การนำโทรศัพท์ ประยุกต์ร่วม ระบบเครือข่ายข้อมูลส่วนตัว

AN INTEGRATED TELEPHONE SYSTEM WITH PRIVATE DATA NETWORK

กมล กลัดคร้าม

KAMOL KLUDKRAM

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า
บัณฑิตวิทยาลัย
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2546

ISBN 974-324-188-4

การนำโทรศัพท์ ประยุกต์ร่วม ระบบเครือข่ายข้อมูลส่วนตัว

AN INTEGRATED TELEPHONE SYSTEM WITH PRIVATE DATA NETWORK

กมล กลัดคร้าม

KAMOL KLUDKRAM

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมไฟฟ้า

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2546

ISBN 974-324-188-4

AN INTEGRATED TELEPHONE SYSTEM WITH PRIVATE DATA NETWORK

KAMOL KLUDKRAM

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ENGINEERING IN ELECTRICAL ENGINEERING

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2003

ISBN 974-324-188-4

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การนำโทรศัพท์ประยุกต์ร่วมระบบเครือข่ายข้อมูลส่วนตัว
AN INTEGRATED TELEPHONE SYSTEM WITH PRIVATE DATA NETWORK

ชื่อนักศึกษา นายกมล กลัดคร้าม

รหัสประจำตัว 42061192

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมไฟฟ้า

อาจารย์ผู้ควบคุมวิทยานิพนธ์ รศ.ดร.กอบชัย เดชหาญ

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
รศ.ดร.ถวิล	พึ่งมา	
รศ.สมยศ	จุณณะปิยะ	
ผศ.เกรียงไกร	วงศ์โรจนภรณ์	
รศ.ดร.กอบชัย	เดชหาญ	

วัน/เดือน/ปี ที่สอบ 16 ธันวาคม 2545 เวลา 12.00-13.00 น.

สถานที่สอบ ณ อาคาร 12 ชั้น ชั้น 4 (ห้อง E12-404)

บัณฑิตวิทยาลัยรับรองแล้ว

(รศ.ดร.บุญวัฒน์ อัตชู)

คณบดีบัณฑิตวิทยาลัย

วันที่.....๒๐.....**เดือน**.....มกราคม.....**พ.ศ.**.....๒๕๔๖.....

หัวข้อวิทยานิพนธ์	การนำโทรศัพท์ ประยุกต์ร่วม ระบบเครือข่ายข้อมูลส่วนตัว
นักศึกษา	นายกมล กลัดคร้าม
รหัสประจำตัว	42061192
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมไฟฟ้า
พ.ศ.	2546
อาจารย์ผู้ควบคุมวิทยานิพนธ์	รศ. ดร. กอบชัย เดชหาญ

บทคัดย่อ

วิทยานิพนธ์นี้เสนอการนำเทคโนโลยีของเสียง มาประยุกต์ส่งผ่านร่วมกับข้อมูลในรูปแบบของโพรโตคอลชนิดต่างๆ ของระบบคอมพิวเตอร์บนเครือข่ายชนิดอินเตอร์เน็ทโพรโตคอล ซึ่งเป็นเทคโนโลยีในการเชื่อมต่อที่มีประสิทธิภาพ ในวิทยานิพนธ์นี้แสดงวิธีการในการประยุกต์ใช้ระบบโทรศัพท์ร่วมกับ ระบบเครือข่ายข้อมูลส่วนตัว โดยใช้โพรโตคอลอินเตอร์เน็ทโพรโตคอล (Internet Protocol) และเทคนิคในการบีบอัดสัญญาณเสียง ตลอดจนรายละเอียดของเทคนิคและวิธีการในการนำเอาสัญญาณเสียง ไปบนเครือข่ายอินเตอร์เน็ทโพรโตคอล สามารถส่งผ่านบนเครือข่ายข้อมูลส่วนตัวสามารถทำได้อย่างมีประสิทธิภาพ

Thesis Title	An Integrated Telephone System with Private Data Network
Student	Mr. Kamol Kludkram
Student ID.	42061192
Degree	Master of Engineering
Programme	Electrical Engineering
Year	2003
Thesis Advisor	Assoc. Prof. Dr. Kobchai Dejhan

ABSTRACT

This thesis presents to use voice technologies for applying to send with the data in the form of various protocols of computer over internet protocol. This thesis proposes a methodology of integrated telephone system with private data network. The applied voice over internet protocol by using RTP header compression in the IP network is an efficient network system for transferring the high bit rate.

กิตติกรรมประกาศ

การจัดทำวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้อย่างดี เพราะได้รับความเมตตากรุณาจาก รองศาสตราจารย์ ดร.กอบชัย เดชหาญ ที่ให้ความช่วยเหลือแนะนำจนวิทยานิพนธ์นี้สำเร็จได้ ผู้เขียนวิทยานิพนธ์รู้สึกซาบซึ้งในความอนุเคราะห์จากท่าน และขอกราบขอบพระคุณเป็นอย่างสูง

ขอกราบขอบพระคุณ คุณแม่เสมอ สุพรรณดี ที่คอยห่วงใย และให้กำลังใจให้เกิดมานะในการศึกษา

ขอขอบคุณคุณชาลิน สุวรรณวงศ์ ที่สนับสนุนในการศึกษา และให้คำแนะนำในการทำวิทยานิพนธ์

ขอขอบคุณ นาวาอากาศตรีหญิง อรประภา กลัดคร้าม ที่คอยดูแล ห่วงใย และให้กำลังใจในการทำวิทยานิพนธ์ครั้งนี้

ขอขอบคุณเพื่อนๆ น้องๆ ที่ทำงานที่คอยช่วยเหลือ ให้คำแนะนำในการทำวิทยานิพนธ์

สุดท้ายขอขอบคุณบัณฑิตวิทยาลัย ที่ได้ให้ทุนสนับสนุนการทำวิทยานิพนธ์ครั้งนี้

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์ฉบับนี้ ผู้วิจัยขอมอบแด่ผู้มีพระคุณทุกท่าน

กมล กลัดคร้าม

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญภาพ

สารบัญภาพ (ต่อ)

สารบัญภาพ (ต่อ)

บทที่ 1
บทนำ

1.1 กล่าวนำ

เนื่องจากในปัจจุบันการใช้บริการระบบโทรศัพท์ในองค์กรต่างๆ ทั้งในภาคธุรกิจเอกชนและรัฐบาลต่างต้องอาศัยการบริการจากผู้ให้บริการต่างๆ ซึ่งมีค่าใช้จ่ายสูง และมีปัญหาด้านคุณภาพของการให้บริการ แต่เนื่องจากองค์กรต่าง ๆ ทั้งในภาครัฐ และภาคเอกชนดังกล่าว ได้มีการนำเอาเครือข่ายชนิดอินเตอร์เน็ต โพรโตคอล มาประยุกต์ใช้งาน เพื่อการส่งผ่านข้อมูลในระยะไกล (Wide Area Network : WAN) กันอย่างแพร่หลายมากขึ้น และการส่งผ่านข้อมูลระหว่างวง LAN ข้ามเครือข่าย WAN ได้อย่างมีประสิทธิภาพ ด้วยความสามารถดังกล่าวและการพัฒนาที่ต่อเนื่องทางเทคโนโลยีของเครือข่าย โดยเฉพาะอย่างยิ่ง การนำพาข้อมูลชนิดต่างๆ เช่น ข้อมูลคอมพิวเตอร์และข้อมูลเสียงส่งผ่านไปบนเครือข่าย IP ที่มีอยู่ โดยเรียกเทคโนโลยีนี้ว่า Voice over Internet Protocol (VoIP)

1.2 วัตถุประสงค์ของวิทยานิพนธ์

ในการนำเอาข้อมูลชนิดต่าง ๆ เช่น สัญญาณเสียง และข้อมูล ส่งรวมกันไปบนเครือข่ายชนิดอินเตอร์เน็ต โพรโตคอลได้นั้น จะเป็นการใช้ช่องทางสื่อสารข้อมูลอย่างคุ้มค่า และมีประสิทธิภาพ อีกทั้งยังเป็นการประหยัดค่าใช้จ่ายอย่างมากในการดำเนินธุรกิจด้วย เนื่องจากเป็นการเพิ่มการส่งผ่านปริมาณข้อมูลชนิดต่าง ๆ ดังกล่าวไปบนเครือข่ายอินเตอร์เน็ต โพรโตคอลที่มีอยู่เดิมโดยไม่ต้องเพิ่มค่าเช่าใช้ช่องทาง หรือวงจรสำหรับสื่อสารข้อมูล

1.3 หลักการใหม่ในวิทยานิพนธ์

นำเอาเทคโนโลยี โพรโตคอล อินเตอร์เน็ทโพรโตคอล มาใช้ในเครือข่ายข้อมูลส่วนตัว โดยการใช้ประโยชน์ของเทคโนโลยีเครือข่ายอินเตอร์เน็ทโพรโตคอล และใช้วิธีการบีบอัดซึ่งเป็นส่วนสำคัญในการส่งผ่านข้อมูลเสียงในรูปแบบของอินเตอร์เน็ทโพรโตคอล ซึ่งช่วยให้สามารถสื่อสารได้ทั้งข้อมูล และเสียง ไปบนช่องทาง หรือวงจรที่ยังคงมีแบนด์วิดท์ เดียวกัน

1.4 เปรียบเทียบกับหลักการเดิม

ในระบบการสื่อสารแบบเดิมนั้นจะเป็นการสื่อสารสำหรับข้อมูลที่เป็น Data ในระบบคอมพิวเตอร์ เช่นข้อมูลในระบบ LAN จะใช้โพรโตคอล IP, IPX, TCP/IP เป็นต้น และ Legacy Protocol เช่น SNA/SDLC, X.25, BSC, Async เป็นต้น ผ่านไปบนเครือข่ายส่วนตัว (Private Data Network) หรือเครือข่ายการสื่อสารแบบเช่าจุดต่อจุด (Point-to-Point) กับเทคโนโลยีของ TDM

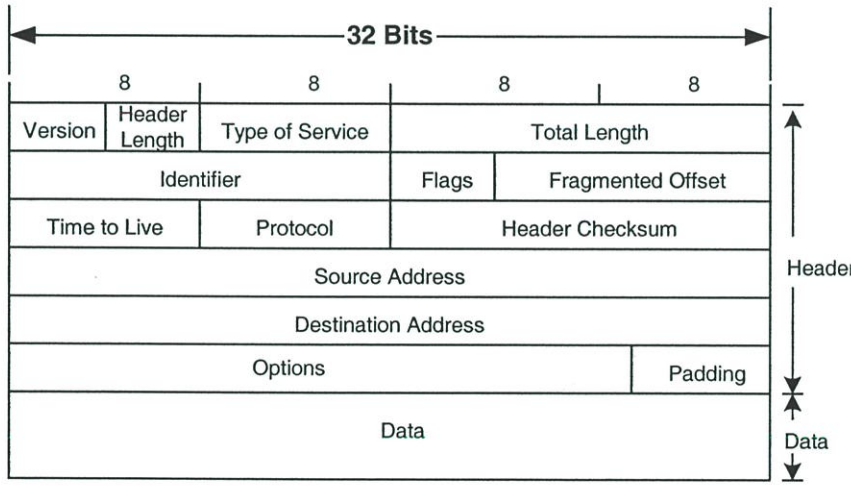
(Time Division Multiplexers) โดยไม่ได้นำรูปแบบของข้อมูลในลักษณะของสัญญาณเสียง ส่งผ่านรวมกันไปกับข้อมูลที่เป็น Data ของระบบคอมพิวเตอร์ บนเครือข่ายชนิดอินเตอร์เน็ทโพรโตคอล ซึ่งถือว่ายังใช้ประโยชน์ของเทคโนโลยีได้ไม่เต็มความสามารถ ซึ่งเทคโนโลยี Voice over Internet Protocol (VoIP) จะช่วยให้มีการบริการทั้งสัญญาณเสียง และแฟกซ์บนเครือข่ายอินเตอร์เน็ทโพรโตคอล โดยจะส่งผลและมีบทบาทสำคัญให้ผู้ใช้งานใช้แบนด์วิดท์ได้อย่างคุ้มค่า และสามารถส่งสัญญาณเสียง และแฟกซ์ระหว่างสำนักงานต่าง ๆ ได้อย่างมีประสิทธิภาพ

บทที่ 2
เครือข่าย TCP/IP

โพรโทคอล TCP/IP เป็นโพรโทคอลที่ทำงานอยู่ในชั้น network ซึ่งมีการเชื่อมต่อแบบ Connection oriented โดยมีอุปกรณ์การสื่อสารซึ่งเรียกว่า เราท์เตอร์ (router) ซึ่งทำหน้าที่ในการส่งผ่านข้อมูลของผู้ใช้ในรูปของ IP datagram กระบวนการในการตัดสินใจเลือกเส้นทางในการส่ง IP datagram ในแต่ละตัวจึงเป็นประเด็นหลักที่ต้องได้รับการพิจารณาและการออกแบบอย่างมีประสิทธิภาพ เพื่อให้การรับส่ง IP datagram มีความรวดเร็วและมีความผิดพลาดน้อยที่สุด

2.1 โครงสร้างของ IP datagram

ในภาพที่ 2.1 แสดงถึงรูปแบบโครงสร้างของ IP datagram [3] ซึ่งจะเห็นได้ว่า IP datagram มีองค์ประกอบหลักอยู่ 2 ส่วน คือ ส่วนของ Header และส่วนของข้อมูล (data)



ภาพที่ 2.1 โครงสร้าง IP datagram

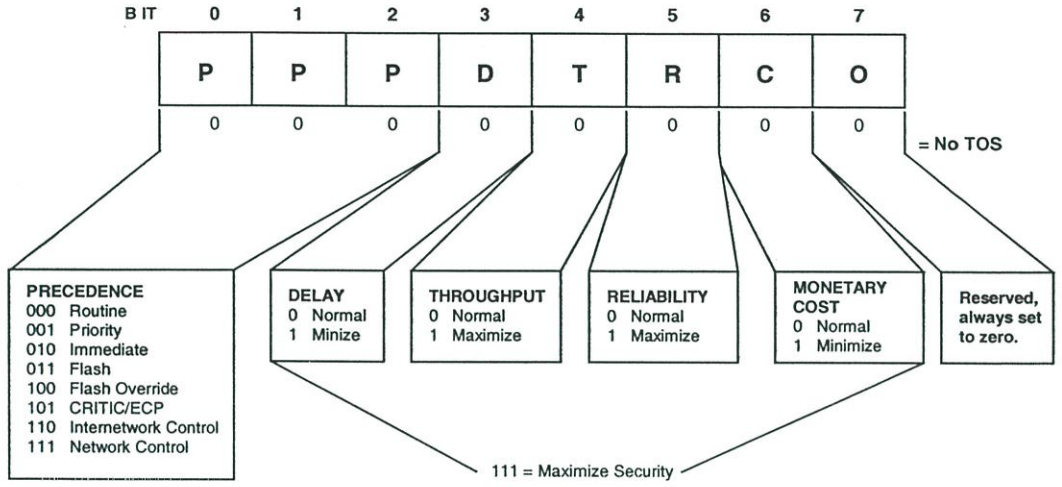
- ฟิลด์ Version : ระบุเวอร์ชันของ IP ที่ใช้ในการสร้าง IP datagram ในฟิลด์นี้จะมีขนาด 4 บิทซึ่งปกติจะเซ็ทเป็น 0100 ในระบบของเลขฐานสอง ซึ่งแสดงถึงเวอร์ชัน 4 (IPv4) ซึ่งเป็นเวอร์ชันที่ใช้อยู่ในปัจจุบัน ในตารางที่ 2.1 แสดงให้เห็นถึงเวอร์ชันในแบบต่าง ๆ ที่สัมพันธ์กันกับ RFC

ตารางที่ 2.1 แสดงหมายเลขเวอร์ชันของ IP

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

- ฟิลด์ Header Length : มีขนาด 4 บิทใช้บอกขนาด Header ของ IP โดยจะบอกในรูปของ word ขนาด 32 บิท ซึ่งปกติจะมีขนาดเท่ากับ 5 หรือเทียบเท่ากับ 20 ไบต์ และถ้าหากมีฟิลด์ Option เพิ่มเข้ามาจะทำให้ขนาดของ Header เท่ากับ 24 ไบต์
- ฟิลด์ Type of Service (TOS) : มีขนาด 8 บิท ใช้สำหรับบ่งบอกถึงคุณลักษณะหรือรูปแบบการให้การบริการที่แพ็กเก็ต IP ต้องการ ในฟิลด์นี้สามารถแบ่งออกได้เป็น 2 ส่วน คือ ส่วนของ Precedence และส่วนของ TOS ดังในภาพที่ 2.2 ส่วนของ Precedence นั้นมีจำนวน 3 บิทใช้สำหรับจัดลำดับความสำคัญของแพ็กเก็ตซึ่งมีได้ 8 ระดับ ในส่วนของ TOS มีไว้เพื่อใช้ในการเลือกการบริการในการส่งมอบแพ็กเก็ตในรูปของ Delay Throughput Reliability และ Monetary cost
- ฟิลด์ Total Length : มีขนาด 16 บิทใช้สำหรับระบุขนาดของ IP datagram ทั้งหมดซึ่งรวม Header ด้วย ขนาดของ IP datagram ที่ใหญ่ที่สุดมีค่าเท่ากับ 65,535 ไบท์
- ฟิลด์ Identifier : มีขนาด 16 บิทใช้ในการเชื่อมต่อฟิลด์ Flags และฟิลด์ Fragment Offset สำหรับการแบ่งแพ็กเก็ตออกเป็นแพ็กเก็ตย่อย ๆ ซึ่งแพ็กเก็ตจะถูกทำ fragment เพื่อทำให้เป็นแพ็กเก็ตย่อย ๆ ก็ต่อเมื่อความยาวของแพ็กเก็ตที่มาจากต้นทางมีความยาวมากเกินกว่าค่า Maximun Transmission Unit (MTU) ของ data link ในแต่ละเส้นทางที่แพ็กเก็ตนี้เดินทางผ่าน เช่น มีแพ็กเก็ตขนาด 5,000 ไบท์ที่จะต้องเดินทางผ่านเครือข่ายร่วมซึ่งมีค่า MTU เป็น 1,500 ไบท์ เพราะฉะนั้นภายในเฟรมหนึ่ง ๆ จะสามารถบรรจุขนาดของแพ็กเก็ตได้สูงสุด 1,500 ไบท์ ทำให้เราท์

เตอร์ซึ่งบรรจุแพ็กเก็ตไปบน data link ทำการ fragment แพ็กเก็ตแต่ละแพ็กเก็ตให้มีขนาดไม่เกิน 1,500 ไบท์ จากนั้นเราท์เตอร์จะทำการ mark แพ็กเก็ตซึ่งถูก fragment แล้วด้วยหมายเลขเดียวกันในฟิลด์ Identifier ซึ่งจะทำให้อุปกรณ์ทางด้านรับสามารถระบุได้ว่าแพ็กเก็ตที่ถูก fragment นั้นเป็นแพ็กเก็ตเดียวกัน



ภาพที่ 2.2 ฟิลด์ Type of Service

- ฟิลด์ Flags : เป็นฟิลด์ที่มีขนาด 3 บิทโดยที่บิทแรกไม่มีการใช้งานและกำหนดให้เป็น 0 เสมอ บิทที่สองเรียกว่าบิท Don't Fragment (DF) มีไว้เพื่อกำหนดว่า IP datagram นี้อนุญาตให้ทำ fragment ได้หรือไม่ ถ้าHost ต้นทางกำหนดให้ DF=0 ก็หมายถึงอนุญาตให้เราท์เตอร์ระหว่างทางทำการ fragment ได้ถ้ามีความจำเป็น แต่ถ้าหากเซ็ท DF=1 หมายความว่าห้ามทำการ fragment ในกรณีนี้ถ้าหากเราท์เตอร์ไม่สามารถส่ง datagram ต่อไปได้หากไม่มีการทำ fragment เราท์เตอร์ก็จะทิ้ง datagram นั้นไป และส่งความผิดพลาดที่เกิดขึ้นกลับไปยัง Host ต้นทาง บิทที่สามเรียกว่าบิท More Fragments (MF) เป็นบิทที่ถูกเซ็ทโดยเราท์เตอร์เมื่อมีการทำ fragment กับ IP datagrtam นั้นโดยจะมีค่า MF=0 เพื่อแสดงว่า fragment นั้นเป็นส่วนสุดท้ายของ IP datagram และจะเซ็ทให้ MF=1 เพื่อแสดงว่ายังมี fragment อื่นตามมาอีก เพราะฉะนั้นฟิลด์ flag จึงเป็นตัวระบุให้ Host ปลายทางทราบจุสิ้นสุดของ IP datagram มีข้อสังเกตว่า เมื่อ fragment ในแต่ละส่วนอาจจะถูกส่งผ่านเครือข่ายด้วยเส้นทางที่แตกต่างกัน และ fragmnet เหล่านี้อาจเดินทางมาถึงจุดหมายในลำดับที่ผิดไปจากเดิมได้ ดังนั้นหาก Host ปลายทางได้รับ fragment ที่บอกว่าเป็น fragment สุดท้าย แต่แท้จริงแล้ว Host ปลายทางได้รับ fragment ของ IP datagram ยังไม่ครบถ้วนสมบูรณ์ ซึ่งจะเห็นได้ว่า การใช้เพียงฟิลด์ Identifier และ Flag จะไม่เพียงพอสำหรับ Host ปลายทางที่จะนำ fragment มาประกอบกันได้อย่างถูกต้อง เพราะขาดข้อมูลที่บอกถึงลำดับการเรียงต่อของ fragment ปัญหานี้สามารถแก้ไขได้โดยอาศัยฟิลด์ Fragment Offset ที่จะได้กล่าวต่อไป

- ฟิลด์ Fragment Offset : ทำหน้าที่ชี้หรือระบุตำแหน่งเริ่มต้นของส่วนย่อยแต่ละส่วนภายใน IP datagram ฟิลด์นี้มีขนาด 13 บิท โดยค่าที่ใช้มีหน่วยเป็นจำนวนเท่าของ 8 ไบท์ เมื่อ Host ปลายทางอ่านค่าฟิลด์นี้ประกอบกับฟิลด์ Total length ของ fragment ที่ได้รับแต่ละตัว ก็จะทำให้สามารถตรวจสอบว่าได้รับ fragment ของ IP datagram ครบถ้วนหรือไม่
- ฟิลด์ Time to Live (TTL) : มีขนาด 8 บิทมีหน้าที่กำหนดจำนวนเราท์เตอร์สูงสุดที่ IP datagram สามารถเดินทางผ่านได้ หรือกล่าวในอีกนัยหนึ่งได้ว่าเป็นการกำหนดอายุของ datagram ที่อนุญาตให้อยู่ในเครือข่ายได้ ขั้นตอนในการทำงาน คือ เมื่อ Host ต้นทางทำการส่ง datagram ออกไปจะตั้งค่าเริ่มต้นให้กับฟิลด์ TTL ค่าหนึ่ง (โดยทั่วไปใช้ 32 หรือ 64) ทุกครั้งที่ datagram เดินทางผ่านเราท์เตอร์ตัวหนึ่งค่าของ TTL จะถูกปรับลดลงหนึ่งหน่วย หากเมื่อใดเราท์เตอร์พบ datagram ที่ค่า TTL ลดลงจนเป็น 0 เราท์เตอร์จะตัด datagram นั้นทิ้งไปพร้อมกับแจ้งให้ Host ต้นทางทราบ การทำเช่นนี้จะทำให้สามารถป้องกัน IP datagram ที่รับส่งผิดพลาดได้
- ฟิลด์ Protocol : เป็นฟิลด์ที่มีขนาด 8 บิท ใช้ระบุว่า datagram ที่ได้รับเป็นโพรโทคอลที่ใช้เชื่อม Host กับ Host หรือ Transport layer แบบใด ดังแสดงตัวอย่างของโพรโทคอลบางรูปแบบในตารางที่ 2.2

ตารางที่ 2.2 ค่าในฟิลด์ Protocol บางส่วนที่รู้จักกันดี

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

- ฟิลด์ Header Checksum : มีขนาด 16 บิทเป็นฟิลด์ที่ทำหน้าที่ตรวจสอบความถูกต้องของ IP header โดยมีลักษณะการทำงานดังนี้ เมื่อ Host ต้นทางทำการสร้าง datagram ขึ้นจะคำนวณค่า header checksum โดยนำ header ทีละ 16 บิทมาบวกกันแบบ one's component จากนั้นนำผลที่ได้มาทำ one's component อีกครั้ง จึงจะได้เป็นค่าที่บรรจุลงใน header checksum โดยที่ด้านรับปลายทางจะตรวจสอบความผิดพลาดของ header โดยนำ header ทีละ 16 บิทมาบวกกับค่าในฟิลด์ header checksum แบบ one's component หากผลลัพธ์ที่ได้มีค่าเป็นหนึ่งทั้งหมด แสดงว่าไม่มีความผิดพลาดเกิดขึ้น หากไม่ใช่ก็แสดงว่ามีความผิดพลาดเกิดขึ้นกับ header ในกรณีนี้ IP datagram จะถูกตัดทิ้งโดยไม่มีการแจ้งความผิดพลาดที่เกิดขึ้น ซึ่งโพรโทคอลในชั้นที่สูงกว่าต้องตรวจสอบปัญหาด้วยตัวเอง
- ฟิลด์ Source และ Destination Addresses : คือ IP address ของต้นทางและ IP address ของปลายทาง มีขนาด 32 บิท
- ฟิลด์ Option : เป็นส่วนที่เพิ่มเติมเมื่อมีการใช้งานบางอย่าง เช่น การทดสอบเครือข่าย และตรวจหาจุดผิดพลาดของระบบ ฟิลด์นี้จะมีขนาดไม่ตายตัวขึ้นอยู่กับชนิดของ option ที่เลือกใช้ เช่น Loose source routing Strict source routing Record route และ Timestamp เป็นต้น
- ฟิลด์ Padding : เป็นส่วนต่อท้ายฟิลด์ Option เพื่อทำให้มีขนาดครบ 32 บิท โดยทำการเติมศูนย์ต่อท้ายให้จนครบจำนวน 32 บิท

