับความสำคัญของ ช่อง Gold ให้สามารถใช้งานได้โดยไม่มีผลกระทบต่อคุณภาพ ตามข้อกำหนด SLA ในตารางที่ 1 ขณะโครงข่าย MPLS เกิดความคับคั่ง

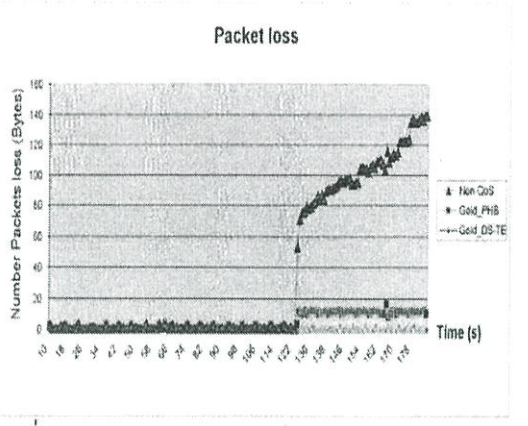
ในการจำลองให้โครงข่าย MPLS ตามรูปที่ 3 เกิดความคับคั่ง จะใช้ IP Traffic Generator ส่ง traffic แบบ Best-Effort (BE) เข้ามาที่ Interface Gi1/0/4 ของ Router P1 โดยจะเพิ่ม BW ของ traffic ที่ส่งเข้า Interface Gi1/0/4 เป็น 3 ช่วง คือ ช่วงเวลา 0 – 50 s ส่ง traffic 200 Mbps, ช่วงเวลา 51 – 120 s ส่ง traffic 500 Mbps และช่วงเวลา 121 – 190 s ส่ง traffic 980 Mbps ซึ่งจะทำให้โครงข่าย MPLS เกิดความคับคั่ง

3.1.1 Packet Loss

ค่า Packet Loss ที่วัดหลังจาก QoS ทำงานของและใช้กลไก QoS แบบ PHB และแบบ DS-TE ผลที่ได้จากรูปที่ 6 และตารางที่ 3 แสดงให้เห็นผลการเปรียบเทียบจำนวน Packet loss ในช่วงเวลาที่ QoS ทำงาน จะมีการ Drop ของ Packet เกิดขึ้น

Mechanism	Tx Packet	Rx Packet	Packet loss	%Packet loss
PHB	50 Mbps	49.85 Mbps	0.15 Mbps	0.3 %
DS-TE	50 Mbps	49.98 Mbps	0.02 Mbps	0.04 %

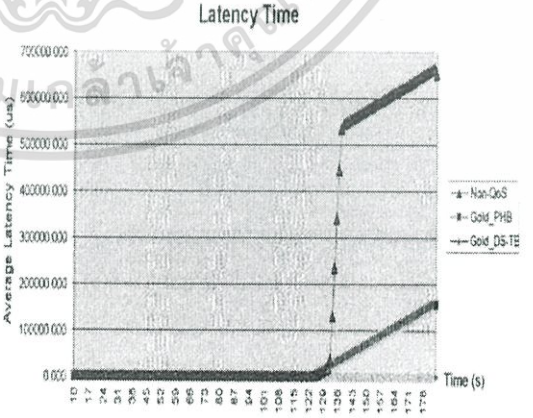
ตารางที่ 3 เปอร์เซ็นต์ Packet loss ของ Video ช่อง Gold



รูปที่ 6 ค่า Packet Loss ในขณะที่โครงข่ายเกิดเหตุการณ์การจราจรคับคั่ง

3.1.3 Latency

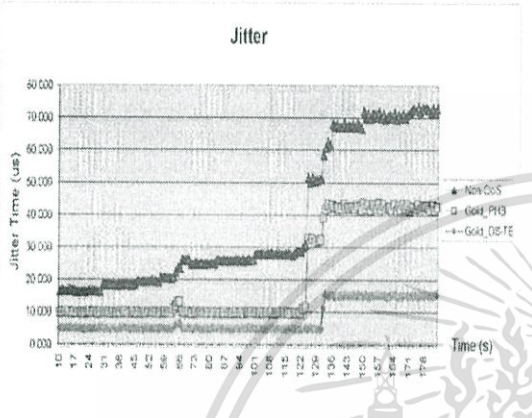
เมื่อพิจารณาค่า latency ของบริการ ของ Video ช่อง Gold ในการควบคุมคุณภาพของบริการ ค่า latency จะมีผลต่อคุณภาพของบริการแบบ Video ถ้าค่า Latency ของบริการ Video เพิ่มขึ้น การดูภาพที่ปลายทางมีความผิดเพี้ยน มีภาพกระตุก หรือค้างได้ โดยทั่วไปการควบคุมค่า Latency ของ Video การมีค่า 150 ms ซึ่งเป็นค่าเดียวกับของบริการแบบ Voice ซึ่งเป็นบริการแบบ Real Time เหมือนกัน จากรูปที่ 7 แสดงให้เห็นการการันตีค่า Latency ของช่อง Gold ขณะที่เกิดความคับคั่ง (Congestion) ในโครงข่าย MPLS