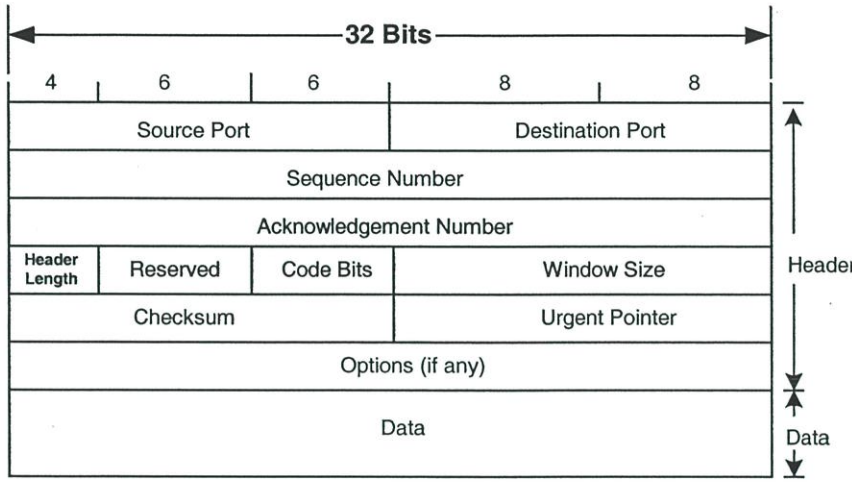
2.2 การทำงานพื้นฐานของโพรโทคอล TCP

ในขั้นตอนแรกข้อมูลของโปรแกรมแอพพลิเคชันจะถูกแบ่งออกเป็นองค์ประกอบย่อย ๆ เรียกว่า เซกเมนต์ (segment) เพื่อส่งผ่านไปในเครือข่ายโดยอาศัย IP datagram ขนาดของเซกเมนต์จะถูกกำหนดโดยโพรโทคอลในชั้น TCP เองและไม่ขึ้นกับขนาดของข้อมูลที่ส่งมาจากโปรแกรมแอพพลิเคชั่น

ทุกครั้งที่ Host ต้นทางส่งเซกเมนต์ออกไปหนึ่งเซกเมนต์ Host ต้นทางจะทำการจับเวลาและรอการตอบกลับจาก Host ปลายทางว่าได้รับเซกเมนต์ที่ส่งออกมาเรียบร้อยหรือไม่ การตอบรับจะอยู่ในรูปของเซกเมนต์ตอบรับที่ Host ปลายทางส่งกลับมา การทำเช่นนี้จะช่วยให้ Host ต้นทางมั่นใจว่าเซกเมนต์ที่ตัวเองเป็นผู้ส่งออกไปจะถึง Host ปลายทางได้อย่างถูกต้อง สำหรับกรณีที่ Host ต้นทางยังไม่ได้รับเซกเมนต์ตอบรับจาก Host ปลายทางและช่วงเวลาที่จับเวลาไว้สิ้นสุดลง Host ต้นทางจะคิดเอาเองว่าการส่งเซกเมนต์ดังกล่าวล้มเหลว และจะทำการส่งเซกเมนต์เดิมออกไปซ้ำอีกครั้ง

2.3 โครงสร้างของ TCP

จากภาพที่ 2.3 แสดงให้เห็นถึงโครงสร้างของ TCP [3] โดยที่ 2 ฟิลด์แรกคือ หมายเลขพอร์ท TCP ของ Host ต้นทาง (Source port) และหมายเลขพอร์ท TCP ของ Host ปลายทาง (Destination port) ฟิลด์ทั้งสองเป็นส่วนที่ทำหน้าที่ระบุหมายเลขพอร์ทหรือชนิดของโปรแกรมแอพพลิเคชัน



ภาพที่ 2.3 โครงสร้างของ TCP

ฟิลด์ sequence number และฟิลด์ acknowledgement number มีขนาดเท่ากันคือ 32 บิท กำหนดให้มีการทำงานร่วมกันสำหรับตรวจสอบความถูกต้องในการส่งผ่านข้อมูล ฟิลด์ sequence number ใช้ระบุหมายเลขไบท์ในสตรีมข้อมูลในขณะที่ Host ต้นทางกำลังส่งอยู่ เนื่องจากไบท์ทุกไบท์ในสตรีมของโพรโทคอล TCP จะมีการจัดสรรหมายเลขให้โดยเรียงลำดับจากค่าน้อยไปหามาก หมายเลขที่ใช้มีค่าอยู่ระหว่าง 0 ถึง 2^{32}-1 เมื่อใดที่ได้ใช้ถึงตัวเลขที่มีค่าสูงสุดแล้วก็จะวนกลับมาใช้เลขศูนย์ใหม่ ส่วนฟิลด์ ackhowledgement number ได้รับการกำหนดจาก Host ปลายทาง ค่าที่บรรจุอยู่ในฟิลด์นี้จะถูกกำหนดให้สอดคล้องกับหมายเลขของฟิลด์ sequence number ในเซกเมนต์ข้อมูลที่ส่งมาจาก Host ต้นทางเพื่อแสดงความหมายว่า Host ปลายทางกำลังรอรับหมายเลขของไบท์ถัดไปในสตรีมข้อมูลหมายเลขใดอยู่ ทั้งนี้หมายเลขของไบท์สตรีมก่อนหน้านี้ทั้งหมดนั้นให้เข้าใจว่ารับได้ถูกต้องเรียบร้อยแล้ว

ฟิลด์ header length มีขนาด 4 บิท ใช้บอกถึงขนาดของ Header ในเซกเมนต์ โดยตัวเลขที่ระบุเป็นจำนวนเท่าของ 4 ไบท์ ซึ่งปกติ Header จะมีขนาดคงที่เท่ากับ 20 ไบท์ หรือเท่ากับ 5 Header จะมีขนาดเพิ่มขึ้นเมื่อมีการใช้ฟิลด์ option ซึ่งมีขนาดไม่คงที่ขึ้นอยู่กับชนิดของ option ที่เลือกใช้ โดย Header จะมีขนาดสูงสุดไม่เกิน 60 ไบท์

ฟิลด์ Reserved ถูกสำรองไว้สำรับใช้ในอนาคต

ฟิลด์ Code Bits จะมีขนาด 6 บิท เป็นฟิลด์ที่ใช้บ่งบอกถึงชนิดของเซกเมนต์ที่ใช้งานอยู่ ซึ่งมีรายละเอียดและหน้าที่ ดังต่อไปนี้

- URG : บิทนี้จะถูกเซ็ทเพื่อแสดงว่า เซกเมนต์มีการใช้งานฟิลด์ urgent pointer อยู่ โดยจะใช้งานร่วมกัน เพื่อบอกให้โปรแกรมของ Host ปลายทางหยุดอ่านสตรีมข้อมูลที่อยู่ก่อนหน้านี้ทั้งหมดชั่วคราว และให้อ่านข้อมูลเร่งด่วนที่อยู่ในเซกเมนต์ส่วนนี่ก่อนที่จะทำกิจกรรมเดิมต่อไป การใช้งานของบิท URG เกิดขึ้นเฉพาะในกรณี เช่น ผู้ใช้อาจต้องการยกเลิกการติดต่อสื่อสารกลางคัน จึงทำการยกเลิก ข้อมูลการขอยกเลิกการสื่อสารจึงถูกส่งออกไปอย่างเร่งด่วนในเซกเมนต์ที่มีการเซ็ทบิท URG ทั้งนี้ ฟิลด์ urgent pointer มีหน้าที่ระบุตำแหน่งจุดสิ้นสุดของข้อมูลเร่งด่วนภายในเซกเมนต์
- ACK : ใช้เพื่อบอกว่ามีการใช้งานฟิลด์ acknowledgement number ในการตอบรับเซกเมนต์
- PSH : บิทนี้จะถูกเซ็ทในกรณีที่ต้องการให้เลเยอร์ TCP ของ Host ปลายทางส่งข้อมูลต่อไปให้โปรแกรมแอพพลิเคชันทันที ทั้งนี้เพราะโดยปกติโพรโทคอล TCP จะสะสมและเก็บเซกเมนต์ไว้จนกว่าจะมีปริมาณมากพอจึงค่อยส่งต่อให้โปรแกรมแอพพลิเคชันเพื่อลดปริมาณงานการติดต่อลง บิท PSH นี้มีความสำคัญต่อโปรแกรมแอพพลิเคชันบางประเภทที่มีการส่งข้อมูลทีละอักขระและมีการโต้ตอบไปมาระหว่างสองฝ่าย
- RST : บิทนี้จะใช้งานเมื่อมีความผิดพลาดของการทำงานเกิดขึ้น และระบบไม่สามารถจัดการกับปัญหาเหล่านี้ได้อีกต่อไป การส่งเซกเมนต์ที่เซ็ทบิท RST จึงเป็นกลไกในการปิดการเชื่อมต่อหรือยกเลิกการเชื่อมต่อ
- SYN : บิทนี้ใช้งานเฉพาะสำหรับแสดงความต้องการในการขอเปิดการเชื่อมต่อระหว่าง Host เริ่มแรก Host ด้านหนึ่งจะส่งเซกเมนต์ที่มีการเซ็ทบิท SYN ออกไป หาก Host ปลายทางต้องการเปิดการเชื่อมต่อก็จะส่งเซกเมนต์ที่เซ็ทบิท SYN ตอบรับกลับไป
- FIN : บิทนี้มีหน้าที่กลับกันกับบิท SYN คือมีไว้สำหรับ Host เพื่อใช้แจ้งการขอยกเลิกการเชื่อมต่อ เนื่องจากไม่มีข้อมูลเหลือสำหรับส่งอีกต่อไป

ฟิลด์ window size มีขนาด 16 บิท มีไว้สำหรับให้ Host ปลายทางใช้ในการประกาศขนาดของ window ที่ตัวเองอนุญาตให้ Host ต้นทางใช้งานได้ ขนาดของ window เป็นตัวกำหนดจำนวนไบท์สตรีมที่ Host ต้นทางสามารถส่งออกอย่างต่อเนื่องโดยไม่ต้องรอการตอบกลับจาก Host

ปลายทาง เพราะฉะนั้น Host ปลายทางจึงสามารถควบคุมปริมาณหรืออัตราการส่งเซกเมนต์ของ Host ต้นทางได้

ฟิลด์ checksum มีขนาด 16 บิททำหน้าที่ตรวจสอบความถูกต้องขององค์ประกอบทุกส่วนในเซกเมนต์คือ ทั้ง Header และข้อมูล

ฟิลด์ urgent pointer มีขนาด 16 บิท จะมีความหมายก็ต่อเมื่อบิท URG= 1 เท่านั้น เมื่อ Host ปลายทางได้รับเซกเมนต์ที่มีการเซ็ทบิท URG ก็จะทำการอ่านค่าฟิลด์ urgent pointer เพื่อให้ทราบถึงตำแหน่งไบท์สุดท้ายของข้อมูลเร่งด่วนในเซกเมนต์นั้น

ฟิลด์ options ใน Header ของโพรโทคอล TCP มีขนาดที่เปลี่ยนแปลงได้ โดยขนาดที่แน่นอนของแต่ละเซกเมนต์สวามารถดูได้จากฟิลด์ Header length

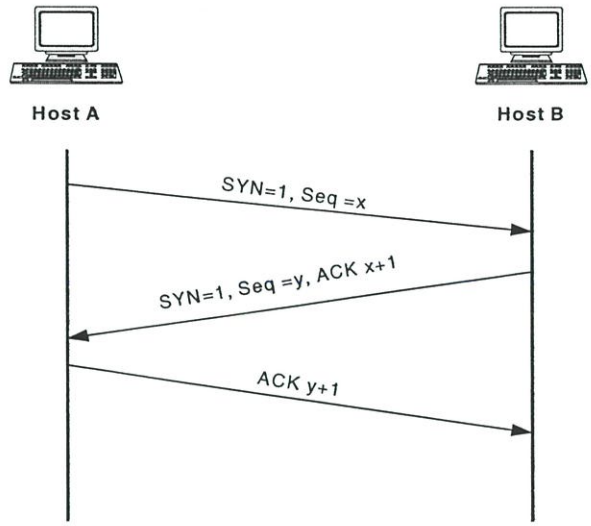
2.4 การสร้างและการยกเลิกการเชื่อมต่อ TCP

ในการติดต่อสื่อสารกันระหว่าง Host ต้นทางและปลายทาง จำเป็นต้องมีการสร้างการเชื่อมต่อกันก่อนและหลังจากที่ไม่มีความจำเป็นหรือไม่ต้องการการเชื่อมต่อนั้น ก็สามารถยกเลิกการเชื่อมต่อได้ โดยสามารถอธิบายได้ ดังนี้

2.4.1 การสร้างการเชื่อมต่อ TCP

กระบวนการในการสร้างการเชื่อมต่อของโพรโทคอล TCP ระหว่าง Host ต้นทางและปลายทาง สามารถแบ่งออกได้เป็น 3 ขั้น ดังภาพที่ 2.4 ดังนี้

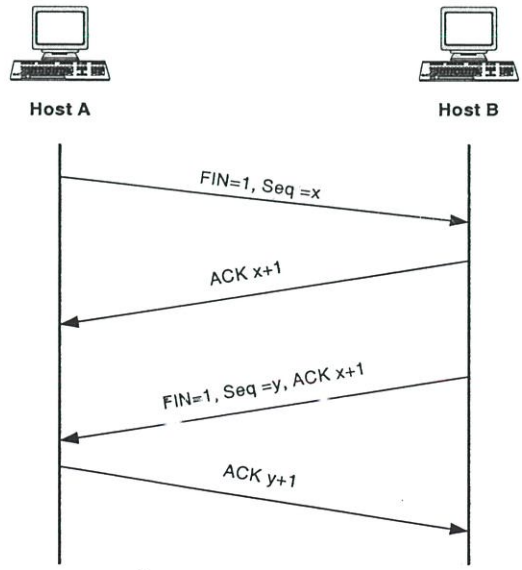
- ขั้นตอนแรก เมื่อ Host A ต้องการเริ่มการติดต่อ ก็จะทำการส่งเซกเมนต์ที่เซ็ตบิท SYN ในฟิลด์ code ให้เป็น 1พร้อมกับเลือกหมายเลข seq ขึ้นหนึ่งค่าเพื่อบรรจุลงในฟิลด์ sequence number ในตัวอย่างนี้คือ x ค่า seq ที่เลือกนี้จะใช้เป็นค่าเริ่มต้นสำหรับการติดต่อสื่อสารที่จะเกิดขึ้นในลำดับต่อไป
- ขั้นต่อมาเมื่อ Host B ตอบรับการขอเปิดการเชื่อมต่อด้วยเซกเมนตที่เซ็ทบิท SYN=1 และ ACK=1 ของฟิลด์ code พร้อมกับเลือกหมายเลข Seq ของตัวเองเพื่อบรรจุลงในฟิลด์ sequence number สำหรับใช้เป็นค่าเริ่มต้นของหมายเลขที่ใช้กำกับให้กับเซกเมนต์ที่จะส่งในลำดับถัดไป ในการตอบรับด้วยบิท ACK จะใช้ควบคุมกับฟิลด์ acknowledgement number ซึ่งจะบรรจุค่า x+1 สังเกตว่าเซกเมนต์ SYN จะใช้หมายเลข sequence number ไปหนึ่งหมายเลข
- ขั้นตอนสุดท้าย เมื่อ Host A ยืนยันการเปิดการเชื่อมต่อกับ Host B โดยการส่งเป็นเซกเมนต์ที่เซ็ทบิท ACK เท่านั้น ไม่ใช้บิท SYN อีกต่อไป ส่วนค่าในฟิลด์ ackhowledgement number ตั้งให้มีค่าเท่ากับ y+1



ภาพที่ 2.4 ขั้นตอนการสร้างการเชื่อมต่อของโพรโทคอล TCP

2.4.2 การยกเลิกการเชื่อมต่อ TCP

เนื่องจากการเชื่อมต่อสื่อสารของโพรโทคอล TCP เป็นแบบ Full duplex คือสามารถรับส่งข้อมูลทั้งสองทิศทางได้พร้อมกันและไม่ขึ้นแก่กัน กระบวนการปิดการเชื่อมต่อเพื่อยกเลิกการเชื่อมต่อระหว่าง Host ในโพรโทคอล TCP จึงสามารถแยกทำแต่ละทิศทางอิสระจากกันได้ คือเมื่อ Host ด้านใดด้านหนึ่งไม่มีข้อมูลจะส่งอีกต่อไป Host ดังกล่าวสามารถขอปิดการเชื่อมต่อสำหรับทิศทางการส่งของตัวเองเพียงด้านเดียวได้โดยส่งเซกเมนต์ที่ได้เซ็ทบิท FIN = 1 ออกไปเพื่อแสดงความต้องการในการปิดการส่งของตัวเอง Host อีกด้านหนึ่งก็จะตอบกลับโดยส่งเซกเมนต์ที่เซ็ทลบิท ACK = x+1 ในขณะเดียวกันก็แจ้งให้โปรแกรมแอพพลิเคชันของตัวเองให้รับทราบว่าจะไม่มีข้อมูลใหม่เข้ามาจากการเชื่อมต่อดังกล่าวอีกต่อไป ดังภาพที่ 2.5



ภาพที่ 2.5 ขั้นตอนการยกเลิกการเชื่อมต่อของโพรโทคอล TCP

บทที่ 3

โพรโทคอล Open Shortest Path First

Open Shortest Path First (OSPF) [3] ได้ถูกพัฒนาขึ้นโดยองค์กร Internet Engineering Task Force (IEFT) ซึ่ง เป็นโพรโทคอลแบบ Link Stateที่ใช้อัลกอลิธึ่มแบบ Dijkstra's Shortest Path First และ เป็นแบบระบบเปิด (Open)

ประโยชน์หลักของ OSPF คือ มีค่า reconvergence ที่เร็ว สามารถรองรับเครือข่ายที่มีขนาดใหญ่มากได้ และมีความหวั่นไหวกับข้อมูลของเส้นทางเดิน (Routing information) น้อย คุณสมบัติอื่น ๆ ของ OSPF มีดังนี้

1. ใช้แอเรีย (Areas) ซึ่งลดผลกระทบของโพรโทคอลต่อ CPU และหน่วยความจำที่บรรจุการไหลเวียนของทราฟฟิกโพรโทคอลของเส้นทาง (routing protocol) และทำให้การสร้างโทโปโลยีของเครือข่ายเป็นไปตามลำดับชั้น (hierarchical) ได้
2. ไม่มีการแบ่งชนชั้น (classless) ซึ่งจะช่วยกำจัดปัญหาของ subnet ที่ไม่อยู่ติดกันได้
3. รองรับตารางเส้นทาง classless VLSM และ supernetting สำหรับการจัดการแอดเดรสได้อย่างมีประสิทธิภาพ
4. สามารถจัดโหลดให้สมดุลย์ได้เมื่อมีเส้นทางหลาย ๆ เส้นทาง
5. ใช้แอดเดรสแบบจุดต่อหลาย ๆ จุด (multicast address) ที่สำรองไว้ เพื่อลดผลกระทบที่เกิดจากอุปกรณ์ที่ไม่ใช้ OSPF
6. รองรับการรับรองตัวตน (authentication) เพื่อการจัดเส้นทางที่ปลอดภัย
7. ใช้ tag เพื่อการติดตามเส้นทางที่มาจากภายนอก

3.1 การทำงานของ OSPF

การทำงานของ OSPF สามารถอธิบายได้ ดังนี้

1. เราท์เตอร์ต่าง ๆ ที่ติดต่อกันด้วย OSPF (OSPF-speaking) จะทำการส่งแพ็คเก็ต Hello ไปยังทุก ๆ interface ที่รองรับ OSPF ถ้าเราท์เตอร์ 2 ตัวมีการแบ่ง data link ร่วมกันตามค่าพารามิเตอร์ที่ตกลงไว้ในแพ็กเก็ต Hello ต่าง ๆ โดยลำดับ เราท์เตอร์ทั้ง 2 ตัวจะกลายเป็นเพื่อนบ้านกัน (Neighbor)

2. การอยู่ติดกัน (Adjaceney) ซึ่งอาจจะถูกคิดได้ตามการเชื่อมต่อแบบจุดต่อจุดเสมือน ได้ถูกจัดรูปแบบไว้ระหว่างเพื่อนบ้านกับเพื่อนบ้าน OSPF ได้กำหนดชนิดของเครือข่ายและชนิดของเราท์เตอร์ไว้มากมาย การสร้างการอยู่ติดกันในรูปแบบหนึ่งได้ถูกกำหนดตามชนิดของการแลกเปลี่ยน Hello ของเราท์เตอร์ และตามชนิดของเครือข่ายที่ Hello ได้ถูกแลกเปลี่ยนกัน

3. เราท์เตอร์แต่ละตัวส่ง Link State Advertisements (LSAs) ให้กับเราท์เตอร์ที่อยู่ติดกัน LSAs จะอธิบายถึงการเชื่อมต่อของเราท์เตอร์ทุก ๆ ตัวหรือทุก ๆ interface และสถานะของการเชื่อมต่อ การเชื่อมต่อเหล่านี้อาจจะเป็น เครือข่าย Stub (เครือข่ายที่ไม่มีเราท์เตอร์ต่ออยู่) เราท์เตอร์อื่น ๆ ที่ใช้ OSPF เครือข่ายในแอเรียอื่น หรือเครือข่ายจากภายนอก (เครือข่ายที่เรียนรู้จากกระบวนการของเส้นทางอื่น)

4. เราท์เตอร์แต่ละตัวที่ได้รับ LSA มาจากเพื่อนบ้านจะทำการบันทึก LSA ลงในฐานข้อมูล link state ในตัวมันเอง และส่งสำเนาของ LSA ไปยังเพื่อนบ้านอื่น ๆ ของตัวมันเองทั้งหมด

5. เนื่องจากการไหลเวียนของ LSA กระจายครอบคลุมทั่วแอเรีย เราท์เตอร์ทั้งหมดจะทำการสร้างฐานข้อมูล link state ที่เหมือนกัน

6. เมื่อฐานข้อมูลเสร็จสมบูรณ์ เราท์เตอร์แต่ละตัวจะใช้อัลกอลิธึ่ม SPF เพื่อคำนวณหากราฟที่ไม่มีการลูป (loop) ที่บ่งบอกถึงเส้นทางที่สั้นที่สุด (มีค่า cost ต่ำที่สุด) กับทุก ๆ ปลายทางที่รู้จักด้วยตัวของมันเอง นั่นคือ root กราฟนี้เรียกว่า SPF tree

7. เราท์เตอร์แต่ละตัวจะทำการสร้างตารางเส้นทางของตัวเองจาก SPF tree

เมื่อข้อมูล link state ทั้งหมดถูกแพร่กระจายไปยังเราท์เตอร์ทุกตัวในแอเรีย นั่นคือ ฐานข้อมูล link state ซิงค์โครไนซ์กัน และตารางเส้นทางถูกสร้างขึ้น OSPF ก็จะเสร็จสิ้น แพ็กเก็ต Hello จะถูกแลกเปลี่ยนกันระหว่างเพื่อนบ้านตามค่า keepalive และ LSAs จะถูกส่งซ้ำ ๆ กัน ทุก ๆ 30 นาที ถ้าหากว่า โทโปโลยีของเครือข่ายมีเสถียรภาพก็จะไม่มีกิจกรรมใด ๆ เกิดขึ้น

3.2 เพื่อนบ้านและการอยู่ติดกัน (Neighbors and Adjacencies)

ก่อนที่จะมีการส่ง LSAs เราท์เตอร์ OSPF ต้องค้นพบเพื่อนบ้านและสร้างการอยู่ติดกัน จากนั้นเพื่อนบ้านจะถูกบันทึกลงในตารางเพื่อนบ้าน (neighbor table) ตามด้วยข่ายเชื่อมโยง หรืออินเทอร์เฟส (interface) ที่ซึ่งเพื่อนบ้านแต่ละตัวตั้งอยู่ และข้อมูลอื่น ๆ ที่จำเป็น ดังภาพที่ 3.1

```
Monet#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.30.70     1   FULL/DR         00:00:34    192.168.17.73   Ethernet0
192.168.30.254    1   FULL/DR         00:00:34    192.168.32.2    Ethernet1
192.168.30.70     1   FULL/BDR        00:00:34    192.168.32.4    Ethernet1
192.168.30.30     1   FULL/ -         00:00:33    192.168.17.50   Serial0.23
192.168.30.10     1   FULL/ -         00:00:32    192.168.17.9    Serial1
192.168.30.68     1   FULL/ -         00:00:39    192.168.21.134  Serial2.824
192.168.30.18     1   FULL/ -         00:00:30    192.168.21.142  Serial2.826
192.168.30.70     1   FULL/ -         00:00:36    192.168.21.170  Serial2.836
```

ภาพที่ 3.1 ตารางเพื่อนบ้านซึ่งติดต่อกันด้วย OSPF

เพื่อการติดตามเราท์เตอร์ OSPF ตัวอื่น ๆ เราท์เตอร์แต่ละตัวจะมี router ID เพียง 1 ID และ 1 IP address ตามที่เราท์เตอร์ถูกจำแนกออกเป็นลักษณะเฉพาะภายในโดเมน OSPF เราท์เตอร์สามารถรับเราท์เตอร์ ID ได้ดังนี้

1. เราท์เตอร์จะเลือกจากค่าไอพีแอดเดรสที่มีค่าสูงที่สุดจากอินเทอร์เฟส loopback ต่าง ๆ ของตัวเอง

2. ถ้าอินเทอร์เฟส loopback ไม่ได้ถูกกำหนดไอพีแอดเดรสไว้ เราท์เตอร์จะทำการเลือกจากไอพีแอดเดรสที่มีค่าสูงที่สุดจากอินเทอร์เฟสต่างในตัวมันเอง ซึ่งไม่จำเป็นต้องรัน OSPF

การใช้แอดเดรสจากอินเทอร์เฟส loopback มีประโยชน์อยู่ 2 ประการ

1. อินเทอร์เฟส loopback มีเสถียรภาพมากกว่าอินเทอร์เฟสอื่น ๆ ซึ่งจะทำงานเมื่อเราท์เตอร์ถูกบูต และจะใช้งานไม่ได้เมื่อเราท์เตอร์พัง

2. เราท์เตอร์ที่ใช้ OSPF จะเริ่มต้นด้วยความสัมพันธ์ของเพื่อนบ้านโดยการประกาศ ID ของเราท์เตอร์ของตัวเองภายในแพ็กเก็ต Hello

3.2.1 โพรโทคอล Hello (Hello Packet)

โพรโทคอล Hello ใช้เพื่อรองรับวัตถุประสงค์ต่าง ๆ ดังนี้

1. เป็นวิธีการที่ใช้ค้นหาเพื่อนบ้าน

2. ทำหน้าที่ประกาศค่าพารามิเตอร์ต่าง ๆ ให้กับเราท์เตอร์ 2 ตัวก่อนที่เราท์เตอร์ทั้ง 2 ตัวจะกลายเป็นเพื่อนบ้านกัน

3. แพ็กเก็ต Hello ทำหน้าที่ keepalives ระหว่างเพื่อนบ้าน

4. รับรองการสื่อสาร 2 ทางระหว่างเพื่อนบ้าน

5. ทำหน้าที่เลือก Designated Routers (DRs) และ Backup Designated Routers (BDRs) บนเครือข่าย Broadcast และ Nonbroadcast Multiaccess (NBMA)

เราท์เตอร์ที่มีการติดต่อกันด้วย OSPF จะส่งแพ็กเก็ต Hello ออกไปยังแต่ละอินเทอร์เฟสที่ใช้งาน OSPF เป็นช่วงเวลา ซึ่งช่วงเวลานี้เรียกว่า Hello Interval โดยมีค่า default อยู่ที่ 30 วินาที ถ้าหากว่าเราท์เตอร์ไม่ได้ยิน Hello จากเพื่อนบ้านภายในเวลาที่กำหนด เราเรียกว่า Router Dead Interval เราท์เตอร์จะบอกสถานะว่า เพื่อนบ้านหาย

3.2.2 องค์ประกอบของแพ็กเก็ต Hello

แพ็กเก็ต Hello ประกอบด้วยข้อมูลดังต่อไปนี้

1. ID เราท์เตอร์ของเราท์เตอร์ตัวต้นทาง

2. ID แอเรียของอินเทอร์เฟสเราท์เตอร์ตัวต้นทาง

3. แอดเดรสมาร์คของอินเทอร์เฟสด้านต้นทาง

4. ชนิดและข้อมูลของการแสดงการมีตัวตน (authentication) สำหรับอินเทอร์เฟสด้านต้นทาง

5. Hello Interval และ Router Dead Interval ของอินเทอร์เฟสด้านต้นทาง

6. ลำดับความสำคัญของเราท์เตอร์

7. DR และ BDR

8. บิท flag 5 บิท ที่แสดงถึงความจุ

9. เราท์เตอร์ ID ของเพื่อนบ้านของเราท์เตอร์ด้านต้นทาง

เมื่อเราท์เตอร์ได้รับ Hello จากเพื่อนบ้าน ก็จะทำการพิสูจน์ว่าค่า แอเรีย ID การรับรองตัวตน network mask HelloInterval RouterDeadInterval และออปชั่นมีค่าตรงกันกับอินเทอร์เฟสด้านรับหรือไม่ ถ้าหากว่าไม่ตรงกัน แพ็กเก็ตจะถูกตัดทิ้งและไม่มีการสร้างการอยู่ติดกันขึ้น แต่ถ้าหากว่าค่าทุก ๆ ค่าที่กล่าวถึงมีค่าตรงกัน แพ็กเก็ต Hello จะถูกประกาศให้มีผลใช้งานได้ และถ้าหากว่า ID ของเราท์เตอร์ด้านต้นทางถูกเก็บรายชื่อไว้ในตารางเพื่อนบ้านสำหรับอินเทอร์เฟสด้านรับแล้ว เวลาของ RouterDeadInterval ก็จะถูกรีเซ็ท ถ้าหากเราท์เตอร์ ID ยังไม่มีอยู่ในตาราง เราท์เตอร์ ID ก็จะถูกเพิ่มเข้าไปในตารางเพื่อนบ้าน

3.3 ชนิดของเครือข่าย (Network Types)

OSPF ได้กำหนดชนิดของเครือข่ายไว้ 5 ชนิด ดังนี้

1. เครือข่ายแบบ จุดต่อจุด (Point-to-Point networks)

2. เครือข่ายแบบบรอดคลาส์ (Broadcast networks)

3. เครือข่ายแบบ การเข้าถึงได้หลายช่องทางชนิดไม่บรอดคลาส์ (Non-broadcast Multi-access [NBMA])

4. เครือข่ายแบบ จุดต่อหลาย ๆ จุด (Point-to-multipoint networks)

5. การเชื่อมโยงเสมือน (Virtual links)

เครือข่ายทั้ง 5 แบบสามารถจัดแบ่งออกได้เป็น 2 ชนิดใหญ่ ๆ ดังนี้

1. เครือข่ายส่งผ่าน (Transit networks) มีเราท์เตอร์ถูกต่ออยู่ 2 ตัวหรือมากกว่า ซึ่งนำพาแพ็กเก็ต “just passing through” ที่เกิดขึ้นและถูกกำหนดไว้สำหรับเครือข่าย ๆ หนึ่ง

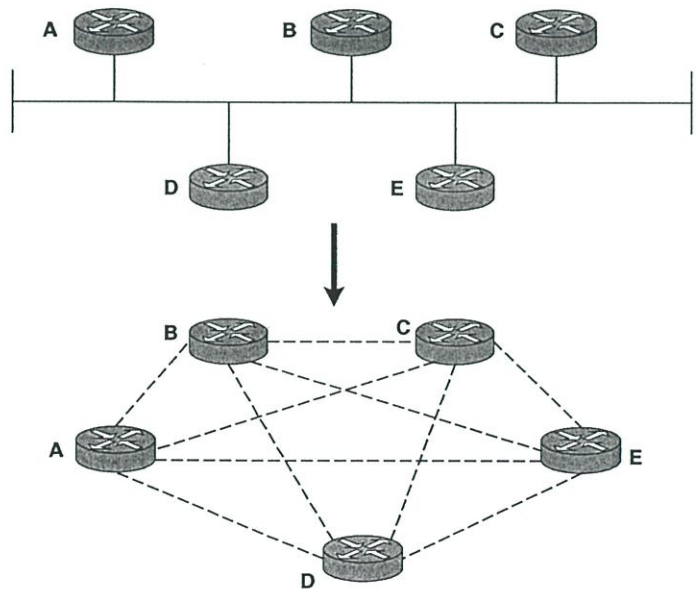
2. เครือข่าย Stub มีเพียงเราท์เตอร์ที่ต่ออยู่เพียงตัวเดียว แพ็กเก็ตบนเครือข่าย stub จะมีแอดเดรสของต้นกำเนิดหรือไม่ก็แอดเดรสของปลายทางที่เป็นของเครือข่ายนั้น นั่นคือ ทุก ๆ แพ็กเก็ตเกิดขึ้นโดยอุปกรณ์ตัวหนึ่งบนเครือข่ายหรือถูกกำหนดไว้สำหรับอุปกรณ์ตัวหนึ่งบนเครือข่าย

3.4 Designated Routers และ Backup Designated Routers

เครือข่ายแบบเข้าถึงหลายช่องทางแสดงให้เห็นถึงปัญหาสำหรับ OSPF 2 อย่างซึ่งสัมพันธ์กับการแพร่กระจายของ LSAs ดังนี้

1. การสร้างการอยู่ติดกันระหว่างเราท์เตอร์ที่ต่อกันทุก ๆ ตัวจะสร้าง LSAs ที่ไม่จำเป็นจำนวนมาก ถ้า n คือจำนวนของเราท์เตอร์บนเครือข่ายแบบเข้าถึงหลายช่องทาง เพราะฉะนั้นจะมีการอยู่ติดกันเท่ากับ n(n-1)/2 (ดังภาพที่ 3.2) เราท์เตอร์แต่ละตัวจะกระจาย LSAs เป็นจำนวน n-1 สำหรับเพื่อนบ้านที่อยู่ติดกันกับตัวมันเอง บวกด้วย 1 LSA สำหรับเครือข่าย ได้ผลลัพธ์เท่ากับ n^2 ที่เกิดจากเครือข่าย

2. การแพร่กระจายของเครือข่ายด้วยตัวเองจะสับสน เราท์เตอร์ตัวหนึ่งจะกระจาย LSA หนึ่ง ๆ ไปยังเพื่อนบ้านที่อยู่ติดกันกับตัวมันทั้งหมด ซึ่งโดยรอบแล้ว LSA นั้นจะแพร่กระจายไปยังเพื่อนบ้านที่อยู่ติดกันของพวกมันทั้งหมด ทำให้เกิดการสร้างสำเนาของLSA เดียวกันบนเครือข่ายเดียวกันเป็นจำนวนมาก



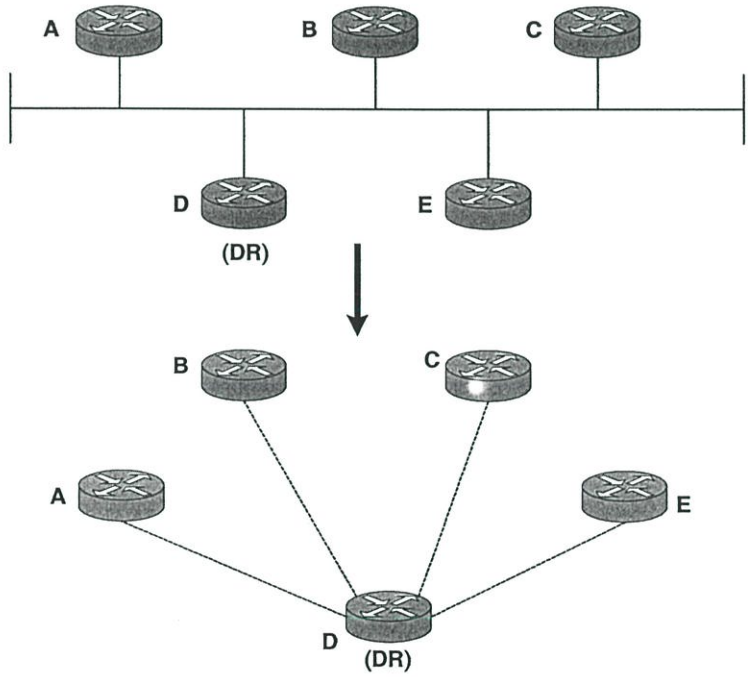
ภาพที่ 3.2 การอยู่ติดกันทั้ง 10 เส้นทางสำหรับเราท์เตอร์ 5 เครื่องบนเครือข่าย OSPF ด้วย 25 LSAs

ในเครือข่ายการเข้าถึงหลายช่องทางจึงได้เลือก Designated Router ขึ้นมาเพื่อป้องกันปัญหาดังกล่าวข้างต้น โดยที่ DR มีหน้าที่ดังนี้

1. แทนเครือข่ายการเข้าถึงหลายช่องทางและเราท์เตอร์ที่ต่ออยู่ของตัวมันเองเพื่อเป็นที่พักของเครือข่ายที่เชื่อมต่อกัน

2. เพื่อการจัดการขบวนการในการแพร่กระจายบนเครือข่ายการเข้าถึงหลายช่องทาง

เราท์เตอร์แต่ละตัวบนเครือข่ายจัดรูปแบบการอยู่ติดกันด้วย DR (ดังภาพที่ 3.3) ซึ่ง DR เท่านั้นที่จะส่ง LSAs ไปยังจุดพักของเครือข่ายที่เชื่อมต่อกัน และเพื่อป้องกันปัญหาที่จะทำให้เครือข่ายไม่สามารถส่งผ่านแพ็กเก็ตได้เมื่อ DR เสียหายหรือพังลง คือจะมีการเลือก Backup Designated Router ซึ่งจะทำให้ DR และ BDR กลายเป็นตัวที่อยู่ติดกันเอง ซึ่งถ้าหากว่า DR พัง BDR ก็จะกลายเป็น DR ตัวใหม่



ภาพที่ 3.3 Designated Router ซึ่งทำหน้าที่เป็นเครือข่ายเข้าถึงได้หลายช่องทาง ทำให้เราท์เตอร์ตัวอื่น ๆ อยู่ติดกันได้โดยผ่าน DR

กระบวนการในการเลือก DR และ BDR มีดังนี้

1. หลังจากการสื่อสาร 2 ทางได้ถูกสร้างขึ้นกับเพื่อนบ้าน ตรวจสอบสิทธิพิเศษ DR และBDR ของ Hello แต่ละตัวจากเพื่อนบ้านแล้ว รายชื่อของเราท์เตอร์ทุกตัวมีสิทธิที่จะได้รับเลือก (นั่นคือ เราท์เตอร์ที่มีสิทธิพิเศษที่มากกว่า 0 และมีสถานะของเพื่อนบ้านไม่น้อยกว่า 2 ทาง) เราท์เตอร์ทั้งหมดก็จะประกาศตัวของมันให้เป็น DR และ BDR (แอดเดรสของอินเทอร์เฟสของตัวพวก

มันเองที่อยู่ในฟิลด์ DR และ BDR ของแพ็กเก็ต Hello) การคำนวณของเราท์เตอร์ได้รวมถึงตัวมันเองที่อยู่ในรายชื่อนี้ ยกเว้นว่าตัวมันเองไม่มีสิทธิในการรับเลือก

2. จากรายชื่อของเราท์เตอร์ที่มีสิทธิได้รับเลือกจะมีการแบ่ง subset ของเราท์เตอร์ที่ประสงค์จะไม่อ้างสิทธิเป็น DR ออก (เราท์เตอร์ที่ประกาศตัวของพวกมันเองที่เป็น DR จะไม่สามารถถูกเลือกให้เป็น BDR ได้)

3. ถ้าเพื่อนบ้าน 1 ตัวหรือมากกว่าที่อยู่ใน subset นี้รวมถึงแอดเดรสของอินเทอร์เฟสของตัวมันเองในฟิลด์ BDR จะทำให้เพื่อนบ้านที่มีค่าสิทธิพิเศษสูงที่สุดถูกประกาศให้เป็น BDR ในทางพันธะ เราท์เตอร์ที่มี ID เราท์เตอร์สูงที่สุดจะถูกเลือก

4. ถ้าไม่มีเราท์เตอร์ใน subset อ้างสิทธิเป็น BDR เพื่อนบ้านที่มีค่าสิทธิพิเศษสูงที่สุดนะกลายเป็น BDR ในทางพันธะ เพื่อนบ้านที่มี ID เราท์เตอร์สูงที่สุดจะถูกเลือก

5. ถ้ามีเราท์เตอร์ 1 ตัวที่มีสิทธิเข้ารับเลือกหรือมากกว่ารวมทั้งแอดเดรสอินเทอร์เฟสของตัวพวกมันเองในฟิลด์ DR เพื่อนบ้านที่ค่าสิทธิพิเศษสูงที่สุดจะถูกประกาศให้เป็น DR ในทางพันธะ เพื่อนบ้านที่มี ID เราท์เตอร์สูงที่สุดจะถูกเลือก

6. ถ้าไม่มีเราท์เตอร์ประกาศตัวเองเป็น DR BDR ที่ถูกเลือกใหม่จะกลายเป็น DR

7. ถ้าเราท์เตอร์ที่กระทำการคำนวณคือ DR หรือ BDR ที่ถูกเลือกขึ้นใหม่ หรือไม่มี DR หรือ BDR อยู่เลย กระบวนที่ 2 ถึง 6 ก็จะเกิดขึ้นซ้ำ

ถ้ากล่าวโดยง่ายคือ เมื่อเราท์เตอร์ OSPF เริ่มทำงานมันก็จะทำการค้นหาเพื่อนบ้าน โดยจะทำการตรวจสอบ DR และ BDR ที่ทำงานอยู่ ถ้าหากว่ามี DR และ BDR อยู่ก่อนแล้ว เราท์เตอร์ก็จะยอมรับ DR และ BDR ถ้าหากไม่มี BDR เราท์เตอร์ตัวที่มีค่าสิทธิพิเศษสูงที่สุดจะถูกเลือกเป็น BDR แต่ถ้าหากมีเราท์เตอร์มากกว่า 1 ตัวมีค่าสิทธิพิเศษเท่ากัน เราท์เตอร์ตัวที่มี ID เราท์เตอร์สูงที่สุดก็จะได้รับเลือก ถ้าหากไม่มี DR แอกทีฟ BDR ก็จะถูกเลื่อนให้เป็น DR และทำการเลือก BDR ขึ้นใหม่

3.5 OSPF Interfaces

ส่วนประกอบสำคัญของโพรโทคอล link state คือการเชื่อมโยงและสถานะของการเชื่อมโยง ซึ่งก่อนที่จะมีการส่ง Hello ก่อนที่การอยู่ติดกันจะถูกสร้างขึ้น และก่อนที่ LSAs ได้ถูกส่งออกไป เราท์เตอร์ OSPF ต้องเข้าใจการเชื่อมโยงของตัวมันเองก่อน ในหัวข้อนี้อธิบายถึงโครงสร้างข้อมูล OSPF ที่เกี่ยวข้องกับอินเทอร์เฟสและสถานะต่าง ๆ ของอินเทอร์เฟส OSPF

3.5.1 โครงสร้างข้อมูลอินเทอร์เฟส (Interface Data Structure)

เราท์เตอร์ OSPF มีโครงสร้างข้อมูลสำหรับอินเทอร์เฟสที่ใช้งาน OSPF ไว้ ดังภาพที่ 3.4 ซึ่งองค์ประกอบของโครงสร้างข้อมูลอินเทอร์เฟสมีดังนี้

- IP Address และ Mask : องค์ประกอบนี้คือแอดเดรสและมาส์คของอินเทอร์เฟสที่ถูกคอนฟิกไว้ แพ็กเก็ต OSPF ที่เกิดจากอินเทอร์เฟสนี้จะมีแอดเดรสนี้เป็นแอดเดรสต้นกำเนิด (Source Address) ในภาพที่ 3.4 แอดเดรสและมาส์คคือ 192.168.21.21/30

- แอเรีย ID : แอเรียที่อินเทอร์เฟสและเครือข่ายต่ออยู่ ในภาพที่ 3.4 แอเรีย ID เท่ากับ 7

- Process ID : คุณสมบัติพิเศษของ Cisco นี้ไม่ใช่มาตรฐาน แต่เนื่องจากเราท์เตอร์ Cisco มีความสามารถที่จะรันได้หลาย ๆ Process OSPF จึงใช้ Process ID เพื่อแยกความแตกต่าง ในภาพที่ 3.4 Process ID เป็น 1

- Router ID : ในภาพที่ 3.4 Router ID คือ 192.168.30.70

```
Renoir#show ip ospf interface Ethernet0
Ethernet0 is up, line protocol is up
  Internet Address 192.168.17.73/29, Area 0
  Process ID 1, Router ID 192.168.30.70, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.30.70, Interface address 192.168.17.73
  Backup Designated router (ID) 192.168.30.80, Interface address 192.168.17.74
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.30.80  (Backup Designated Router)
  Message digest authentication enabled
    Youngest key id is 10
```

ภาพที่ 3.4 ข้อมูลบนอินเทอร์เฟสและชนิดของเครือข่ายแบบ point-to-point

- ชนิดของเครือข่าย : ชนิดของเครือข่ายที่อินเทอร์เฟสถูกต่ออยู่ เช่น broadcast point-to-point NBMA point-to-multipoint หรือ virtual link ในภาพที่ 3.4 ชนิดของเครือข่ายคือ point-to-point

- Cost : ค่า Cost ขาออกสำหรับแพ็กเก็ตที่ถูกส่งออกจากอินเทอร์เฟสนี้ ค่า Cost คือ OSPF metric แสดงได้ด้วย เลขจำนวนเต็ม 16 บิทซึ่งอยู่ในช่วง 1 ถึง 65535 ค่า default เท่ากับ 108/BW โดยที่ BW คือค่าแบนด์วิดส์ของอินเทอร์เฟสที่ถูกคอนฟิกไว้ และ 10^8 เป็นแแบนด์วิดส์อ้างอิง ในภาพที่ 3.4 ค่าแบนด์วิดส์ที่ถูกคอนฟิกไว้มีค่าเท่ากับ 128K (ไม่ได้แสดงไว้ในรูป) เพราะฉะนั้นค่า Cost จะเท่ากับ $10^8/128K = 781$

- InfTransDelay : เวลาในการปรากฏ LSA

- State : สถานะหน้าที่ของอินเทอร์เฟส

- ค่าสิทธิพิเศษเราท์เตอร์ : จำนวนเต็ม 8 บิทที่อยู่ในช่วง 0 ถึง 255 เพื่อเลือก DR และ BDR ค่าสิทธิพิเศษนี้ไม่ได้ถูกแสดงไว้ในภาพที่ 3.4 เพราะชนิดของเครือข่ายเป็นแบบจุดต่อจุด จึงทำให้ไม่มี DR หรือ BDR ในเครือข่ายชนิดนี้ ในภาพที่ 3.5 แสดงอินเทอร์เฟส OSPF อื่นในเราท์เตอร์ตัวเดียวกัน อินเทอร์เฟสนี้แสดงให้เห็นถึงชนิดของเครือข่ายที่ต่ออยู่เป็นแบบ broadcast ดังนั้น DR และ BDR จะถูกเลือก ค่าสิทธิพิเศษที่แสดงในรูปมีค่าเป็น 1

- Designated Router : DR สำหรับเครือข่ายที่ซึ่งอินเทอร์เฟสถูกต่ออยู่ได้ถูกบันทึกไว้ทั้ง เราท์เตอร์ ID ของตัวเอง และแอดเดรสของอินเทอร์ที่ต่ออยู่กับเครือข่าย ในภาพที่ 3.5 DR คือ 192.168.30.70 และแอดเดรสของอินเทอร์เฟสเป็น 192.168.17.73

- Backup Designated Router : BDR สำหรับเครือข่ายที่ซึ่งอินเทอร์เฟสถูกต่ออยู่ได้ถูกบันทึกไว้ทั้งเราท์เตอร์ ID ของตัวมันเอง และแอดเดรสของอินเทอร์เฟสที่ต่ออยู่ ในภาพที่ 3.5 BDR คือ 192.168.30.80 และแอดเดรสอินเทอร์เฟสคือ 192.168.17.74

```
Renoir#show ip ospf interface Serial1.738
Serial1.738 is up, line protocol is up
  Internet Address 192.168.21.21/30, Area 7
  Process ID 1, Router ID 192.168.30.70, Network Type Point_To_Point, Cost: 781
  Transmit Delay is 1 sec, State Point_To_Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.30.77
  Message digest authentication enabled
    Youngest key id is 10
```

ภาพที่ 3.5 อินเทอร์เฟสที่มีชนิดของเครือข่ายแบบ broadcast และเราท์เตอร์เป็น DR

- HelloInterval : คาบเวลา (มีหน่วยเป็นวินาที) ระหว่างการส่งแพ็กเก็ต Hello บนอินเทอร์เฟส คาบเวลานี้ถูกประกาศในแพ็กเก็ต Hello ที่ถูกส่งจากอินเทอร์เฟส ค่า Default เท่ากับ 10 วินาที

- RouterDeadInterval : คาบเวลา (หน่วยเป็นวินาที) ที่เราท์เตอร์จะคอยรับ Hello จากเพื่อนบ้านบนเครือข่าย ซึ่งอินเทอร์เฟสถูกเชื่อมต่อก่อนการแจ้งว่าเพื่อนบ้านหายไป RouterDeadInterval ได้ถูกประกาศอยู่ในแพ็กเก็ต Hello ที่ส่งจากอินเทอร์เฟส ค่า Default เท่ากับ 4 เท่าของ HelloInterval

- Wait Timer : ช่วงเวลาที่เราท์เตอร์ใช้คอย DR และ BDR เพื่อการประกาศไปในแพ็กเก็ต Hello ของเพื่อนบ้านก่อนการเริ่มต้นเลือก DR และ BDR ช่วงเวลาของ Wait Timer เท่ากับ RouterDeadInterval

- RxmtInterval : คาบเวลา (หน่วยเป็นวินาที) ที่เราท์เตอร์จะคอยการส่งแพ็กเก็ต OSPF ซ้ำเมื่อไม่มีการตอบรับ (acknowledge) ค่า Default เป็น 5 วินาที