รูปที่ 7 ค่า latency time ของช่อง Gold เปรียบเทียบ กลไก QoS แบบ DS-TE และ PHB

3.1.4 Jitter

ค่าแปรผันหน่วงเวลา (Latency Variation) หรือ Jitter เป็นค่าที่สำคัญเหมือนกับค่า Latency สำหรับการให้บริการแบบ Real Time ซึ่งจะมีผลกับคุณภาพในการบริการ รูปที่ 8 แสดงให้เห็นว่า ขณะที่เกิดความคับคั่งของโครงข่าย MPLS ค่า Jitter มีค่าเพิ่มขึ้น



รูปที่ 8 แสดงประสิทธิภาพของ กลไกควบคุม QoS แบบ DS-TE ในการการันตี Application ต่างๆของ CE

4. สรุปผล

บทความนี้ เสนอการศึกษาและ ผลการทดสอบประสิทธิภาพในด้านคุณภาพของบริการ (Quality of Service) โดยจำลอง Traffic แบบ Video ของช่อง Gold ที่มีการ รับประกันคุณ ภาพตามข้อตกลงระดับบริการ (Service Level Agreement) แบบ end-to-end โดยใช้กลไกของ QoS แบบ Per-Hop Behavior (PHB) และแบบ DiffServ-aware Traffic Engineering (DS-TE) ควบคุม QoS ผลที่ได้จากการทดสอบแสดงให้เห็นว่า การ นำกลไก QoS แบบ DS-TE ใช้บนโครงข่าย MPLS เพื่อควบคุม QoS ของช่อง Gold ค่า Packet loss ที่ได้เป็น 0.04% ค่าหน่วงเวลา (Latency) เป็น 685 µs และค่าหน่วงเวลาแปรผัน (Latency Variation) 15 µs ในขณะโครงข่ายเกิดความคับคั่ง กลไก QoS แบบ PHB จะมีค่าจำนวณ Packet loss เพิ่มขึ้น ค่าหน่วงเวลาเพิ่มขึ้น และ ค่า Jitter เพิ่มขึ้น ทำให้ไม่สามารถควบคุมคุณภาพของบริการตามข้อตกลงระดับบริการได้

5. เอกสารอ้างอิง

[1] T. Szigeti and C. Hattingh, "End-to-End QoS Network Design," Indianapolis, Indiana : Cisco Press, 2005.

[2] S. Alvarez, "QoS for IP/MPLS Networks," Indianapolis, Indiana : Cisco Press, 2006.

[3] E. Osborne and A. J. Simha, "Traffic Engineering with MPLS," Indianapolis, Indiana : Cisco Press 2002.

[4] Student Guide "Implementing Cisco Quality of Service (QoS)," Indianapolis, Indiana : Cisco Press 2004.

[5] D.L. Zhang and D. Inescu, "QoS Performance Analysis in Deployment of DiffServ-aware MPLS Traffic Engineering," IEE Software Engineering Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007 Eight ACIS International Conference, July 30 2007-Aug. 1 2007

[6] F. L. Faucheur and W. Lai, "Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering," RFC 3564, July 2003.

[7] J. Heinanen, F. Baker, W. Weiss, and J Wroclawski, "Assured Forwarding PHB Group," RFC 2597 (Proposed Standard), June 1999, updated by RFC 3260.

ประวัติผู้เขียน

นายวิรัช ชัยขุนพล เกิดเมื่อวันที่ 30 มีนาคม พ.ศ.2521 ที่จังหวัดลำปาง สำเร็จการศึกษาปริญญาตรีวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร จากภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีราชมงคล ในปีการศึกษา 2545 และเข้าศึกษาต่อในระดับปริญญาโท หลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมโทรคมนาคม ภาควิชาวิศวกรรมโทรคมนาคม คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ในปีการศึกษา 2550 โดยในปี พ.ศ. 2546 ได้เข้าทำงานในตำแหน่งวิศวกร ส่วนเทคนิคบรอดแบนด์ ฝ่ายวิศวกรมสื่อสารข้อมูล บริษัท กสท โทรคมนาคม จำกัด (มหาชน)