- Hello Timer : เวลาที่ถูกตั้งให้กับ HelloInterval แพ็กเก็ต Hello ได้ถูกส่งจากอินเทอร์เฟสเมื่อ Hello Timer หมดลง

- Neighboring Routers : รายชื่อเพื่อนบ้านทั้งหมดบนเครือข่ายที่ต่ออยู่ ภาพที่ 3.6 แสดงถึงอินเทอร์เฟสอื่นบนเราท์เตอร์ตัวเดียวกัน มี 5 เพื่อนบ้านที่เป็นที่รู้จักบนเครือข่าย แต่มีเพียงการอยู่ติดกันเท่ากับ 2 ตัว (เราท์เตอร์ ID ของเพื่อนบ้านเท่านั้นที่ถูกแสดง) เราท์เตอร์ได้สร้างการอยู่ติดกันกับ DR และ BDR เท่านั้น

- Au Type : ชนิดของการแสดงการมีตัวตน (Authentication) ที่ใช้กับเครือข่าย ชนิดของการแสดงการมีตัวตนอาจจะเป็น Null (ไม่มีการแสดงการมีตัวตน) รหัสผ่านแบบง่าย (Simple Password) หรือ Cryptographic (Message Digest)

- Authentication Key : ใช้รหัสผ่านขนาด 64 บิท ถ้าหากการแสดงการมีตัวตนอย่างง่ายถูกใช้งานกับอินเทอร์เฟส หรือใช้ message digest key ถ้าใช้การแสดงการมีตัวตนแบบ Cryptographic

```
Renoir#show ip ospf interface Ethernet1
Ethernet1 is up, line protocol is up
  Internet Address 192.168.32.4/24, Area 78
  Process ID 1, Router ID 192.168.30.70, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.30.254, Interface address 192.168.32.2
  Backup Designated router (ID) 192.168.30.80, Interface address 192.168.32.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 5, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.30.80  (Backup Designated Router)
    Adjacent with neighbor 192.168.30.254  (Designated Router)
  Message digest authentication enabled
    Youngest key id is 10
```

ภาพที่ 3.6 เราท์เตอร์สามารมองเห็นเพื่อนบ้านได้ 5 เครื่องแต่ถูกจัดรูปแบบการอยู่ติดกันด้วย DR และ BDR

ในภาพที่ 3.7 แสดงให้เห็นถึงอินเทอร์เฟสที่ถูกเชื่อมต่อกับเครือข่าย NBMA สังเกตว่าค่า Default ของ HelloInterval เท่ากับ 30 วินาที และค่า Default ของ RouterDeadInterval เท่ากับ 4 เท่าของ HelloInterval

```
Renoir#show ip ospf interface Serial3
Serial3 is up, line protocol is up
  Internet Address 192.168.16.41/30, Area 0
  Process ID 1, Router ID 192.168.30.105, Network Type NON_BROADCAST, Cost: 64
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 192.168.30.210, Interface address 192.168.16.42
  Backup Designated router (ID) 192.168.30.105, Interface address 192.168.16.41
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.30.210  (Designated Router)
```

ภาพที่ 3.7 แสดงให้เห็นว่าอินเทอร์เฟสนี้ถูกต่อถูกกับเครือข่ายเฟรมรีเลย์ NBMA และทำหน้าที่เป็น BDR บนเครือข่ายนี้

3.5.2 The Interface State Machine

อินเทอร์เฟสที่ใช้ OSPF จะผ่านสถานะหลายอย่างก่อนที่อินเทอร์เฟสนั้นจะทำงานได้อย่างเต็มที่ สถานะเหล่านั้นได้แก่ การลง (Down) การเชื่อมต่อจุดต่อจุด (Point-to-Point) การรอคอย (Waiting) DR การสำรอง (Backup) Drother และ Loopback

Down : เป็นสถานะเริ่มต้นของอินเทอร์เฟส ซึ่งเป็นสถานะที่อินเทอร์เฟสไม่สามารถทำงานได้และไม่มีทราฟฟิกถูกส่งหรือรับผ่านอินเทอร์เฟส

Point-to-Point : สถานะนี้เหมาะสมกับอินเทอร์เฟสที่เชื่อมต่อกับเครือข่ายแบบจุดต่อจุด จุดต่อหลายจุด และการเชื่อมโยงเสมือน เท่านั้น เมื่ออินเทอร์เฟสเข้าสู่สถานะนี้ มันจะเริ่มต้นส่งแพ็กเก็ต Hello ไปยังทุก ๆ ช่วงเวลา HelloInterval และจะพยายามสร้างการอยู่ติดกันกับเพื่อนบ้านที่ปลายทางของการเชื่อมโยง

Waiting : สถานะนี้เหมาะสมกับอินเทอร์เฟสที่เชื่อมต่อกับเครือข่ายแบบ broadcast และ NBMA เท่านั้น เมื่ออินเทอร์เฟสเข้าสู่สถานะนี้ มันจะเริ่มส่งและรับแพ็กเก็ต Hello และเซ็ทค่า wait timer เราท์เตอร์จะพยายามระบุ DR และ BDR ของเครือข่ายขณะที่อยู่ในสถานะนี้

DR : ในสถานะนี้ เราท์เตอร์ที่เป็น DR จะสร้างการอยู่ติดกันกับเราท์เตอร์ตัวอื่น ๆ ที่อยู่บนเครือข่ายแบบเข้าถึงได้หลายช่องทาง

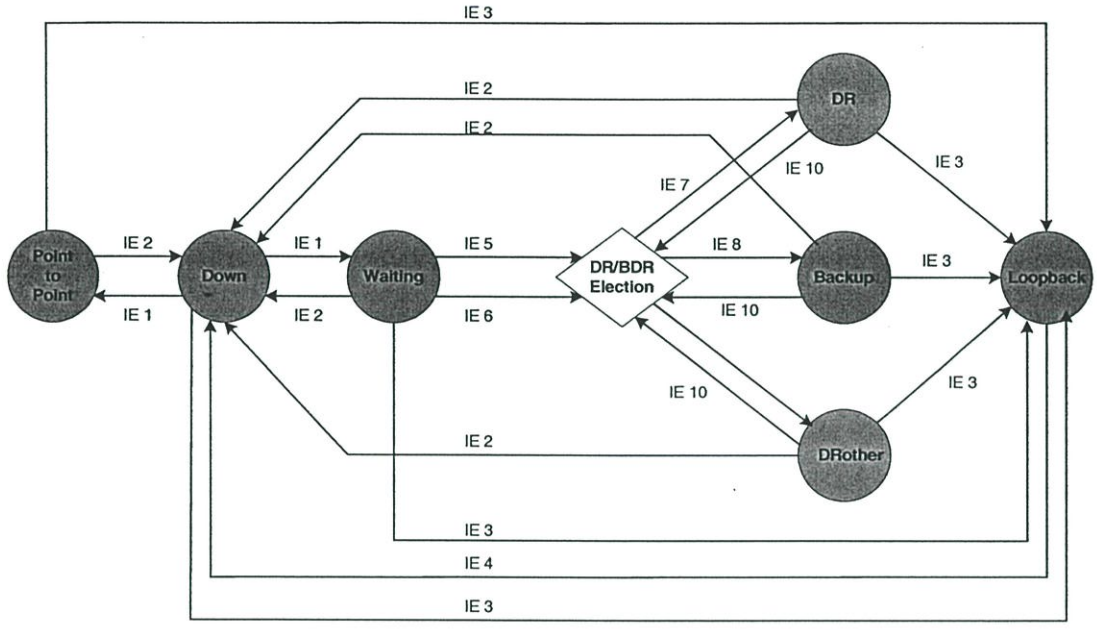
Backup : ในสถานะนี้ เราท์เตอร์ที่เป็น BDR จะสร้างการอยู่ติดกันกับเราท์เตอร์ตัวอื่น ๆ ที่อยู่บนเครือข่ายแบบเข้าถึงได้หลายช่องทาง

DRother : ในสถานะนี้ เราท์เตอร์ที่ไม่ใช่ทั้ง DR และ BDR จะสร้างการอยู่ติดกันกับ DR และ BDR เท่านั้น

Loopback : ในสถานะนี้ อินเทอร์เฟสได้ถูกลูปกลับโดยผ่านทาง software หรือ hardware ถึงแม้ว่าแพ็กเก็ตไม่สามารถส่งผ่านด้วยอินเทอร์เฟสนี้ ค่าแอดเดรสของอินเทอร์เฟสก็ยัง

คงถูกประกาศไปใน LSAs เราท์เตอร์ได้ เพื่อที่ว่าแพ็กเก็ต Test สามารถค้นหาเส้นทางของพวกมันเองได้

จากภาพที่ 3.8 แสดงให้เห็นถึงสถานะอินเทอร์เฟส OSPF และเหตุการณ์ด้านอินพุทที่จะเกิดจากการส่งผ่านในแต่ละขั้นตอน เหตุการณ์ด้านอินพุทได้ถูกอธิบายไว้ในตารางที่ 3.1



ภาพที่ 3.8 กลไกของ OSPF interface state machine

3.6 OSPF Neighbors

ในหัวข้อนี้อธิบายนี้ถึงความสัมพันธ์ของเราท์เตอร์กับเพื่อนบ้านที่อยู่บนเครือข่าย จุดประสงค์สุดท้ายของความสัมพันธ์ของเพื่อนบ้านคือการสร้างการอยู่ติดกันด้วยข้อมูลเส้นทาง (Routing Information) การอยู่ติดกันได้ถูกสร้างขึ้นโดยผ่านขั้นตอนทั่วไป 4 อย่าง คือ

1. การค้นพบเพื่อนบ้าน
2. การสื่อสารแบบ 2 ทิศทาง : การสื่อสารนี้สำเร็จลงได้ต่อเมื่อเพื่อนบ้าน 2 ตัวลงรายชื่อ Router ID ซึ่งกันและกันลงในแพ็กเก็ต Hello ของพวกมัน
3. การจัดทำฐานข้อมูลให้ตรงกัน : รายละเอียดของฐานข้อมูล การร้องขอสถานะการเชื่อมโยง และแพ็กเก็ตที่อัฟเดตสถานะการเชื่อมโยง ได้ถูกแลกเปลี่ยนกันเพื่อให้แน่ใจว่าเพื่อนบ้านทั้งคู่มีข้อมูลเหมือนกัน จุดประสงค์สำหรับกระบวนการนี้คือ เพื่อให้เพื่อนบ้านตัวหนึ่งเป็น master และอีกตัวเป็น slave ซึ่งตัว master จะทำหน้าที่ควบคุมการแลกเปลี่ยนแพ็กเก็ตที่เกี่ยวกับรายละเอียดของฐานข้อมูล
4. การอยู่ติดกันอย่างสมบูรณ์

ตารางที่ 3.1 เหตุการณ์อินพุทสำหรับกลไกที่บ่งบอกถึงสถานะของอินเทอร์เฟส

เหตุการณ์อินพุท	รายละเอียด
IE 1	โพรโทคอลระดับล่างบ่งบอกว่าอินเทอร์เฟสของเครือข่ายมีการทำงาน
IE 2	โพรโทคอลระดับล่างบ่งบอกว่าอินเทอร์เฟสของเครือข่ายไม่มีการทำงาน
IE 3	ตัวจัดการเครือข่าย หรือโพรโทคอลระดับล่างบ่งบอกว่าอินเทอร์เฟสมีการลูปเกิดขึ้น
IE 4	ตัวจัดการเครือข่าย หรือโพรโทคอลระดับล่างบ่งบอกว่าอินเทอร์เฟสไม่มีการลูป
IE 5	ได้รับแพ็กเก็ต Hello ในกรณีที่เพื่อนบ้านตัวต้นกำเนิดแสดงรายชื่อของตัวเองเป็น BDR หรือไม่ก็ได้รับแพ็กเก็ต Hello ในกรณีที่เพื่อนบ้านตัวต้นกำเนิดแสดงรายชื่อของตัวเองเป็น DR และบ่งบอกว่าไม่มี BDR
IE 6	เวลาในการคอย (wait timer) สิ้นสุดลง
IE 7	เราท์เตอร์ถูกเลือกเป็น DR สำหรับเครือข่ายนี้
IE 8	เราท์เตอร์ถูกเลือกเป็น BDR สำหรับเครือข่ายนี้
IE 9	เราท์เตอร์ไม่ถูกเลือกให้เป็น DR หรือ BDR สำหรับเครือข่ายนี้
IE 10	การเปลี่ยนแปลงเกิดขึ้นกับกลุ่มเพื่อนบ้านบนเครือข่ายนี้ การเปลี่ยนแปลงนี้อาจเกิดได้จาก มีการสร้างการสื่อสาร 2 ทางกับเพื่อนบ้าน สูญเสียการสื่อสาร 2 ทางกับเพื่อนบ้าน ได้รับ Hello ในกรณีที่เพื่อนบ้านตัวต้นกำเนิดแสดงรายชื่อรายใหม่ของตัวเองเป็น DR หรือ BDR ได้รับ Hello จาก DR ในกรณีที่เราท์เตอร์ถูกแสดงรายชื่อว่าสูญหาย ได้รับ Hello จาก BDR ในกรณีที่เราท์เตอร์ถูกแสดงรายชื่อว่าสูญหาย การสิ้นสุดของ RouterDeadInterval โดยไม่ได้รับ Hello จาก DR หรือ BDR หรือทั้งคู่

ตามที่ได้อธิบายไว้ก่อนหน้านี้ว่า ความสัมพันธ์ของเพื่อนบ้านได้ถูกสร้างขึ้นและถูกรักษาไว้โดยการแลกเปลี่ยนแพ็กเก็ต Hello บนเครือข่ายแบบ broadcast และ point-to-point แพ็กเก็ต Helloใช้การ multicast ไปยังเราท์เตอร์ทุกตัว (224.0.0.5) บนเครือข่ายแบบ NBMA point-to-multipoint และ virtual link แพ็กเก็ต Hello ใช้การ unicast ไปยังเพื่อนบ้านเป็นราย ๆ ไป ความ

สัมพันธ์ของการ unicast คือเราท์เตอร์ต้องมีการเรียนรู้ความเป็นอยู่ของเพื่อนบ้านของตัวเองก่อน โดยวิธีการคอนฟิกด้วยมือ หรือด้วยกลไก เช่น Inverse ARP

3.6.1 Neighbor State Machine

เราท์เตอร์ OSPF จะมีการส่งมอบเพื่อนบ้านผ่านกระบวนต่าง ๆ ก่อนที่เพื่อนบ้านจะถูกพิจารณาให้เป็นการอยู่ติดกันอย่างสมบูรณ์

Down : สถานะเริ่มต้นของการสนทนากันของเพื่อนบ้านซึ่งชี้ว่า ไม่มี Hello ได้ยินเพื่อนบ้านในช่วงเวลา RouterDeadInterval ครั้งสุดท้าย Hello จะไม่ถูกส่งไปยังเพื่อนบ้านที่ down ยกเว้นว่าเพื่อนบ้านเหล่านั้นอยู่บนเครือข่าย NBMA ซึ่งในกรณีนี้ Hello จะถูกส่งทุก ๆ PollInterval ถ้าเพื่อนบ้านมีการส่งผ่านไปถึงสถานะที่ down จากสถานะที่สูงกว่า รายการของการส่งสถานะการเชื่อมโยงซ้ำ รายการผลรวมของฐานข้อมูล และรายการร้องขอสถานะการเชื่อมโยงจะถูกลบทิ้ง

Attempt : สถานะนี้ใช้กับเพื่อนบ้านที่อยู่บนเครือข่าย NBMA เท่านั้น โดยที่เพื่อนบ้านถูกคอนฟิกด้วยมือ เราท์เตอร์ซึ่งได้รับเลือกเป็น DR จะส่งผ่านเพื่อนบ้านไปยังสถานะ Attempt เมื่ออินเทอร์เฟสกับเพื่อนบ้านครั้งแรกแล้วแอกทีฟ หรือเมื่อเราท์เตอร์เป็น DR หรือ BDR เราท์เตอร์จะส่งแพ็กเก็ตไปยังเพื่อนบ้านในสถานะ Attempt ที่เวลา HelloInterval

Init : สถานะนี้ชี้ว่าแพ็กเก็ต Hello ได้ถูกมองเห็นจากเพื่อนบ้านในช่วง RouterDeadInterval สุดท้าย แต่การสื่อสาร 2 ทางยังไม่ได้ถูกสร้างขึ้น เราท์เตอร์จะรวมเอา Router ID ของเพื่อนบ้านทั้งหมดเข้าไปในสถานะนี้หรือสูงกว่าสถานะนี้เข้าไปในฟิลด์เพื่อนบ้านของแพ็กเก็ต Hello

2-Way : สถานะนี้แสดงให้เห็นว่าเราท์เตอร์ได้เห็น Router ID ของตัวมันเองในฟิลด์เพื่อนบ้านของแพ็กเก็ต Hello ที่มาจากเพื่อนบ้าน ซึ่งหมายความว่าการสนทนา 2 ทิศทางได้ถูกสร้างขึ้นแล้ว บนเครือข่ายแบบเข้าถึงได้ปลายช่องทาง เพื่อนบ้านต้องอยู่ในสถานะนี้หรือสูงหว่านี้เพื่อมีสิทธิเข้ารับเลือกเป็น DR หรือ BDR การต้อนรับแพ็กเก็ตที่บอกถึงรายละเอียดของฐานข้อมูลจากเพื่อนบ้านในสถานะ Init จะทำให้เกิดการส่งผ่านแบบ 2 ทางด้วย

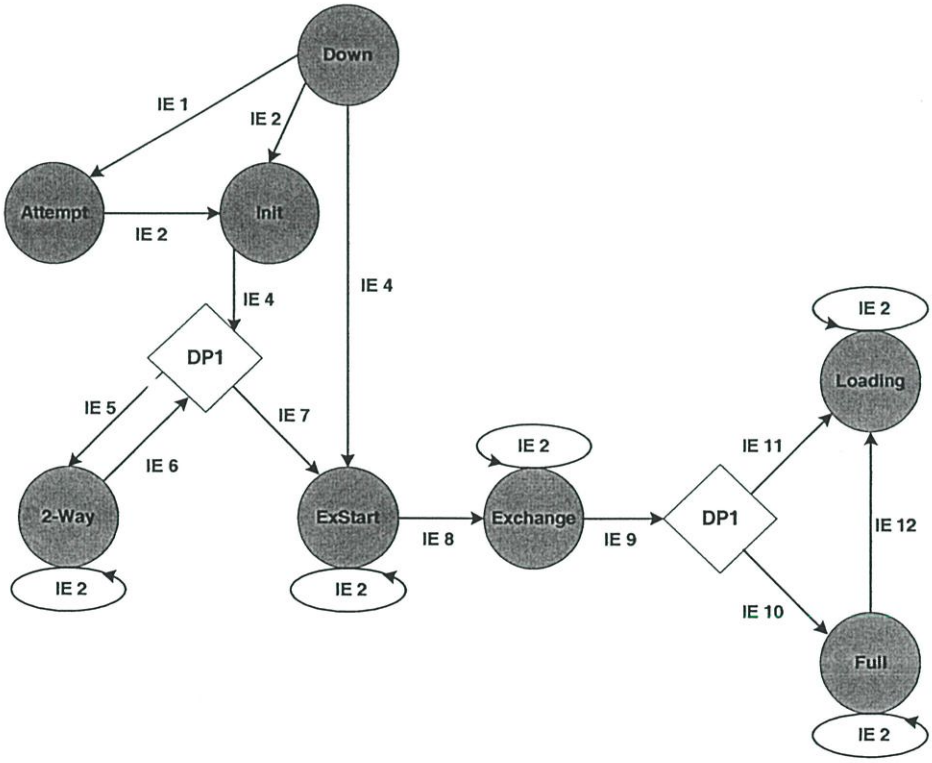
ExStart : ในสถานะนี้ เราท์เตอร์และเพื่อนบ้านของมันสร้างความสัมพันธ์กับ master/slave และกำหนดลำดับเลขหมาย DD เริ่มต้น ในการเตรียมการสำหรับการแลกเปลี่ยนแพ็กเก็ตที่บอกถึงรายละเอียดของฐานข้อมูล เพื่อนบ้านที่มีแอดเดรสอินเทอร์เฟสสูงที่สุดจะได้เป็น master

Exchange : เราท์เตอร์ส่งแพ็กเก็ตที่บอกถึงรายละเอียดของฐานข้อมูลที่อธิบายถึงฐานข้อมูลของสถานะการเชื่อมโยงทั้งหมดของตัวเองแกเพื่อนบ้านที่อยู่ในสถานะ Exchange เราท์เตอร์สามารถส่งแพ็กเก็ตการร้องขอสถานะการเชื่อมโยง (การร้องขอ LSAs เพิ่ม) แก่เพื่อนบ้านในสถานะนี้ได้ด้วย

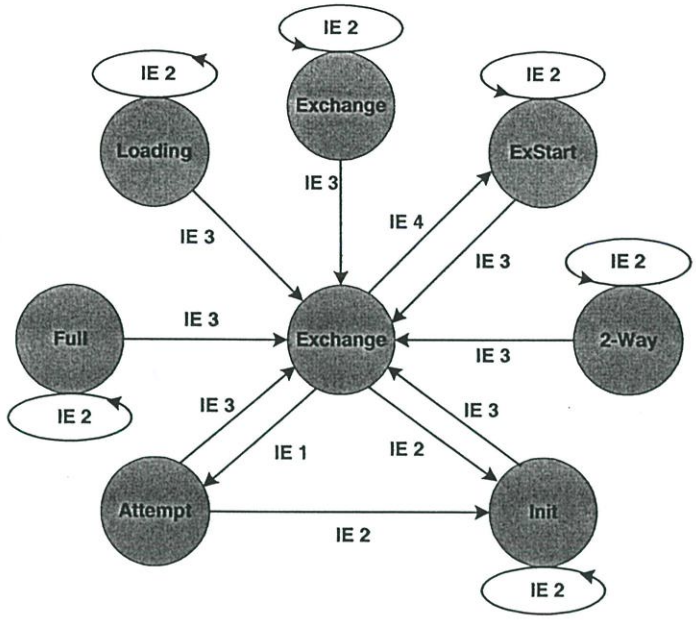
Loading : เราท์เตอร์จะส่งแพ็กเก็ตการร้องขอสถานะการเชื่อมโยงแก่เพื่อนบ้านที่อยู่ในสถานะ Loading การร้องขอ LSAs เพิ่มที่ได้ถูกค้นพบในสถานะ Exchange แต่ยังไม่ได้รับ

Full : เพื่อนบ้านในสถานะนี้คือการอยู่ติดกันอย่างสมบูรณ์ และการอยู่ติดกันจะปรากฏอยู่ใน Router LSAs และ Network LSAs

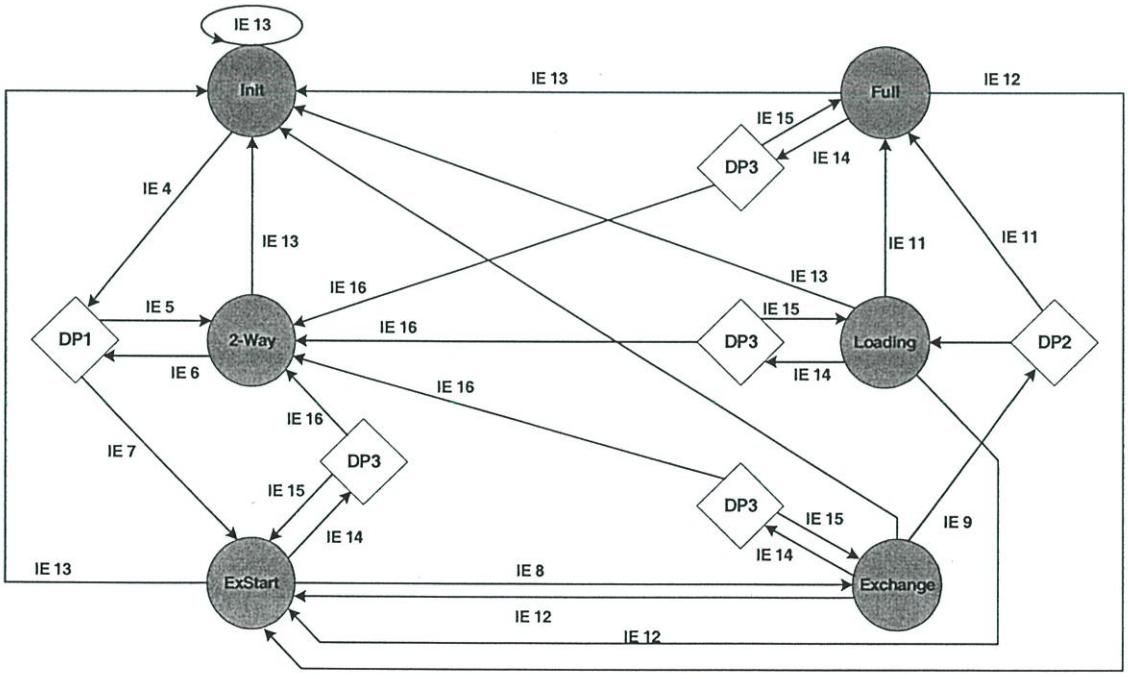
ในภาพที่ 3.10 ถึง 3.12 แสดงถึงสถานะเพื่อนบ้าน OSPF และเหตุการณ์ของอินพุทที่จะทำให้เกิดสถานะการส่งผ่าน เหตุการณ์ของอินพุทได้ถูกอธิบายไว้ในตารางที่ 3.2 และจุดในการตัดสินใจได้ถูกกำหนดในตารางที่ 3.3 ภาพที่ 3.10 แสดงขบวนการแบบปกติจากสถานะการทำงานที่น้อยที่สุดไปยังสถานะที่สมบูรณ์แบบ ภาพที่ 3.11 และ 3.12 แสดงกลไกของสถานะเพื่อนบ้าน OSPF ที่สมบูรณ์



ภาพที่ 3.10 กลไก OSPF ในการมองหาเพื่อนบ้านจากสภาวะ Down เป็น Full



ภาพที่ 3.11 กลไกในการจัดหาเพื่อนบ้านจากสภาวะ Down เป็น Init



ภาพที่ 3.12 กลไกจัดหาเพื่อนบ้านจากสภาวะ Init เป็น Full

ตารางที่ 3.2 เหตุการณ์ที่เกิดขึ้นในภาพที่ 3.10 3.11 และ 3.12

เหตุการณ์อินพุท	รายละเอียด
IE 1	เหตุการณ์นี้เกิดขึ้นกับเพื่อนบ้านที่เชื่อมต่อแบบ NBMA เท่านั้น เหตุการณ์อินพุทจะถูกทริกภายใต้เงื่อนไข ดังนี้ (1) อินเทอร์เฟสที่ต่อกับเครือข่าย NBMA เป็น active และเพื่อนบ้านมีสิทธิเหมาะสมกับการเข้ารับเลือกเป็น DR (2) เราท์เตอร์กลายเป็น DR หรือ BDR และเพื่อนบ้านไม่เหมาะสมที่จะได้รับการคัดเลือกเป็น DR
IE 2	ได้รับแพ็กเก็ต Hello จากเพื่อนบ้าน
IE 3	เพื่อนบ้านไม่สามารถมาถึงได้ตามที่กำหนดไว้โดยโพรโทคอลระดับล่าง โดยคำแนะนำที่แน่นอนจากกระบวนการ OSPF ในตัวเอง หรือโดยการสิ้นสุดของเวลา
IE 4	เราท์เตอร์ตัวแรกพบ Router ID ของตัวมันเองในรายชื่อที่อยู่ในฟิลด์ Neighbor ของแพ็กเก็ต Hello ของเพื่อนบ้าน หรือได้รับแพ็กเก็ต Database Description จากเพื่อนบ้าน
IE 5	เพื่อนบ้านจะไม่กลายเป็นการอยู่ติดกัน
IE 6	เหตุการณ์อินพุทเกิดขึ้นภายใต้เงื่อนไข ดังนี้ (1) สถานะเพื่อนบ้านตัวแรกส่งมอบเป็น 2 ทาง (2) สถานะอินเทอร์เฟสเปลี่ยนแปลง
IE 7	การอยู่ติดกันควรจะถูกจัดอยู่ในรูปเพื่อนบ้าน
IE 8	ความสัมพันธ์ master/slave ได้ถูกสร้างขึ้น และแลกเปลี่ยนหมายเลขลำดับ DD ระหว่างกัน
IE 9	การแลกเปลี่ยนแพ็กเก็ต Database Description เสร็จสมบูรณ์
IE 10	แพ็กเก็ต Database Description ปรากฏอยู่ในรายชื่อของ Link State Request
IE 11	รายชื่อของ Link State Request ว่างเปล่า
IE 12	การอยู่ติดกันควรจะถูกทำลายและเริ่มต้นใหม่ เหตุการณ์อินพุทอาจจะถูกทริกโดยสิ่งต่าง ๆ ดังนี้ (1) การได้รับแพ็กเก็ต Database Description ด้วยหมายเลขลำดับ DD ที่ไม่ได้คาดหวังไว้ (2) การได้รับแพ็กเก็ต Database Description ด้วยฟิลด์ option ที่เซ็ทไว้แตกต่างกว่าฟิลด์ option ของแพ็กเก็ต DD สุดท้าย

	(3) การได้รับแพ็กเก็ต Database Description ในกรณีที่บิท Init ถูกเซ็ท (4) การได้รับแพ็กเก็ต Link State Request สำหรับ LSA ที่ไม่อยู่ในฐานข้อมูล
IE 13	แพ็กเก็ต Hello ถูกรับมาจากเพื่อนบ้าน ซึ่ง Router ID ของเราท์เตอร์ด้านรับข้อมูลไม่ถูกเก็บรายชื่อในฟิลด์เพื่อนบ้าน
IE 14	เหตุการณ์นี้เกิดขึ้นเมื่อสถานะอินเทอร์เฟสเปลี่ยน
IE 15	การปรากฏหรือการประกอบการอยู่ติดกันด้วยเพื่อนบ้าน จะดำเนินต่อไป
IE 16	การปรากฏหรือการประกอบการอยู่ติดกันด้วยเพื่อน จะไม่ดำเนินต่อไป

ตารางที่ 3.3 จุดตัดสินใจสำหรับภาพที่ 3.10 และ 3.12

การตัดสินใจ	รายละเอียด
DP1	การอยู่ติดกันควรจะถูกสร้างด้วยเพื่อนบ้านหรือไม่ การอยู่ติดกันควรจะถูกประกอบขึ้นถ้าเงื่อนไขข้อใดข้อหนึ่งเป็นจริง ดังนี้ (1) ชนิดเครือข่ายเป็นแบบจุดต่อจุด (2) ชนิดเครือข่ายเป็นแบบจุดต่อหลายจุด (3) ชนิดเครือข่ายเป็นแบบการเชื่อมโยงเสมือน (4) เราท์เตอร์เป็น DR ของเครือข่ายที่ซึ่งเพื่อนบ้านตั้งอยู่ (5) เราท์เตอร์เป็น BDR ของเครือข่ายที่ซึ่งเพื่อนบ้านตั้งอยู่ (6) เพื่อนบ้านคือ DR (7) เพื่อนบ้านคือ BDR
DP2	รายชื่อ Link State Request ของเพื่อนบ้านนี้ว่างเปล่ากรือไม่
DP3	การปรากฏหรือการประกอบการอยู่ติดกันกับเพื่อนบ้านควรดำเนินต่อไปหรือไม่

3.7 การสร้างการอยู่ติดกัน (Building an Adjacency)

เพื่อนบ้านที่อยู่บนเครือข่ายแบบจุดต่อจุด จุดต่อหลายจุด และการเชื่อมโยงเสมือนจะกลายเป็นเพื่อนบ้านกันเสมอ ยกเว้นว่าค่าพารามิเตอร์ของ Hello ไม่ตรงกัน บนเครือข่ายแบบ broadcast และ NBMA DR และ BDR จะกลายเป็นการอยู่ติดกันกับเพื่อนบ้านทั้งหมด แต่การอยู่ติดกันจะไม่มีอยู่ระหว่าง Drothers ด้วยกัน

กระบวนการสร้างการอยู่ติดกันใช้แพ็กเก็ต OSPF อยู่ 3 ชนิด ดังนี้

1. แพ็กเก็ต Database Description (Type 2)
2. แพ็กเก็ต Link State Request (Type 3)
3. แพ็กเก็ต Link State Update (Type 4)

แพ็กเก็ต Database Description มีความสำคัญอย่างยิ่งต่อกระบวนการสร้างการอยู่ติดกัน แพ็กเก็ตนี้ทำหน้าที่นำพารายละเอียดผลสรุปของ LSA แต่ละตัวเข้าไปในฐานข้อมูลสถานะการเชื่อมโยงของเราท์เตอร์ตัวกำเนิด รายละเอียดเหล่านี้ไม่ใช่ LSAs ที่สมบูรณ์ แต่เป็นข้อมูลที่เพียงพอสำหรับเราท์เตอร์ด้านรับเพื่อตัดสินใจว่ามันมีสำเนาล่าสุดของ LSA อยู่ในฐานข้อมูลของตัวมันเองหรือไม่ นอกจากนี้ แฟลก (Flag) 3 ตัวในแพ็กเก็ต DD ถูกใช้สำหรับจัการกระบวนการสร้างการอยู่ติดกัน ดังนี้

1. บิท I หรือบิทเริ่มแรก (Initial bit) เมื่อถูกเซ็ทจะชี้ให้เห็นว่า แพ็กเก็ต DD แพ็กเก็ตแรกได้ส่งออกไป
2. บิท M หรือบิท More ซึ่งเมื่อถูกเซ็ท จะชี้ให้เห็นว่าแพ็กเก็ต DD ไม่ใช่แพ็กเก็ตสุดท้ายที่ส่งออกไป
3. บิท MS หรือบิท Master/Slave ซึ่งถูกเซ็ทในแพ็กเก็ต DD ที่เกิดจาก master

เมื่อการเจรจาของ master/slave เริ่มขึ้นในสถานะ ExStart เพื่อนบ้านทั้งคู่จะเรียกร้องสิทธิเพื่อเป็น master โดยการส่งแพ็กเก็ต DD ที่ว่างเปล่าด้วยบิท MS ที่เซ็ทเป็น 1 หมายเลขลำดับของ DD ใน 2 แพ็กเก็ตนี้จะถูกเซ็ทตามความคิดของเราท์เตอร์ด้านต้นกำเนิดตามที่มันควรจะเป็น เพื่อนบ้านที่มี Router ID ต่ำที่สุดจะกลายเป็น slave และจะตอบกลับด้วยแพ็กเก็ต DD ที่มีบิท MS เป็น 0 และมีหมายเลขลำดับ DD ที่ถูกเซ็ทตามหมายเลขลำดับของ master แพ็กเก็ต DD นี้จะเป็นแพ็กเก็ตแรกที่อาศัยอยู่กับผลรวมของ LSA เมื่อการเจรจาของ master/slave เสร็จสิ้น สถานะเพื่อนบ้านจะส่งต่อไปยัง Exchange

ในสถานะ Exchange เพื่อนบ้านจะทำให้ฐานข้อมูลสถานะการเชื่อมโยงสอดคล้องกันโดยการพิจารณาค่าที่มีอยู่ทั้งหมดในฐานข้อมูลสถานะการเชื่อมโยงโดยลำดับ รายการผลรวมของฐานข้อมูลได้ถูกรวมกับ Header ของ LSAs ทั้งหมดที่มีอยู่ในฐานข้อมูลของเราท์เตอร์ แพ็กเก็ตรายละเอียดของฐานข้อมูลที่บรรจุอยู่ใน Header ของ LSA ที่ถูกขึ้นรายการไว้จะถูกส่งไปยังเพื่อนบ้าน

ถ้าเราท์เตอร์เห็นว่าเพื่อนบ้านของมันมี LSA ที่ไม่ได้อยู่ในฐานข้อมูลของตัวเอง หรือไม่ก็เพื่อนบ้านมีสำเนาของ LSA ที่รู้จักก่อนหน้านี้ เราท์เตอร์จะจัดวาง LSA เข้าไปในรายการร้องขอสถานะการเชื่อมโยง หลังจากนั้นเราท์เตอร์ส่งแพ็กเก็ตร้องขอสถานะการเชื่อมโยงเพื่อขอสำเนา LSA ที่สมบูรณ์ แพ็กเก็ต update สถานะการเชื่อมโยงก็จะพา LSA ที่ถูกร้องขอมาให้ ขณะที่ได้รับ LSA ที่ถูกร้องขอ พวกมันจะถูกลบออกจากรายการร้องขอสถานะการเชื่อมโยง

LSAs ทั้งหมดที่ส่งไปในแพ็กเก็ต update ต้องถูกรับรอง (acknowledge) เป็นรายตัว เพราะฉะนั้น LSA ที่ถูกส่งออกไปซึ่งได้เข้าไปอยู่ในรายการการส่งสถานะการเชื่อมโยงซ้ำ เมื่อ LSA ถูกรับรองก็จะถูกลบออกจากรายการ LSA อาจจะถูกรับรองได้ด้วย 1 ใน 2 วิธี ดังนี้

- Explicit Acknowledgment : ได้รับแพ็กเก็ตการรับรองสถานะการเชื่อมโยงที่บรรจุ LSA header
- Implicit Acknowledgment : ได้รับแพ็กเก็ต update ที่บรรจุตัวอย่างเดียวกันกับ LSA

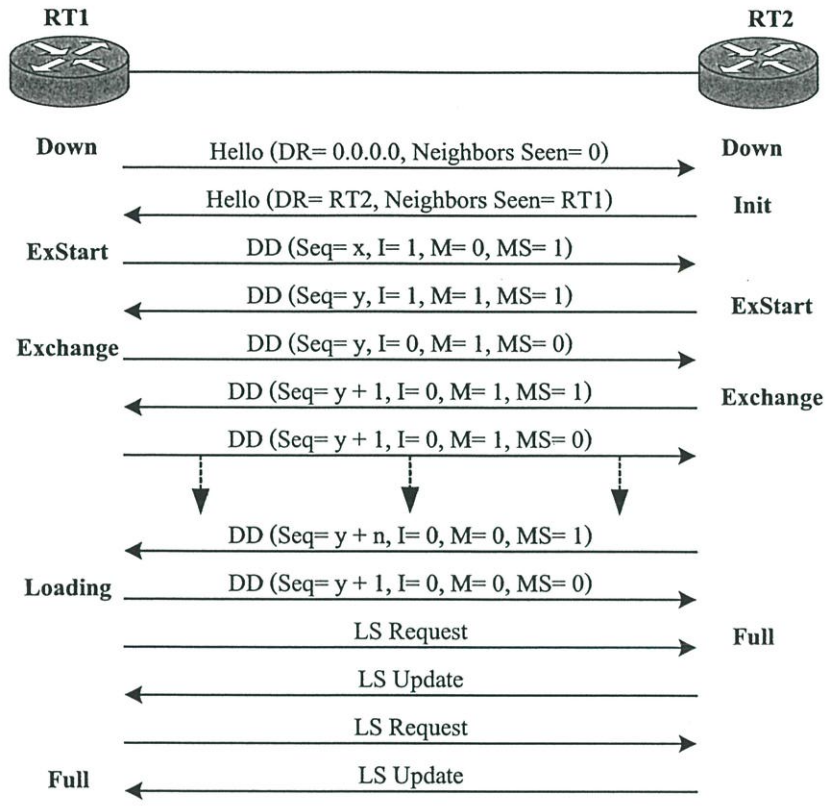
Master ทำหน้าที่ควบคุมกระบวนการที่ทำให้เกิดความสอดคล้องกัน และรับรองว่ามีแพ็กเก็ต DD เพียงแพ็กเก็ตเดียวที่สำคัญในช่วงเวลาหนึ่ง เมื่อ Slave ได้รับแพ็กเก็ต DD จาก Master Slave จะทำการรับรองแพ็กเก็ตนั้นโดยการส่งแพ็กเก็ต DD ที่มีหมายเลขลำดับเดียวกัน ถ้า Master ไม่ได้รับการรับรองของแพ็กเก็ต DD ภายในช่วง RxmtInterval Master จะส่งสำเนาของแพ็กเก็ตใหม่ออกไป

Slave จะทำการส่งแพ็กเก็ต DD เท่านั้นในการตอบสนองกับแพ็กเก็ต DD ที่ได้รับจาก Master ถ้าแพ็กเก็ตที่ได้รับมีหมายเลขลำดับใหม่ Slave จะส่งแพ็กเก็ต DD ด้วยหมายเลขลำดับเดียวกัน ถ้าหากว่าหมายเลขลำดับที่ได้รับเหมือนกันกับแพ็กเก็ต DD ที่ได้รับรองไปก่อนหน้านี้ แพ็กเก็ตการรับรองก็จะถูกส่งออกไปใหม่

เมื่อกระบวนการที่ทำให้ฐานข้อมูลมีความสอดคล้องกันเสร็จสมบูรณ์ สถานะการส่งมอบอย่างใดอย่างหนึ่งนี้ก็จะเกิดขึ้น ดังนี้

- ถ้ายังคงมีรายการร้องขอสถานะการเชื่อมโยงอยู่ทั้งหมด เราท์เตอร์จะทำการส่งมอบจากสถานะเพื่อนบ้านไปเป็น Loading
- ถ้ารายการร้องขอสถานะการเชื่อมโยงว่างเปล่า เราท์เตอร์จะส่งผ่านจากสถานะเพื่อนบ้านไปเป็น Full

เมื่อ Master รู้ว่ากระบวนการทำให้เกิดความสอดคล้องเสร็จสมบูรณ์ Master จะทำการส่งแพ็กเก็ต DD ทั้งหมดแก่ฐานข้อมูลสถานะการเชื่อมโยงของตัวเอง และรับแพ็กเก็ต DD ที่มีบิท M เป็นศูนย์ และ Slave จะรู้ว่ากระบวนการเสร็จสมบูรณ์เมื่อ Slave ได้รับแพ็กเก็ต DD ที่มีบิท M เป็นศูนย์ และส่งแพ็กเก็ต DD รับรองซึ่งมีบิท M ศูนย์ด้วย Slave จะต้องรู้เป็นคนแรกว่ากระบวนการที่ทำให้เกิดความสอดคล้องเสร็จสมบูรณ์ เพราะว่า Slave ต้องรับรองแพ็กเก็ตที่ได้รับในแต่ละแพ็กเก็ตในภาพที่ 3.13 แสดงถึงกระบวนการสร้างการอยู่ติดกัน ตัวอย่างนี้ถูกนำมาจาก RFC 2328



ภาพที่ 3.13 กระบวนการซิงโครไนซ์ฐานข้อมูล Link State และสถานะของเพื่อนบ้าน

ขั้นตอนที่แสดงในภาพที่ 3.13 สามารถอธิบายได้ ดังนี้

1. เมื่อ RT1 เริ่มแอกทีฟบนเครือข่ายที่มีการถึงเข้าได้หลายช่องทางและส่งแพ็กเก็ต Hello RT1 จะยังไม่ได้ยินอะไรเลยจากเพื่อนบ้านตัวใด ๆ ดังนั้นแพ็กเก็ตในฟิลด์เพื่อนบ้านจะว่างเปล่า และฟิลด์ DR และ BDR ถูกเซ็ทเป็น 0.0.0.0

2. เมื่อ RT2 ได้รับ Hello จาก RT1 RT2 จะสร้างโครงสร้างข้อมูลของเพื่อนบ้านสำหรับ RT1 และเซ็ทสถานะของ RT1 เป็น Init RT2 จะส่งแพ็กเก็ต Hello ด้วย Router ID ของ RT1 ไปในฟิลด์เพื่อนบ้านในฐานะที่เป็น DR RT2 ยังรวมแอดเดรสอินเทอร์เฟสของตัวมันเองเข้าไปในฟิลด์ DR ด้วย

3. การมองเห็น Router ID ของตัวมันเองในแพ็กเก็ต Hello ที่ได้รับ (IE4 ในตารางที่ 9.2) RT1 ได้สร้างโครงสร้างข้อมูลเพื่อนบ้านสำหรับ RT2 และเซ็ทสถานะ RT2 เป็น ExStart เพื่อการเจรจา mater/slave จากนั้น RT1 จะสร้างแพ็กเก็ตรายละเอียดของฐานข้อมูลที่ว่างเปล่า (ไม่มีผลรวม LSA) หมายเลขลำดับ DD ถูกเซ็ทเป็น x บิท I ถูกเซ็ทขึ้นเพื่อชี้ว่าแพ็กเก็ตนี้เป็นแพ็กเก็ต DD เริ่มแรกของ RT1 บิท M ถูกเซ็ทขึ้นเพื่อชี้ว่าแพ็กเก็ตนี้ไม่ใช่แพ็กเก็ต DD สุดท้าย และบิท MS ถูกเซ็ทขึ้นเพื่อชี้ว่า RT1 กำลังอ้างสิทธิให้ตัวมันเองเป็น master

4. RT2 ส่งมอบสถานะของ RT1 ด้วย Exstart ในโอกาสที่ได้รับแพ็กเก็ต DD จากนั้นมันจึงส่งแพ็กเก็ต DD ตอบสนองด้วยหมายเลขลำดับ DD ด้วย y ซึ่ง RT2 มี Router ID สูงกว่า RT1 ดังนั้น RT2 จึงเซ็ทบิท MS เป็น 1 แพ็กเก็ต DD นี้เหมือนกับแพ็กเก็ต DD แรกที่ถูกใช้สำหรับการเจรจา master/slave ด้วยเหตุนี้มันจึงว่าง

5. เมื่อตกลงได้ว่า RT2 เป็น master RT1 จึงส่งมอบสถานะของ RT2 ด้วย Exchange RT1 จะสร้างแพ็กเก็ต DD ด้วยหมายเลขลำดับ DD ของ RT2 เป็น y และ MS = 0 ซึ่งเป็นการชี้ว่า RT1 เป็น slave แพ็กเก็ตนี้จะถูกอาศัยอยู่กับ LSA header จากรายการสรุปสถานะการเชื่อมโยงของ RT1

6. RT2 ส่งมอบสถานะเพื่อนบ้านของมันด้วย Exchange ที่ระบุว่าได้รับแพ็กเก็ต DD ของ RT1 RT2 จะส่งแพ็กเก็ต DD ที่บรรจุด้วย LSA header จากรายการสรุปสถานะการเชื่อมโยงของตัว RT2 เอง และจะเพิ่มหมายเลขสำดับ DD เป็น y+1

7. RT1 ส่งแพ็กเก็ตรับรองที่บรรจุหมายเลขสำดับเดียวกันตามแพ็กเก็ต DD ที่ เพิ่งได้รับจาก RT2 กระบวนการยังคงดำเนินต่อไป ด้วย RT2 ส่งแพ็กเก็ต DD แพ็กเก็ตเดียวและรอคอยแพ็กเก็ตรับรองจาก RT1 ที่บรรจุหมายเลขลำดับเดียวกันก่อนการส่งแพ็กเก็ตถัดไป เมื่อ RT2 ส่งแพ็กเก็ต DD ด้วยผลรวม LSA ของตัวเองเป็นแพ็กเก็ตสุดท้าย RT2 จะเซ็ท M = 0

8. การรับแพ็กเก็ตนี้และการรับรู้ว่าแพ็กเก็ตการรับรองที่มันจะส่งไปประกอบด้วยผลรวม LSA ของตัวมันเองเป็นผลรวมสุดท้าย RT1 จึงรับรู้ว่ากระบวนการ Exchange เสร็จสิ้นแล้ว อย่างไรก็ตาม RT1มี entires อยู่ในรายการร้องขอสถานะการเชื่อมโยงของตัวมันเอง เพราะฉะนั้น RT1 จะส่งผ่านไปยัง Loading

9. เมื่อ RT2 รับแพ็กเก็ต DD สุดท้ายของ RT1 RT2 จะส่งมอบสถานะของ RT1 เป็น Full เพราะ RT2 ไม่มี entires อยู่ในรายการร้องขอสถานะการเชื่อมโยงของตัวเองอยู่

10. RT1 ส่งแพ็กเก็ตร้องขอสถานะการเชื่อมโยง และ RT2 ส่ง LSA ที่ถูกร้องขอไปในแพ็กเก็ต update สถานะการเชื่อมโยง จนกระทั่งรายการร้องขอการเชื่อมโยงของ RT1 ว่าง RT1 จึงจะส่งมอบสถานะของ RT2 เป็น Full

สังเกตว่าถ้าเราท์เตอร์มี entires อยู่ในรายการร้องขอสถานะการเชื่อมโยง เราท์เตอร์ไม่จำเป็นต้องคอยสถานะ Loading เพื่อส่งแพ็กเก็ตร้องขอสถานะการเชื่อมโยงก็ได้ เราท์เตอร์อาจจะไม่รอคอยในขณะที่เพื่อนบ้านยังคงอยู่ในสถานะ Exchange ผลที่สุดกระบวนการที่ทำให้เกิดความสอดคล้องกันก็จะไม่เรียบร้อยเท่ากับที่แสดงไว้ในภาพที่ 3.13 แต่จะมีประสิทธิภาพมาก

3.8 แอเรีย (Areas)

แอเรียเป็นกลุ่มตรรก (logical) ของเราท์เตอร์ OSPF และการเชื่อมโยง ซึ่งแบ่งโดเมน OSPF ออกเป็นโดเมนย่อย ๆ (sub-domain) ดังภาพที่ 3.14 เราท์เตอร์ในแอเรียหนึ่งจะไม่มีการรับรู้ในรายละเอียดของโทโปโลยีจากภายนอกของแอเรียของพวกมัน เพราะว่าเงื่อนไขเหล่านี้

- เราท์เตอร์ ต้องแบ่งฐานข้อมูลสถานะการเชื่อมโยงเฉพาะกับเราท์เตอร์ตัวอื่นที่อยู่ในแอเรียของมันเองเท่านั้น ไม่ใช่กับเครือข่ายที่เชื่อมต่อกันทั้งหมด ขนาดของฐานข้อมูลที่ลดลงช่วยลดผลกระทบที่จะเกิดขึ้นกับหน่วยความจำของเราท์เตอร์

- ฐานข้อมูลสถานะการเชื่อมโยงที่มีขนาดเล็กหมายความว่า LSA มีขนาดน้อยเพื่อผ่านกรรมวิธีการทำงาน เพราะฉะนั้นผลกระทบต่อ CPU จึงน้อย

- เพราะว่าฐานข้อมูลสถานะการเชื่อมโยงต้องถูกรักษาอยู่ภายในแอเรียเท่านั้น การแพร่กระจาย (flooding) โดยส่วนใหญ่จึงถูกจำกัดอยู่ในแอเรีย

แอเรียได้ถูกแบ่งแยกด้วย Area ID ซึ่งมีขนาด 32 บิท ดังภาพที่ 3.14 แสดงถึง Area ID ที่อาจจะแสดงได้ด้วยเลขฐานสิบ หรือเลขฐานสิบที่มีจุด และรูปแบบของทั้งสองแบบสามารถใช้ร่วมกันได้ ตัวอย่างเช่น แอเรีย 0 และแอเรีย 0.0.0.0 มีค่าเท่ากัน แอเรีย 16 เท่ากับ 0.0.0.16 และแอเรีย 271 เท่ากับ 0.0.0.15 เป็นต้น

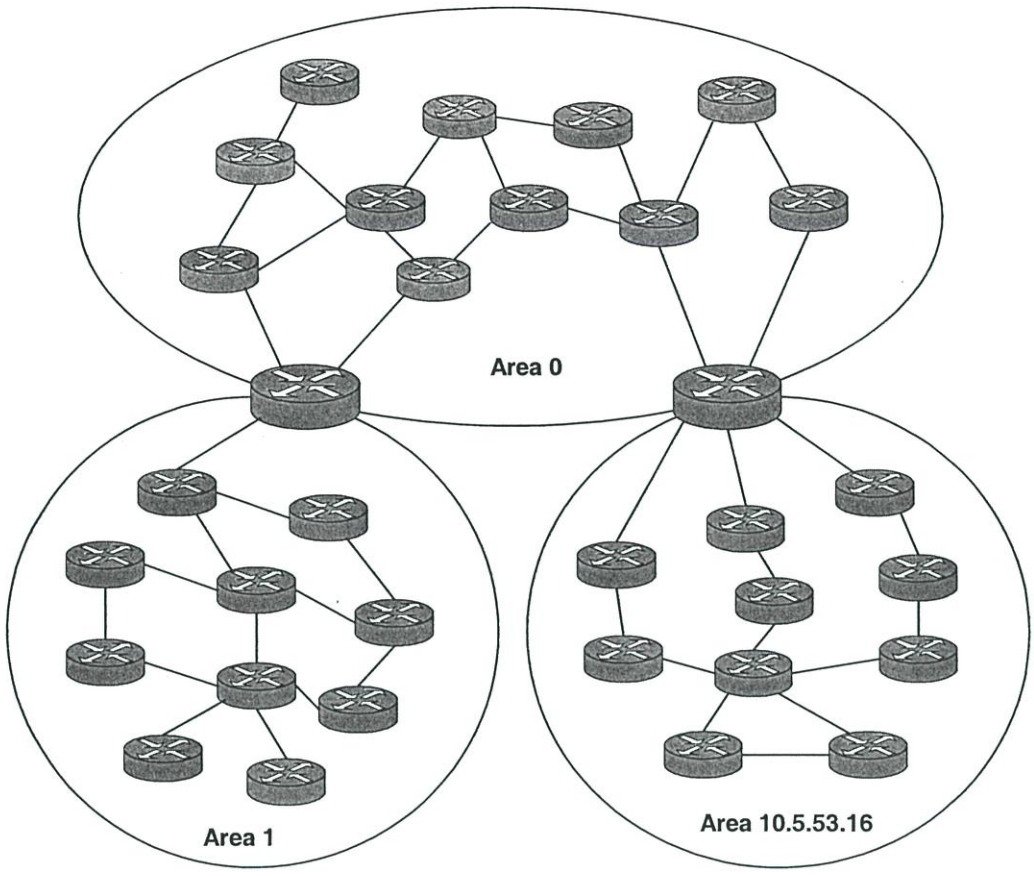
ทราฟฟิก 3 ชนิดที่ถูกกำหนดขึ้นตามความสัมพันธ์ของแอเรีย มีดังนี้

- Intra-area : เป็นทราฟฟิกที่ประกอบด้วยแพ็กเก็ตที่ถูกส่งผ่านกันระหว่างเราท์เตอร์ที่อยู่ภายในแอเรียเดียวกัน

- Inter-area : เป็นทราฟฟิกที่ประกอบด้วยแพ็กเก็ตที่ถูกส่งผ่านกันระหว่างเราท์เตอร์ที่อยู่ในแอเรียต่างกัน

- External-area : เป็นทราฟฟิกที่ถูกส่งผ่านระหว่างเราท์เตอร์ที่อยู่ภายในโดเมน OSPF กับเราท์เตอร์ที่อยู่ภายในระบบ autonomous อื่น

แอเรีย 0 (หรือ 0.0.0.0) ได้ถูกสำรองไว้สำหรับ backbone ซึ่ง backbone ทำหน้าที่รวบรวม topography ต่าง ๆ ของแต่ละแอเรียกับแอเรียอื่น ๆ ทุกแอเรีย เหตุผลคือเพื่อให้ทราฟฟิกของ inter-area ทั้งหมดต้องผ่านทะลุ backbone แอเรียที่ไม่ใช่ backbone ไม่สามารถแลกเปลี่ยนแพ็กเก็ตได้โดยตรง



ภาพที่ 3.14 กลุ่มเราท์เตอร์ในเชิงตรรกที่ถูกจัดแบ่งเป็นแอเรียต่าง ๆ

3.9 ชนิดของเราท์เตอร์ (Router Types)

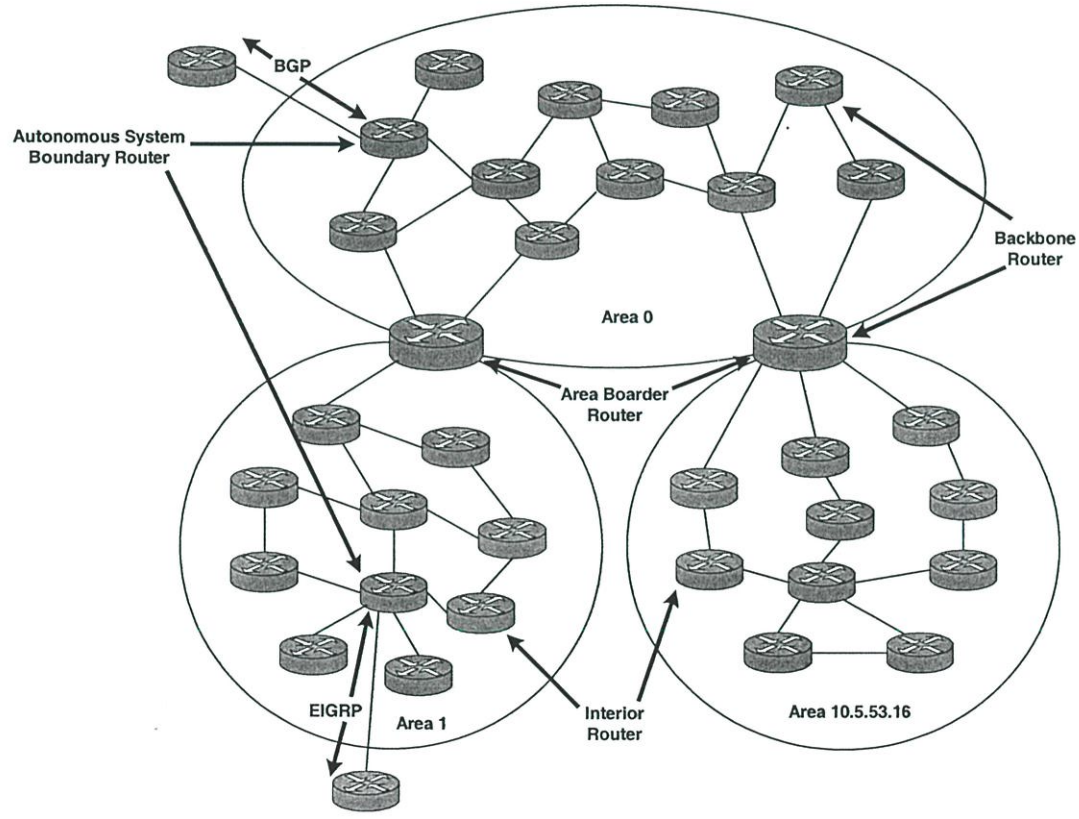
เราท์เตอร์ก็เหมือนกับทราฟฟิกที่สามารถจัดแบ่งเป็นกลุ่มตามความสัมพันธ์กับแอเรีย เราท์เตอร์ OSPF ทั้งหมดจะถูกแบ่งออกเป็น 4 แบบ ดังภาพที่ 3.15

- Internal Router : คือ เราท์เตอร์ที่มีอินเทอร์เฟสทั้งหมดอยู่ในแอเรียเดียวกัน เราท์เตอร์เหล่านี้มีฐานข้อมูลสถานะการเชื่อมโยงเดียว

- Area Border Routers (ABRs) : คือเราท์เตอร์ที่เชื่อมต่อกับ 1 แอเรียหรือมากกว่ากับ backbone และทำหน้าที่เป็น gateway สำหรับทราฟฟิกแบบ inter-area ABR ต้องมีอย่างน้อยหนึ่งอินเทอร์เฟสเสมอที่เป็นของ backbone และต้องรักษาฐานข้อมูลสถานะการเชื่อมโยงแยกกันสำหรับแอเรียแต่ละแอเรียที่ถูกต่ออยู่ เพราะว่า ABR มีหน่วยความจำและมีหน่วยประมวลผลที่มีความสามารถสูงกว่า Internal Router ABR จะสรุปข้อมูล topological ของแอเรียของมันเองที่ถูกต่ออยู่เข้าไปใน backbone จากนั้นจึงแร่กระจายข้อมูลสรุปให้แก่แอเรียอื่น ๆ

- Backbone Routers : เป็นเราท์เตอร์ที่มีอย่างน้อยหนึ่งอินเทอร์เฟสต่ออยู่กับ backbone ถึงแม้ว่าความต้องการนี้หมายความว่า ABR ก็เป็น Backbone Router ด้วย ซึ่งในภาพที่ 3.15 แสดงให้เห็นว่า Backbone Routers ทั้งหมดไม่ใช่ ABR Internal Router ที่มีอินเทอร์เฟสทั้งหมดเป็นของแอเรีย 0 ยังเป็น Backbone Router ด้วย

Autonomous System Boundary Routers (ASBRs) คือ gateway สำหรับทราฟฟิกที่มาจากภายนอก การปล่อยเส้นทางเข้าไปในโดเมน OSPF ที่ได้เรียนรู้จากโพโทคอลชนิดอื่น เช่น BGP และ EIGRP ดังแสดงในภาพที่ 3.15 ASBR สามารถวางไว้ที่ไหนก็ได้ภายใน autonomous system ของ OSPF ซึ่งอาจจะเป็น Internal Backbone หรือ ABR ก็ได้

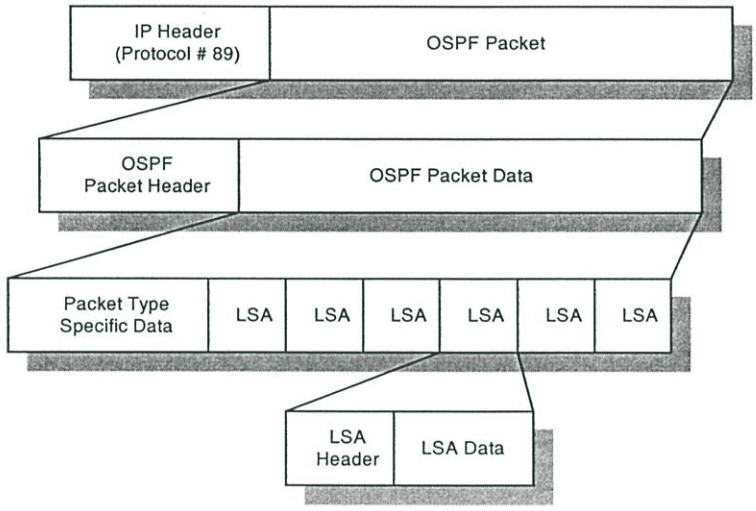


ภาพที่ 3.15 การจัดแบ่งเราท์เตอร์เป็น Internal Router Backbone Router Area Border Router(ABR) หรือ Autonomous System Boundary Router (ASBR)

3.10 รูปแบบแพ็กเก็ต OSPF (OPSF Packet Formats)

แพ็กเก็ต OSPF ประกอบด้วยการบีบอัดข้อมูล (encapsulation) หลาย ๆ ครั้ง ดังแสดงในภาพที่ 3.16 การบีบอัดข้อมูลภายใน IP header เป็น 1 ใน 5 ชนิดของแพ็กเก็ต OSPF แพ็กเก็ตแต่

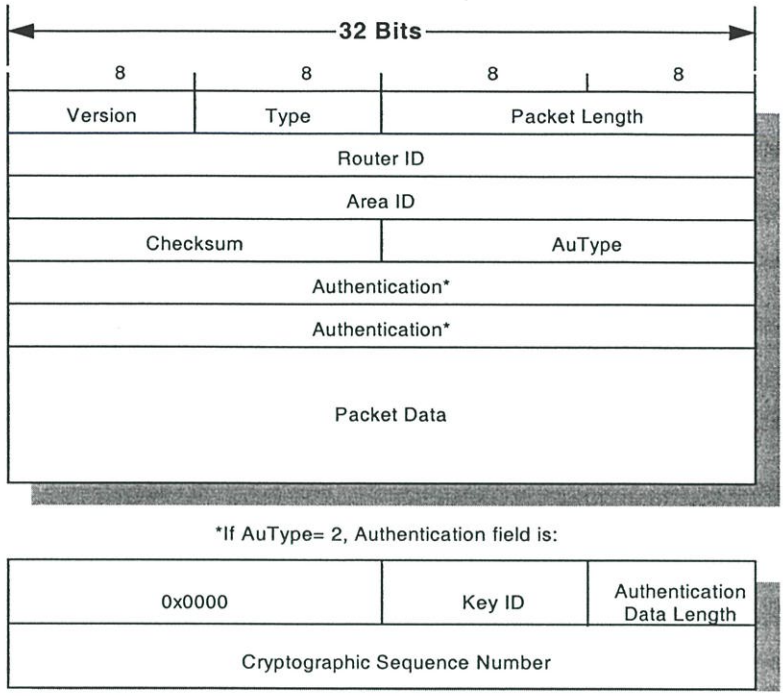
ละชนิดเริ่มด้วย header ของแพ็กเก็ต OSPF ส่วนข้อมูลของแพ็กเก็ต OSPF ที่ตามหลัง header จะแปรเปลี่ยนเพื่อให้สอดคล้องตามชนิดของแพ็กเก็ต ชนิดของแพ็กเก็ตในแต่ละชนิดจะมีหมายเลขฟิลด์ตามชนิดที่ระบุไว้ตามด้วยข้อมูลเป็นจำนวนมาก ข้อมูลที่บรรจุอยู่ในแพ็กเก็ต Hello จะเป็นรายชื่อของเพื่อนบ้าน แพ็กเก็ตร้องของ LS จะบรรจุ series ของฟิลด์ แพ็กเก็ต update LS จะบรรจุรายชื่อของ LSA ดังแสดงในภาพที่ 3.16 LSA พวกนี้ก็มี header และฟิลด์ ข้อมูลตามชนิดที่ระบุไว้เป็นของตัวเอง แพ็กเก็ตที่เป็นรายละเอียดข้อมูลและการรับรอง LS จะบรรจุรายชื่อ header ของ LSA



ภาพที่ 3.16 โครงสร้างแพ็กเก็ต OSPF ในรูปของการบีบอัด

3.10.1 Header ของแพ็กเก็ต (Packet Header)

แพ็กเก็ต OSPFทั้งหมดเริ่มต้นด้วย header ขนาด 24 octet ดังภาพที่ 3.17



ภาพที่ 3.17 แพ็กเก็ต Header ของ OSPF

ตารางที่ 3.7 ชนิดแพ็กเก็ต OSPF

Type Code	รายละเอียด
1	Hello
2	Database Description
3	Link State Request
4	Link State Update
5	Link State Acknowledgment

- Version คือหมายเลขเวอร์ชั่น OSPF โดยส่วนใหญ่มีค่าเวอร์ชั่นเป็น 2
- Type ระบุชนิดของแพ็กเก็ตตาม header ตารางที่ 3.7 แสดงชนิดของแพ็กเก็ตมีอยู่ 5 ชนิดตามหมายเลขที่ปรากฏในฟิลด์ type
- Packet length คือความยาวของแพ็กเก็ต OSPF (อยู่ในรูป octets) ซึ่งรวม header ด้วย
- Router ID คือ ID ของเราท์เตอร์ตัวต้นกำเนิด

- Area ID คือ แอเรียที่ได้จากแพ็กเก็ตที่เกิดขึ้นมา ถ้าแพ็กเก็ตถูกส่งผ่านไปบนการเชื่อมโยงเสมือน Area จะเป็น 0.0.0.0 (backbone area ID) เพราะว่าการเชื่อมโยงเสมือนถือเป็นส่วนหนึ่งของ backbone

- Checksum คือ การตรวจสอบผลรวม IP มาตรฐานของแพ็กเก็ตทั้งหมดรวมถึง header ด้วย

- Au Type คือโหมดที่ใช้ในการรับรองการมีตัวตน ตารางที่ 3.8 เป็นรายชื่อโหมดของการรับรองการมีตัวตนที่เป็นไปได้

- Authentication คือ ข้อมูลที่มีความจำเป็นต่อแพ็กเก็ตที่ถูกรับรองการมีตัวตนด้วยโหมดที่ถูกระบุไว้ในฟิลด์ AuType ถ้า Au Type = 0 ฟิลด์จะไม่ถูกตรวจสอบเพราะฉะนั้นภายในฟิลด์จะบรรจุอะไรก็ได้ ถ้า Au Type = 1 ภายในฟิลด์จะบรรจุด้วยรหัสผ่านขนาด 64 บิท ถ้า Au Type = 2 ภายในฟิลด์ Authentication จะบรรจุ Key ID ความยาวข้อมูลการรับรองการมีตัวตน และหมายเลขลำดับของ Cryptographic ที่ไม่มีการลดจำนวน สาระสำคัญของข่าวสาร (message digest) จะถูกใส่เพิ่มไว้ท้ายสุดของแพ็กเก็ต OSPF และจะไม่ถูกพิจารณาว่าเป็นส่วนหนึ่งของแพ็กเก็ตของตัวมันเอง

ตารางที่ 3.8 ชนิด authentication ของ OSPF

AuType	Authentication Type
0	Null (ไม่มีการทำ authentication)
1	Simple (clear text) Password Authentication
2	Crytographic (MD5) Checksum

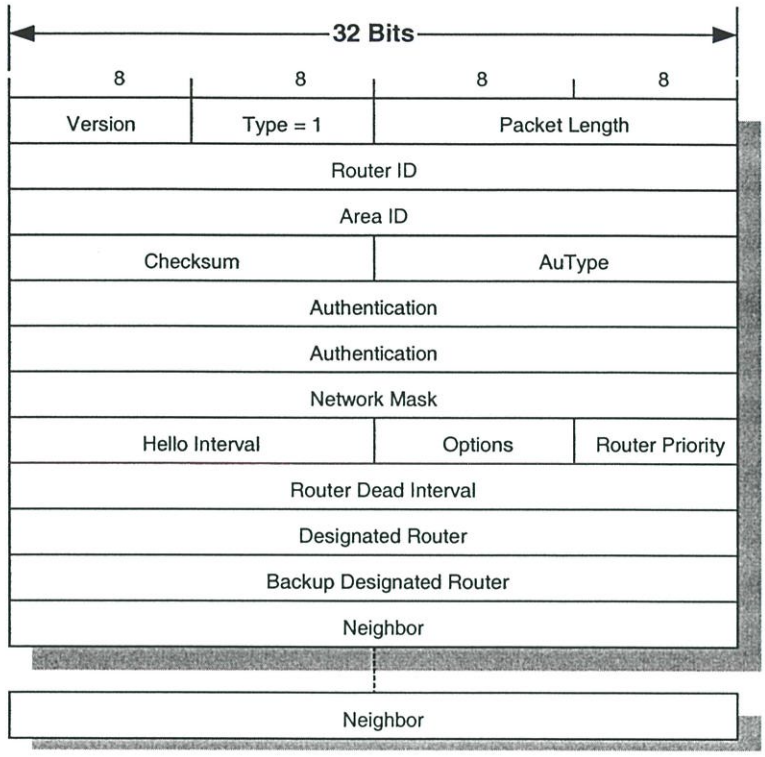
- Key ID บ่งบอกถึงอัลกอลิธึ่มของการรับรองการมีตัวตน และ secret key ที่ใช้สร้างสาระสำคัญของข่าวสาร (message digest)

- Authentication Data Length ระบุถึงความยาว (หน่วยเป็น octets) ของสาระสำคัญของข่าสารที่ถูกใส่เพิ่มไว้ท้ายสุดของแพ็กเก็ต

- Cryptographic Sequence Number คือหมายเลขที่ไม่ลดจำนวนใช้เพื่อป้องกันการพยายามเล่นซ้ำ

3.10.2 Hello Packet

Hello packet (ภาพที่ 3.18) ทำหน้าที่สร้างและรักษาการอยู่ติดกัน Hello จะนำเอาค่าพารามิเตอร์ที่เพื่อนบ้านต้องตกลงกันเพื่อจัดรูปแบบการอยู่ติดกัน



ภาพที่ 3.18 แพ็กเก็ต Hello ของ OSPF

- Network Mask คือแอดเดรสมาส์คของอินเทอร์เฟสที่มีแพ็กเก็ตส่งออกไป ถ้ามาส์คนี้ไม่ตรงกับมาส์คของอินเทอร์เฟสที่รับแพ็กเก็ตเข้ามา แพ็กเก็ตจะถูกตัดทิ้ง เทคนิคนี้รับรองว่าเราท์เตอร์จะกลายเป็นเพื่อนบ้านกันได้ถ้าเราท์เตอร์สามารถตกลงกันด้วยแอดเดรสที่แน่นอนของเครือข่ายร่วม

- Hello Interval คือคาบเวลา (หน่วยเป็นวินาที) ระหว่างการส่งแพ็กเก็ต Hello บนอินเทอร์เฟส ถ้าเราท์เตอร์ตัวส่งและตัวรับมีค่าพารามิเตอร์นี้ต่างกัน เราท์เตอร์ทั้งสองจะไม่สร้างความสัมพันธ์การเป็นเพื่อนบ้าน

- Options ฟิลด์นี้ถูกรวมอยู่ในแพ็กเก็ต Hello เพื่อทำให้แน่ใจว่าเพื่อนบ้านมีความสามารถที่สามารถเข้ากันได้ เราท์เตอร์สามารถปฏิเสธการเป็นเพื่อนบ้านเพราะว่ามีความสามารถไม่ตรงกัน

- Router Priority ถูกใช้ในการเลือก DR และ BDR ถ้าหากเซ็ทเป็น 0 เราท์เตอร์ตัวต้นกำเนิดจะไม่ได้รับเลือกให้เป็น DR หรือ BDR

- Router Dead Interval คือเวลามีหน่วยเป็นวินาทีที่เราท์เตอร์ตัวต้นกำเนิดจะคอย Hello จากเพื่อนบ้านก่อนประกาศว่าเพื่อนบ้านตายไป (dead) ถ้าได้รับ Hello ในช่วงเวลาที่ไม่ตรงกันกับ RouterDeadInterval ของอินเทอร์เฟสด้านรับ แพ็กเก็ตจะถูกตัดทิ้ง

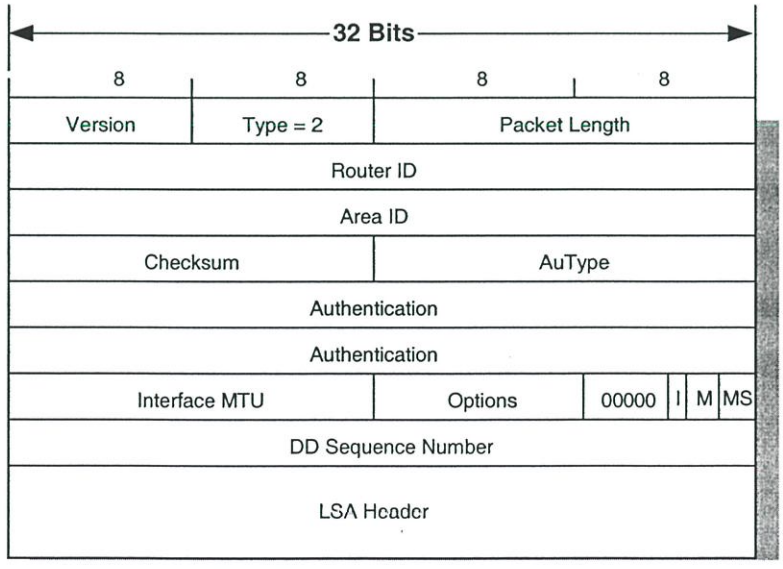
- Designated Router คือแอดเดรส IP ของอินเทอร์เฟสของ DR ที่อยู่บนเครือข่าย (ไม่ใช่ Router ID ของตัวมันเอง)

- Backup DR คือแอดเดรส IP ของอินเทอร์เฟสของ BDR ที่อยู่บนเครือข่าย

- Neighbor คือฟิลด์ที่เกิดขึ้นซ้ำซึ่งแสดงรายชื่อเพื่อนบ้านทั้งหมดที่อยู่บนเครือข่ายจากที่ ๆ ซึ่งเราท์เตอร์ตัวต้นกำเนิดได้รับ Hello ในช่วง past RouterDeadInterval

3.10.3 Database Description Packet

แพ็กเก็ต Database Description (ดังภาพที่ 3.19) ถูกใช้เมื่อการอยู่ติดกันกำลังถูกสร้างขึ้น จุดประสงค์หลักของแพ็กเก็ต DD คือใช้เพื่ออธิบาย LSA บางส่วนหรือทั้งหมดที่อยู่ในฐานข้อมูลของตัวกำเนิด เพื่อที่ว่าตัวรับสามารถกำหนดได้ว่ามันมี LSA ที่เหมาะสมกับฐานข้อมูลของตัวมันเองหรือไม่ สิ่งนี้ถูกกระทำโดยการตรวจสอบรายชื่อ header ของ LSA เท่านั้น เนื่องจากว่าแพ็กเก็ต DD หลาย ๆ แพ็กเก็ตอาจจะถูกแลกเปลี่ยนกันในช่วงกระบวนการนี้ flags จึงได้ถูกใส่รวมไว้เพื่อทำการจัดก ารแลกเปลี่ยนโดยผ่านทางความสัมพันธ์ที่ใช้ในการโพล master/slave



ภาพที่ 9.19 แพ็กเก็ต Database Description ของ OSPF

- Interface MTU : คือขนาด (หน่วยเป็น octets) ของแพ็กเก็ต IP ที่ใหญ่ที่สุดที่สามารถส่งออกไปยังอินเทอร์เฟสของตัวต้นกำเนิดโดยปราศจากการแบ่งเป็นส่วนย่อย ๆ (fragmentation) ฟิลด์นี้จะถูกเซ็ทเป็น 0x0000 เมื่อแพ็กเก็ตถูกส่งออกไปบนการเชื่อมโยงเสมือน

- Options : ฟิลด์นี้ถูกรวมเข้าไปแพ็กเก็ตรายละเอียดฐานข้อมูล เพื่อให้เราท์เตอร์เลือกหรือไม่ก็ส่ง LSA ที่แน่นอนแก่เพื่อนบ้านที่ไม่รองรับความสามารถที่จำเป็น

- 5 บิทแรกของ octet ถัดไปไม่ได้ใช้ และถูกเซ็ทให้มีค่า 00000b เสมอ

- I-bit หรือ Initial bit จะถูกเซ็ทเป็น 1 เมื่อแพ็กเก็ตเป็นแพ็กเก็ตเริ่มแรก (Initial) ใน series ของแพ็กเก็ต DD โดยที่แพ็กเก็ต DD ถัดไปจะมี I-bit = 0

- M-bit หรือ More bit จะถูกเซ็ทเป็น 1 เพื่อชี้ว่าแพ็กเก็ตนี้ไม่ใช่แพ็กเก็ต DD แพ็กเก็ตสุดท้ายใน series แพ็กเก็ต DD โดยที่แพ็กเก็ตสุดท้ายจะมี M-bit = 0

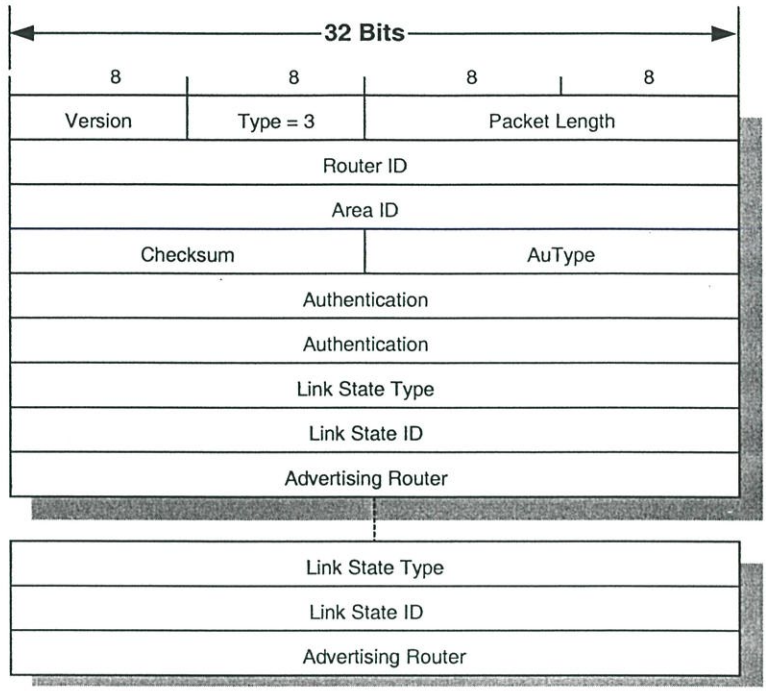
- MS-bit หรือ Master/Slave bit ถูกเซ็ทเป็น 1 เพื่อชี้ว่าตัวกำเนิดเป็น master (นั่นคืออยู่ในความควบคุมของขั้นตอนการโพล) ในช่วงเวลาการทำให้ฐานข้อมูลมีความสอดคล้องกัน Slave จะมี MS-bit = 0

- DD Sequence Number ทำให้แน่ใจว่าลำดับของแพ็กเก็ต DD ทั้งหมดถูกรับได้ในขั้นตอนการทำให้ฐานข้อมูลมีความสอดคล้องกัน หมายเลขลำดับจะถูกเซ็ทโดย master ซึ่งเป็นค่าเฉพาะในแพ็กเก็ต DD แรก และลำดับจะถูกเพิ่มขึ้นในแพ็กเก็ตลำดับถัดไป

- LSA Headers รายชื่อ header ของ LSAs ทั้งหมดหรือเพียงบางส่วนในฐานข้อมูลสถานะการเชื่อมโยงของตัวกำเนิด

3.10.3 Link State Request Packet

เนื่องจากแพ็กเก็ตรายละเอียดฐานข้อมูลถูกรับได้ในช่วงกระบวนการที่ทำให้ฐานข้อมูลมีค่าตรงกัน เพราะฉะนั้นเราท์เตอร์จะทำการเก็บ LSAs ไว้บางส่วนซึ่งไม่มีอยู่ในฐานข้อมูลของมันเอง LSA เหล่านี้ได้ถูกบันทึกอยู่ในรายการร้องขอสถานะการเชื่อมโยง จากนั้นเราท์เตอร์จะส่งแพ็กเก็ตการร้องขอสถานะการเชื่อมโยง (ดังภาพที่ 3.20) ไป 1 แพ็กเก็ตหรือมากกว่า เพื่อขอสำเนาของ LSA จากเพื่อนบ้าน สังเกตว่าแพ็กเก็ตบ่งชี้ LSA ที่มีเอกลักษณ์เฉพาะโดยฟิลด์ชนิด (Type) ฟิลด์ ID และฟิลด์การประกาศของเรท์เตอร์ แต่ไม่ได้ร้องขอตัวอย่างชี้เฉพาะของ LSA



ภาพที่ 3.20 แพ็กเก็ต Link State Request ของ OSPF

- Link State Type คือ หมายเลขชนิดของ LSA ซึ่งแสดงถึง LSA ที่เป็น LSA เราท์เตอร์ LSA เครือข่าย และอื่น ๆ หมายเลขชนิดถูกแสดงไว้ในตารางที่ 3.9

- Link State ID คือ ฟิลด์ type-dependent ของ LSA header และ ส่วนของ LSA-specfic สำหรับรายละเอียดทั้งหมดของวิธีที่ LSA หลาย ๆ แบบใช้อยู่

- Advertisting Router คือ Router ID ของเราท์เตอร์ที่กำเนิด LSA

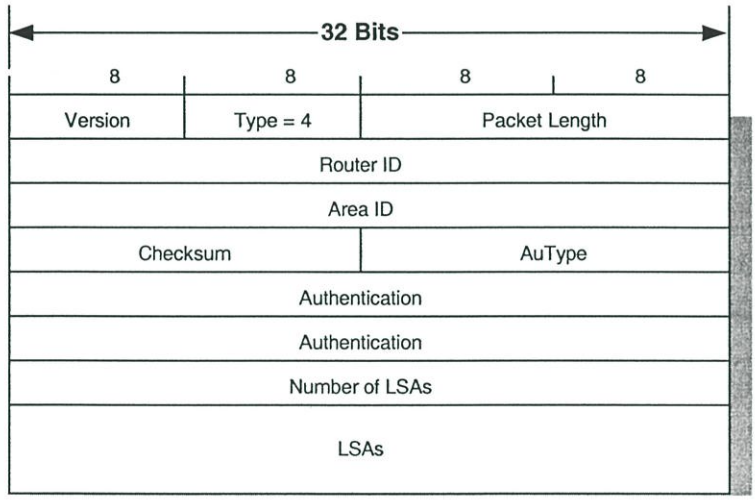
ตารางที่ 3.9 ชนิดของ LSA

Type Code	รายละเอียด
1	Router LSA
2	Network LSA
3	Network Summary LSA
4	ASBR Summary LSA
5	AS External LSA
6	Group Menbership LSA
7	NSSA External LSA

8	External Attributes LSA
9	Opaque LSA (link-local scope)
10	Opaque LSA (area-local scope)
11	Opaque LSA (AS scope)

3.10.4 Link State Update Packet

Link State Update Packet (ดังภาพที่ 3.21) ที่ถูกใช้ในการกระจาย LSAs และส่ง LSA ในการตอบสนองการร้องขอสถานะการเชื่อมโยง ระลึกไว้ว่าแพ็กเก็ตไม่ได้ทิ้งเครือข่ายไว้กับที่ ๆ ซึ่งแพ็กเก็ตกำเนิดขึ้น ดังนั้นแพ็กเก็ต Link State Update นำพา LSAs เท่านั้นเพียง 1 hop จากเราท์เตอร์ตัวต้นกำเนิดของพวกมัน เพื่อนบ้านด้านรับมีหน้าที่ re-encapsulate LSA ที่เหมาะสมลงในแพ็กเก็ต update LSA แพ็กเก็ตใหม่เพื่อการแพร่กระจายต่อ ๆ ไป



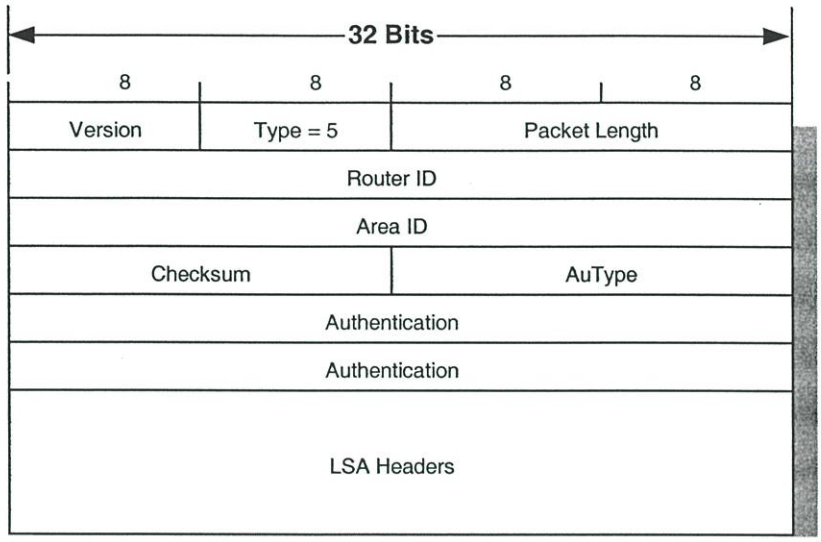
ภาพที่ 3.21 แพ็กเก็ต Link State Update ของ OSPF

- Number of LSAs ระบุหมายเลขของ LSA ที่รวมอยู่ในแพ็กเก็ตนี้
- LSAs คือ LSAs ที่สมบูรณ์ ในการ update แต่ละครั้งอาจจะนำพาได้หลาย ๆ LSAs ซึ่งขึ้นอยู่กับขนาดแพ็กเก็ตที่มากที่สุดที่ยอมรับได้ในข่ายเชื่อมโยง

3.10.5 Link State Acknowledgment Packet

Link State Acknowledgment packet ถูกใช้เพื่อสร้างความน่าเชื่อถือให้กับการแพร่กระจาย LSAs ในแต่ละ LSA ที่รับได้โดยเราท์เตอร์จากเพื่อนบ้านที่ต้องรับรู้อย่างแท้จริงในแพ็กเก็ต Link State Acknowledgment ใน LSA ที่ถูกรับรู้ได้ถูกระบุโดยการรวม header ของตัวมันเอง

เข้าไปในแพ็กเก็ต LS ACK และหลาย ๆ LSAs อาจจะถูกรับรู้ในแพ็กเก็ตเดียวได้ ดังภาพที่ 3.22 แสดงถึงแพ็กเก็ต LS ACK ประกอบด้วย OSPF header และ LSA headers



ภาพที่ 3.22 แพ็กเก็ต Link State Acknowledgment ของ OSPF

บทที่ 4
รูปแบบที่ใช้อ้างอิงและรายละเอียดการบริการ

4.1 ชุดโปรโตคอล H.323

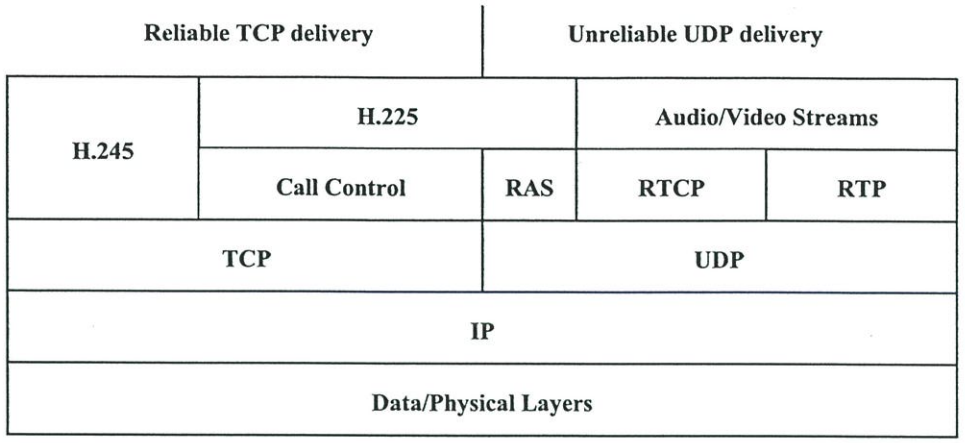
H.323 เป็น คุณลักษณะของ ITU-T สำหรับส่งข้อมูลแบบมัลติมีเดีย (เสียง,ภาพ และข้อมูล) ข้ามผ่านไปในเครือข่ายระยะใกล้ ที่ไม่รับรองในคุณภาพของการให้บริการ (QoS) เครือข่ายแพ็กเก็ตพื้นฐาน สามารถที่จะใช้ได้ทั้ง IP, IPX หรือ โพรโตคอลอื่นๆ H.323 ยอมให้สำหรับมาตรฐานการเชื่อมต่อ กับอุปกรณ์ H.323 ของผู้ขายอื่นที่เข้ากันได้

มาตรฐานของ H.323 ประกอบด้วยองค์ประกอบและโปรโตคอล ดังต่อไปนี้

คุณลักษณะ	โปรโตคอล
Call Signalling	H.225
Media Control	H.245
Audio Coders	G.711, G.722, G.723, G.729
Video Coders	H.261, H.263
Data Sharing	T.120
Media Transport	RTP/RTCP

4.1.1 โปรโตคอล H.323

โปรโตคอล H.323 [2] ขึ้นอยู่กับหลายๆโปรโตคอล ดังแสดงในภาพที่ 5.4 โดยโปรโตคอลเหล่านี้สนับสนุน call admissions, setup, status, teardown, meadia stream และ messages ในระบบ H.323 โปรโตคอลเหล่านี้สนับสนุนด้วยทั้ง ความแน่นอน และความไม่แน่นอนของกลไกการส่งแพกเก็ตบนเครือข่ายข้อมูล แม้ว่าการเพิ่มการใช้ประโยชน์จาก H.323 ส่วนใหญ่ในวันนี้ TCP เป็นกลไกในการส่งผ่านสำหรับสัญญาณ และ H.323 version 2 สามารถส่งผ่าน UDP มาตรฐานอื่นๆได้ถูกตรวจสอบการใช้งานอื่นๆบนกลไก UDP บนความน่าเชื่อถืออื่นๆ ซึ่งสร้างวิธีการของสัญญาณ



ภาพที่ 4.1 เลเยอร์ของชุดโปรโตคอล H.323

ชุดโปรโตคอล H.323 ได้ถูกแยกออกเป็น 3 ส่วนของการควบคุม

- สัญญาณ Registration, Admissions และ Status (RAS) จะเตรียมการควบคุมก่อนเรียกใน Gatekeeper H.323 พื้นฐานเครือข่าย

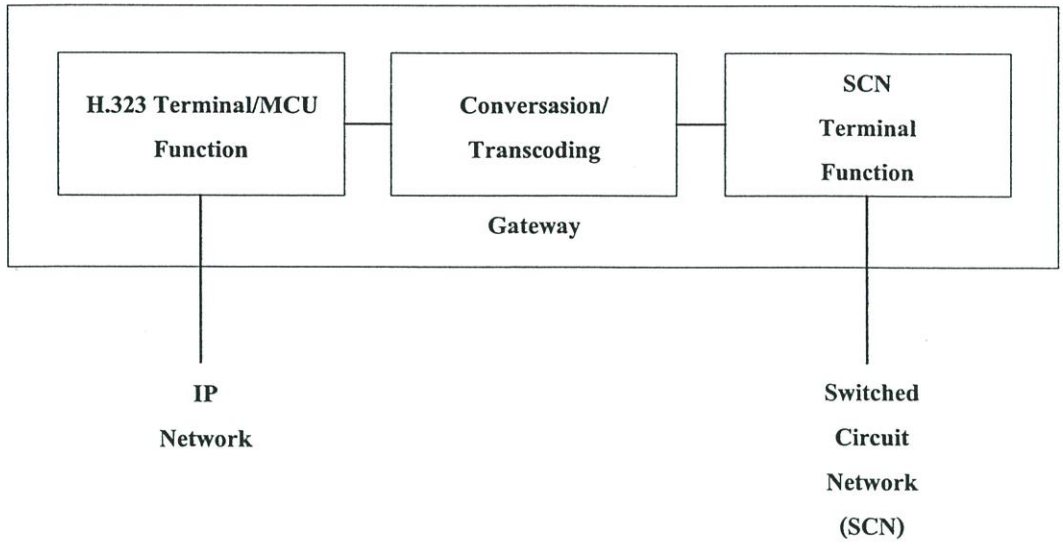
- Call Control Signaling ใช้ในการเชื่อมต่อ (Connect) รักษา (Maintain) และเลิกล้ม(Disconnect) การเรียก (Call) ระหว่างเครื่องโทรศัพท์

- Media Control and Transport จัดการโดยอาศัยช่องทาง H.245 ที่พาตัวกลางที่ควบคุมข่าวสาร การส่งเกิดขึ้นในส่วนที่ไม่ขึ้นอยู่กับกระแส UDP

4.2 Gateway

H.323 gateway [2] มีคุณสมบัติ ทำให้เห็น จุดปลายทางของ Switched Circuit Network (SCN) และ จุดปลายทางของ H.323 มันทำการแปลงระหว่าง เสียง ภาพ และ รูปแบบการส่งข้อมูลพร้อมกับระบบสื่อสารและโปรโตคอล รวมถึงการสร้างการเรียก และการขาดออกของทั้งคู่ บนเครือข่าย IP และ SCN

Gateway จะไม่จำเป็นจนกว่าการเชื่อมต่อระหว่างกันด้วย SCN นั้นถูกเรียกร้อง ดังนั้นจุดปลายทางของ H.323 สามารถที่จะสื่อสารโดยตรงข้ามบนเครือข่ายแพกเก็จ โดยปราศจากการเชื่อมต่อไปยัง gateway ซึ่ง gateway ทำหน้าที่เหมือน H.323 terminal หรือ MCU บนเครือข่าย และ SCN terminal หรือ MCU บน SCN ดังแสดงในภาพที่ 4.2



ภาพที่ 4.2 ส่วนของ H.323 Gateway

4.3 Gatekeeper

หน้าที่ทางเลือกของ gatekeeper เตรียมการ pre-call และ call-level ควบคุมการให้บริการ ไปยังจุดปลายทาง H.323 gatekeeper คือแยก logically จากส่วนเครือข่ายอื่นใน H.323 ถ้ามี gatekeeper เพิ่มมากกว่าหนึ่ง ระหว่างการสื่อสาร ได้ทำสำเร็จลงในแบบไม่เจาะจง

Version ใหม่ของ H.323 เช่น H.323 version 3 ซึ่งได้ถูกกำหนดล่าสุดเป็นเอกสาร เมื่อปลายปี 1999 จะพยายามสนับสนุนรายละเอียดการสื่อสารระหว่างกันของ gatekeeper gatekeeper สามารถใช้ตัวอย่างลำดับ query/response (Location Request [LRQ] หรือ Location Confirmation [LCF]) ถึงสถานที่ users ไกล การแลกเปลี่ยนข้อมูล H.323 version 3 ใช้ Annex G สำหรับถามหรือแลกเปลี่ยนฐานข้อมูล ยังมี protocol อื่น Open Settlements Protocol (OSP) ด้วย รายละเอียดตาม European Telecommunication Standards Institute (ETSI) TS 101 321 ถูกใช้ส่วนใหญ่สำหรับติดต่อกัน intra-domain จาก gateway และ gatekeeper

ถ้า gatekeeper อยู่ในระบบ H.323 มันมักจะประกอบด้วยดังต่อไปนี้

- Address Translation จะให้ IP address ปลอม หรือ E.164 address
- Admissions Control จะให้ การอนุญาตการเข้าไปใน H.323 โดยใช้ messages ดังนี้ Admission Request/Admission Confirm/Admission Reject (ARQ/ACF/ARJ)
- Bandwidth Control ประกอบด้วยการจัดการความต้องการ bandwidth ที่ endpoint โดยการใช้ message ดังนี้ Bandwidth Request/Bandwidth Confirm/Bandwidth Reject (BRQ/BCF/BRJ)
- Zone Management จะทำการ register terminal, gateways และ MCUs

Gatekeeper discovery เป็นกระบวนการแบบ manual หรือ automatic endpoint ใช้แสดงซึ่ง register กับ gatekeeper ในวิธีการแบบ manual endpoint ถูก configured ด้วย IP address ของ gatekeeper และ ด้วยเหตุนั้น สามารถที่พยายาม registration ทันที แต่เฉพาะกับการกำหนดขั้นต้นของ gatekeeper ในวิธีการแบบ automatic สามารถที่จะมีความสัมพันธ์กันระหว่าง endpoint และ gatekeeper ที่จะเปลี่ยนเวลาและ ความต้องการทางกลไกที่เรารู้จักกันคือ auto discovery

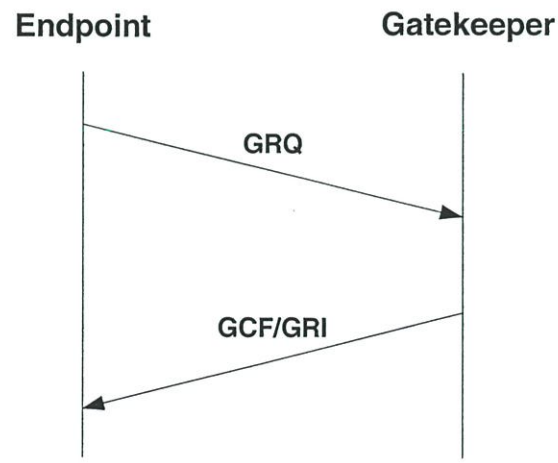
ความสามารถของ endpoint ใน Auto discovery ซึ่ง gatekeeper อาจไม่รู้จักมัน ทำการ discover มัน ไปยัง multicast message เพราะว่า endpoint ไม่มี configured คงที่ หรือเปลี่ยนแปลง configured สำหรับ gatekeeper นี้คือวิธีการที่บริหารให้มี overhead น้อย gatekeeper จะทำการค้นหา multicast address คือ 224.0.1.41 gatekeeper UDP ค้นหาดโดยใช้ port 1718 และ gatekeeper UDP registration status port 1719

- Gatekeeper Request (GRQ) Multicast message จะถูกส่งโดย endpoint ที่มองหา gatekeeper

- Gatekeeper Confirm (GCF) การตอบไปยัง endpoint GRQ แสดงถึงการส่ง address ของ gatekeeper's RAS channel

- Gatekeeper Reject (GRJ) รายงาน endpoint ว่า gatekeeper ไม่ต้องการยอมรับการ registration ในที่นี้มักจะใช้ตามกำหนดเวลา ที่ configuration บน gateway หรือ gatekeeper

จากภาพที่ 4.3 แสดงถึง messaging และ ลำดับของกระบวนการของ auto discovery



ภาพที่ 4.3 Gatekeeper Auto Discovery

4.4 Call Control Singnaling (H.225)

ในเครือข่าย H.323 ระเบียบการของ call control [5] คือ ขึ้นอยู่กับ International Telecommunication Union (ITU) Recommendation H.225 ซึ่งกำหนดให้ใช้และสนับสนุน Q.931 signaling ความเชื่อถือได้ของ call control channel คือสร้างข้ามบนเครือข่าย IP บน TCP port 1720 port นี้เป็นขั้นตอนแรกของ Q.931 call control message ระหว่าง 2 endpoints สำหรับ จุดประสงค์ของ การเชื่อมต่อ (connecting) การบำรุงรักษา (maintaining) และการตัดการเชื่อมต่อ (disconnecting calls)

ที่จริง call control และ keepalive message เคลื่อนที่ไปยัง port ที่อยู่ไม่ได้นาน หลังจากการเริ่ม call setup แต่ 1720 คือที่รู้จัก port สำหรับการเรียก H.323 ใน H.225 ด้วยที่กำหนดการใช้ของ Q.931 message สำหรับการบริการย่อย ตาม Q.931 และ Q.932 message เหมือนกันทั้งหมด โดยใช้ signaling messages ใน เครือข่าย H.323

- Setup ข่าวขาไปถูกส่งโดย calling H.323 พยายามสร้างการเชื่อมต่อไปยัง H.323 โดย message นี้ส่งไปบนที่รู้จักกัน H.225 TCP port 1720

- Call Proceeding ข่าวสารขากลับ ส่งจากผู้ถูกเรียกมายังผู้เรียก แจ้งว่าการเรียกกระบวนการสร้างถูกเริ่มต้น

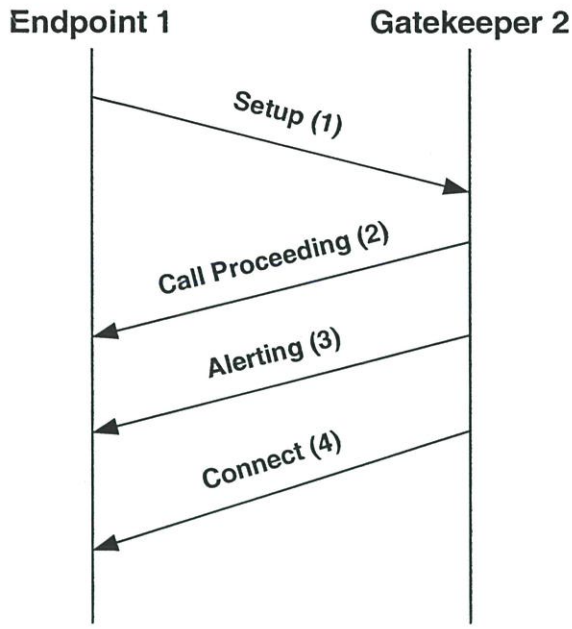
- Alerting ข่าวสารย้อนกลับส่งจากผู้ถูกเรียกเพื่อแจ้งว่าผู้ถูกเรียกส่วน ringing ถูกเริ่มต้น

- Connecting ข่าวสารย้อนกลับจากผู้ถูกเรียก ไปยังผู้เรียก แสดงว่าส่วนของผู้ถูกเรียกตอบรับการเรียก การเชื่อมต่อข้อความวามารถประกอบด้วยการขนส่ง UDP/IP address สำหรับ H.245 control signaling

- Release Complete ส่งโดย endpoint หลังจาก เริ่ม การตัดการเชื่อมต่อ ซึ่งแสดงถึงการเรียกถูกปลดออก ท่านสามารถส่ง message อย่างเดียวถ้า call signaling channel ถูก open หรือ active

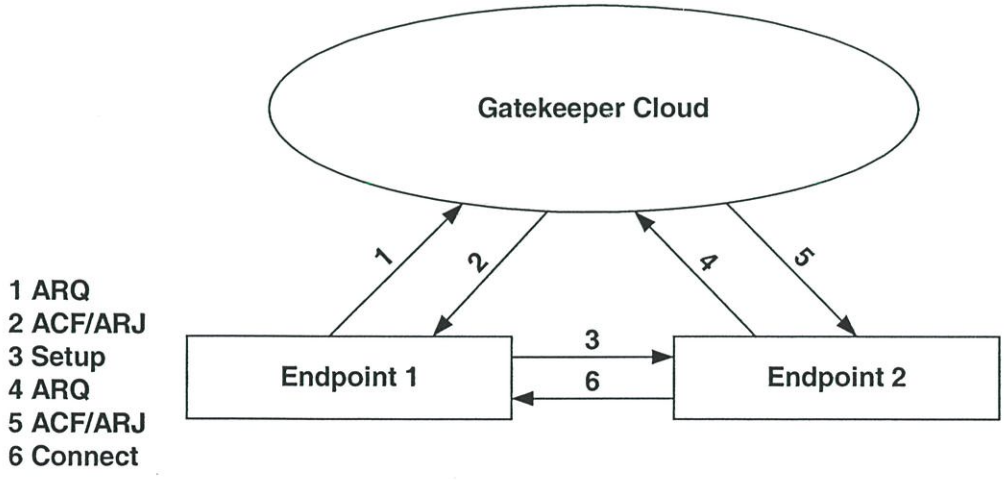
- Facility ใน message Q.931 ใช้สำหรับการขอ (Request) หรือ การรับรอง (Acknowledge)บริการย่อย มันถูกใช้เสมอที่จะแสดงการเรียกแบบตรงหรือตรงผ่านไปยัง gatekeeper

ภาพที่ 4.4 แสดงให้เห็น signaling message สำหรับ call setup การติดโต้ตอบระหว่างกันด้วย gatekeeper ถูกจำกัดไปยัง RAS message สำหรับ call permission และ อาจจะเป็นไปได้บน status messages



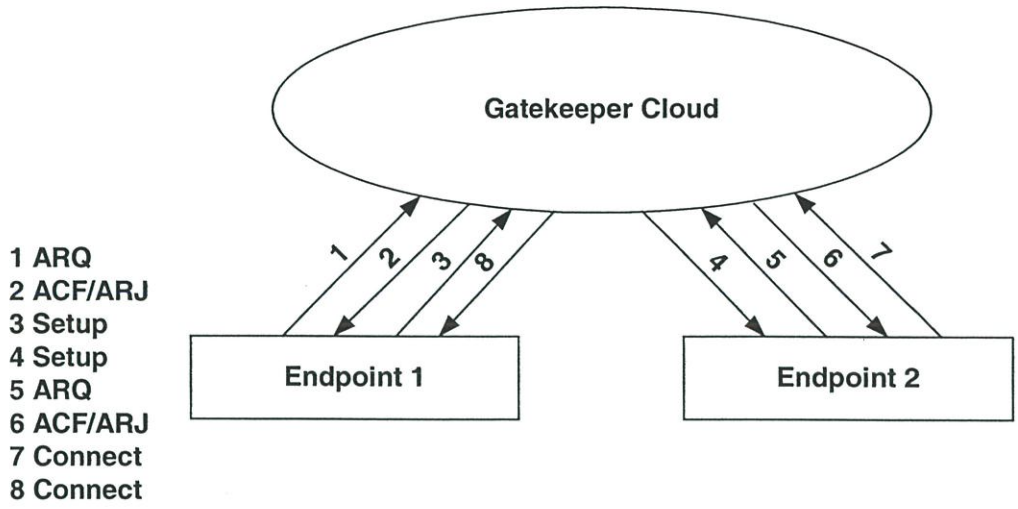
ภาพที่ 4.4 Call Setup Signaling Message

ท่านสามารถเปลี่ยน call signaling channel ในเครือข่าย H.323 ใน 2 ทางคือ Direct Endpoint Call Signaling และ GKRCS ในวิธีการ Direct Endpoint Call Signaling call signaling message จะส่งโดยตรงระหว่าง 2 endpoints ดังแสดงในภาพที่ 4.5



ภาพที่ 4.5 Direct Endpoint Call Signaling

ในวิธีการ GKRCS call signaling messages ระหว่าง endpoint ถูก route ผ่านไปยัง gatekeeper ดังแสดงในภาพที่ 4.4



ภาพที่ 4.6 Gatekeeper Routed Call Signaling

บทที่ 5
มาตรฐานและเทคนิคในการเข้ารหัส สัญญาณเสียง

5.1 การเข้ารหัสสัญญาณเสียง

การเข้ารหัสสัญญาณเสียง เป็นกระบวนการแปลงเสียงเป็นสัญญาณอนาลอก ให้อยู่ในรูปของสัญญาณดิจิตอล จากนั้นสัญญาณจะถูกส่งผ่านช่องสัญญาณสื่อสารและเมื่อสัญญาณนี้เดินทางถึงจุดหมายก็จะถูกแปลงกลับมาเป็นสัญญาณเสียงอีกครั้ง ซึ่งเป็นที่แน่นอนว่าเราต้องการวิธีการเข้ารหัสที่สามารถให้คุณภาพเสียงที่ดี มีดีเลย์ไทม์ที่น้อย และต้องการอัตราบิตในการเข้ารหัสต่ำๆ แต่ในทางปฏิบัติ คุณภาพของเสียงขึ้นอยู่กับอัตราบิตที่ใช้ในการเข้ารหัสอย่างเห็นได้ชัด นั่นคือยิ่งใช้อัตราบิตที่สูงขึ้นเท่าไรคุณภาพของเสียงก็มักจะดีขึ้นตามไปด้วย และในทางกลับกันยิ่งเราลดอัตราบิตลงมากเท่าใดคุณภาพของเสียงที่ได้ก็จะแย่ลงตามไปด้วย

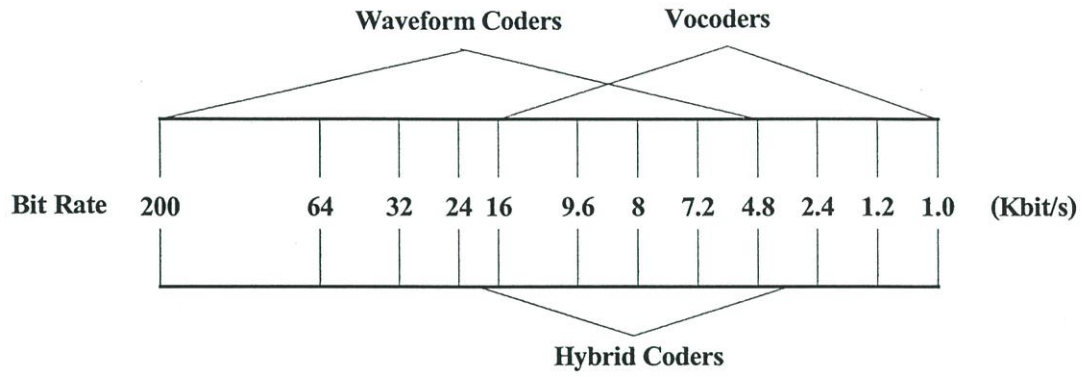
วิธีการเข้ารหัสสัญญาณเสียงแบ่งออกได้เป็น 3 กลุ่ม คือ

- วิธีการเข้ารหัสเสียงแบบ Waveform Coders
- วิธีการเข้ารหัสเสียงแบบ Parametric Coders หรือ vocoders
- วิธีการเข้ารหัสเสียงแบบ Hybrid

Waveform coders เป็นวิธีการที่สนใจเฉพาะกับรูปร่างของสัญญาณเป็นหลัก โดยในกระบวนการเข้ารหัสจะพยายามสร้างสัญญาณให้มีรูปร่างใกล้เคียงกับสัญญาณจริงมากที่สุด จากการที่เข้ารหัสแบบนี้มิได้คำนึงถึงว่าสัญญาณที่กำลังทำการเข้ารหัสอยู่นั้นจะเกิดจากแหล่งกำเนิดสัญญาณประเภทใด จึงสามารถนำมาใช้งานกับแหล่งกำเนิดสัญญาณได้หลายประเภท ในทางกลับกัน parametric coders หรือ vocoders อาศัยการที่ทราบถึงคุณสมบัติเฉพาะบางอย่างของแหล่งกำเนิดสัญญาณและนำมาใช้ให้เป็นประโยชน์ ดังนั้น โดยทั่วไปแล้วการเข้ารหัสสัญญาณเสียงแบบนี้จึงเหมาะสมกับแหล่งกำเนิดสัญญาณประเภทนั้นๆ ประเภทเดียว การเข้ารหัสแบบนี้มีจุดเด่นที่น่าสนใจคือสามารถเข้ารหัสสัญญาณเสียงได้ด้วยอัตราบิตต่ำกว่าการเข้ารหัสแบบ wave coders มาก แต่สัญญาณเสียงที่ออกมาไม่เป็นธรรมชาตินัก

การเข้ารหัสอีกประเภทหนึ่งซึ่งรวมคุณสมบัติที่ดีของการเข้ารหัสทั้งสองแบบนี้เข้าด้วยกันคือ hybrid coders วิธีการเข้ารหัสแบบนี้สามารถใช้ประโยชน์จากการที่ทราบถึงคุณสมบัติของแหล่งกำเนิดเสียงนั้นๆ และยังอาศัยวิธีของ Waveform coders เพื่อช่วยเพิ่มคุณภาพของเสียงให้ดีขึ้น เมื่อเปรียบเทียบวิธีนี้กับวิธี waveform coders แล้วจะพบว่าวิธีนี้ต้องการอัตราบิตในการเข้ารหัสที่ต่ำกว่า โดยที่คุณภาพเสียงที่ได้อาจไม่ดีเท่ากับวิธี waveform coders แต่อยู่ในระดับที่สามารถนำมาใช้งานได้ ทั้งนี้คุณภาพของเสียงก็ขึ้นอยู่กับอัตราบิตที่ใช้ด้วย นั่นคือยิ่งใช้อัตราบิทในการเข้ารหัสที่สูงขึ้นเท่าใดก็จะได้เสียงที่มีคุณภาพมากขึ้นตามไปด้วย แต่ถ้าเปรียบเทียบกับการเข้ารหัสแบบ

vocoders วิธีแบบ hybrid coders นี้สามารถให้คุณภาพเสียงที่ดีกว่ามาก แต่ก็ต้องข้ารหัสที่อัตราบิตสูงกว่า จากภาพที่ 5.1 แสดงการเปรียบเทียบช่วงของอัตราบิตที่ต้องใช้สำหรับวิธีการเข้ารหัสแต่ละประเภท



ภาพที่ 5.1 การเปรียบเทียบช่วงของอัตราบิตที่ต้องใช้สำหรับวิธีการเข้ารหัสแต่ละประเภท

5.2 วิธีการเข้ารหัสเสียงแบบ Waveform Coders

วิธีการเข้ารหัสแบบ waveform coders สามารถแบ่งออกเป็น 2 แบบคือ

- ไทม์โดเมน (Time Domain)
- ฟรีเควนซี่โดเมน (frequency domain)

ตัวอย่างของวิธีการเข้ารหัสในไทม์โดเมน คือ PCM, ADPCM และ DM (Delta Modulation) ส่วนตัวอย่างของการเข้ารหัสในโดเมนความถี่คือ SBC (subband coding) ในส่วนต่อไปนี้จะกล่าวถึงตัวอย่างวิธีการเข้ารหัสแบบ waveform coders บางประเภทที่น่าสนใจ

5.2.1 การเข้ารหัสเสียงแบบ DPCM (Differential Pulse Code Modulation)

วิธีการ DPCM หรือ Differential Pulse Code Modulation เป็นวิธีที่ปรับปรุงและพัฒนามาจากวิธีการเข้ารหัส PCM ที่มีการใช้งานอย่างแพร่หลายในปัจจุบัน หลักการของวิธี DPCM อาศัยคุณสมบัติเฉพาะอย่างหนึ่งของสัญญาณเสียงตรงที่ระดับของสัญญาณเสียงโดยทั่วไปแล้วมักจะมีความต่อเนื่อง ไม่เปลี่ยนแปลงอย่างฉับพลันบ่อยครั้งนัก ดังนั้นแทนที่จะควอนไทซ์ระดับของสัญญาณจริงโดยตรงดังที่วิธี PCM ใช้อยู่ ก็จะนำเฉพาะผลต่างของสัญญาณในปัจจุบันเทียบกับสัญญาณก่อนหน้ามาทำการควอนไทซ์แทน ซึ่งโดยปกติแล้วช่วงของความแตกต่างจะมีขนาดเล็กกว่าช่วงของระดับสัญญาณ ด้วยเหตุนี้เราสามารถเข้ารหัสสัญญาณเสียงด้วยจำนวนบิตที่น้อยลงกว่าวิธี PCM

5.2.2 การเข้ารหัสเสียงแบบ ADPCM (Adaptive Differential PCM)

จากหลักการของวิธีการเข้ารหัสแบบ DPCM เราสามารถที่จะเพิ่มประสิทธิภาพของการเข้ารหัสให้สูงขึ้นได้อีก โดยการเพิ่มวงจรทำนายขนาดของสัญญาณล่วงหน้า นั่นคือแทนที่จะส่งค่าระดับความแตกต่างของสัญญาณที่เวลา t กับที่เวลา t-1 ก็จะใช้ค่าของสัญญาณที่เวลา t-1, t2.....t-d มาใช้ในการทำนายว่าค่าของสัญญาณที่เวลา t มีขนาดเป็นเท่าใด โดยค่าของ d นั้นขึ้นอยู่กับอันดับ (order) ของวงจรทำนายที่ใช้ ถ้า d มีค่าใหญ่ก็หมายความว่าจะใช้ค่าในอดีตเพียงไม่กี่ค่ามาใช้ในการทำนาย ในกรณีที่ d=1 ก็คือการใช้ค่าก่อนเวลาปัจจุบันเพียงค่าเดียวซึ่งก็คือ DPCM นั่นเอง จากนั้นก็จะจะส่งเฉพาะความแตกต่างของสัญญาณที่ทำนายนี้ กับระดับของสัญญาณจริง ซึ่งจากคุณสมบัติของเสียงที่ระดับของสัญญาณที่อยู่ช่วงเวลาใกลๆ กันมักจะมีความสัมพันธ์ระหว่างกัน จึงทำให้เราสามารถที่จะทำนายค่าของสัญญาณปัจจุบันจากค่าในอดีตได้ใกล้เคียงกับค่าจริงได้ดีพอสมควร ด้วยเหตุนี้จึงช่วยลดจำนวนบิตที่ต้องใช้ในการเข้ารหัสต่อสัญญาณหนึ่งแซมเปิล (Bit/Sample) ลงได้อีกเมื่อเทียบกับการเข้ารหัสแบบ DPCM

5.2.3 การเข้ารหัสเสียงแบบ SBC (Subband Coding)

การเข้ารหัสสัญญาณเสียงแบบ SBC หรือ Subband Coding จะแบ่งสเปกตรัมของสัญญาณเสียงออกแถบความถี่จำนวน 4 หรือ 8 ช่วง โดยอาศัยวงจรกรองความถี่จำนวน 4 หรือ 8 ชุดตามลำดับ ขนาดความกว้างของแถบความถี่แต่ละช่วงอาจจะกำหนดให้มีขนาดเท่ากันทั้งหมดหรือไม่ก็ได้ จากนั้นนำสัญญาณเสียงในแต่ละแถบความถี่เหล่านี้ไปแซมเปิลด้วยอัตราไนควิสต์ (Nyquist rate) สังเกตุว่าอัตราการแซมเปิลของแต่ละแถบความถี่ที่ต้องใช้โดยปกติจะมีขนาดต่ำกว่าอัตราที่ต้องใช้ในกรณีที่มิได้มีการแบ่งสเปกตรัมความถี่ของสัญญาณเสียงออกเป็นช่วงๆเลย นำสัญญาณที่ได้จากการแซมเปิลของแต่ละแถบความถี่มาทำการควอนไทซ์ ทั้งนี้ระดับความละเอียดนั้นให้พิจารณาจากความไวของหูคนฟังที่มีต่อระดับความเพี้ยนของเสียงที่เกิดขึ้นจากการทำควอนไทเซชั่นสำหรับแถบความถี่นั้นๆ ซึ่งโดยปกติความไวต่อความเพี้ยนเนื่องจากความผิดพลาดของการทำควอนไทเซชั่นของหูมนุษย์ จะลดลงอย่างเอ็กโพเนชี่ยลเมื่อค่าความถี่ของสัญญาณมีขนาดสูงขึ้น ดังนั้น ที่ช่วงความถี่สูงจำนวนระดับของการทำควอนไทเซชันก็มักจะกำหนดให้มีความละเอียดที่น้อยลง อัตราบิตที่ต้องใช้ในการเข้ารหัสสัญญาณเสียงแบบ SBC โดยทั่วไปมีค่าอยู่ในช่วง 9.6 – 32 kbps และคุณภาพของเสียงที่ได้ก็ใกล้เคียงกับการเข้ารหัสสัญญาณเสียงแบบ ADPCM เมื่อกำหนดให้อัตราบิตที่ค่าเท่ากัน

5.3 วิธีการเข้ารหัสเสียงแบบ Parametric Coders (Vocoders)

Parametric coders หรือที่รู้จักกันในชื่อ vocoders เป็นวิธีการเข้ารหัสสัญญาณเสียงที่อาศัยการจำลองกลไกและกระบวนการสร้างสัญญาณเสียงของแหล่งกำเหนิดเสียง ดังนั้นวิธีนี้จะไม่

สนใจถึงรูปร่างของสัญญาณเสียงเลยหากแต่จะพยายามเน้นวิธีการสังเคราะห์สัญญาณเสียงให้ใกล้เคียงกับวิธีการสร้างเสียงของมนุษย์มากที่สุด ในการจำลองแหล่งกำเนิดของสัญญาณนั้นมีได้หลายวิธีเช่น channel vocoder ,formant vocoder และ linear predictive coder (LPC) แต่วิธีที่ได้รับความสนใจมากที่สุดคือวิธีการจำลองแบบ LPC ซึ่งเราจะกล่าวถึงต่อไปในบทนี้ vocoders มีประโยชน์ต่อการนำมาใช้งานในวงการทหารเป็นหลัก แต่มิได้มีการนำมาใช้งานในระบบโทรศัพท์เคลื่อนที่เนื่องจากคุณภาพของเสียงที่ได้ยังไม่อยู่ในระดับที่ดีพอ เพราะผู้ฟังจะสามารถบอกได้ว่าเสียงที่ได้นั้นเป็นเสียงที่เกิดจากการสังเคราะห์และไม่เป็นธรรมชาติ

5.3.1 การเข้ารหัสเสียงแบบ LPC (Linear-Predictive Coding)

Linear Predictive Coder (LPC) เป็นวิธีการเข้ารหัสประเภทหนึ่งของการเข้ารหัสแบบ vocoder ที่ได้รับความสนใจมากเป็นพิเศษ เพราะสามารถจำลองหารทำงานของแหล่งกำเนิดเสียงได้อย่างมีคุณภาพที่ดีกว่าวิธีการเข้ารหัส vocoders ประเภทอื่น เช่น formant vocoder หลักการเข้ารหัสเสียงแบบ LCR คือจะแบ่งสัญญาณเสียงออกเป็นช่วงสั้นๆ ช่วงละประมาณ 5 – 30 ms แล้วทำการวิเคราะห์สัญญาณ เพื่อหาองค์ประกอบและค่าพารามิเตอร์ต่างๆของสัญญาณเสียงในช่วงเวลานั้นๆ

องค์ประกอบหรือค่าพารามิเตอร์เหล่านี้จะถูกส่งผ่านช่องสัญญาณสื่อสารไปที่ภาครับเพื่อทำการสังเคราะห์สัญญาณเสียงกลับคืนมา ค่าพารามิเตอร์ตัวแรกก็คือชนิดของเอ็กซ์ไซเทชันซึ่งใช้สำหรับบ่งบอกว่าสัญญาณเสียงในช่วงนี้เป็นประเภท voiced หรือ unvoiced เพื่อที่ภาคสร้างสัญญาณเสียงจะได้เลือกแหล่งกำเนิด สัญญาณให้ถูกประเภท และในกรณีที่เป็นสัญญาณแบบ voiced ก็ต้องทำการส่งคาบของพิตช์ไปด้วยเพื่อใช้ควบคุมความยาวคาบของสัญญาณเอกซ์ไซเทชัน ค่าพารามิเตอร์อีกตัวหนึ่งคือค่าอัตราขยาย ซึ่งใช้สำหรับควบคุมพลังงานของสัญญาณเอกซ์ไซเทชัน จากนั้นสัญญาณนี้ก็จะส่งเข้าวงจรที่ใช้สำหรับจำลองการทำงานของช่องกำเนิดสัญญาณเสียงหรือที่เรียกว่า vocal tract ซึ่งในการจำลองนั้นจะใช้จำนวนสัมประสิทธิ์ของ LPC ทั้งหมดประมาณ 10 – 15 ตัว

5.4 วิธีการเข้ารหัสเสียงแบบ Hybrid Coders

Hybrid coders เป็นวิธีการเข้ารหัสสัญญาณเสียงที่รวมเอาเทคนิควิธีการเข้ารหัสสัญญาณเสียง 2 แบบคือ waveform coders และ parametric coders เข้าด้วยกัน นั่นคือมีการทำ LPC เหมือนกับวิธี parametric coders และก็มีการใช้วิธีการจาก waveform coders มาช่วยในการเข้ารหัสสัญญาณส่วนที่เหลือ ตัวอย่างของวงจรเข้ารหัสแบบ hybrid coders คือ MPE-LPC, CELP, RELP, VSELP และ RPE-LTP ซึ่งจะกล่าวถึงวิธีการเข้ารหัสแต่ละประเภทพอสังเขป

5.4.1 การเข้ารหัสเสียงแบบ Multi-pulse Excited LPC

จากการศึกษาที่ผ่านมาพบว่าการใช้แหล่งกำเนิดสัญญาณเอกซ์ไซเทชันที่มีเพียงหนึ่งพัลส์ในทุกๆคาบของหนึ่งพิตช์จะไม่สามารถจำลองแหล่งกำเนิดเสียงได้อย่างมีคุณภาพ ด้วยเหตุนี้จึงได้มีผู้เสนอแนวความคิดใหม่โดยให้ใช้พัลส์มากกว่าหนึ่งพัลส์ในแต่ละคาบ ซึ่งโดยทั่วไปแล้วจะใช้ค่า 8 พัลส์ต่อหนึ่งคาบจากนั้นก็จะทำการเลือกขนาดและปรับตำแหน่งที่เหมาะสมของพัลส์เหล่านั้นเพื่อให้ได้สัญญาณเสียงที่มีความเพี้ยนน้อยที่สุด วิธีการนี้มีชื่อเรียกว่า Multi-pulse excited LPC หรือ MPE-LPC วิธีการนี้มีข้อดีตรงที่ไม่ต้องมีการคำนวณหาค่าของช่วงเวลาพิตช์และสัญญาณเสียงที่ได้จากการเข้ารหัสก็มีคุณภาพที่ดีกว่าการเข้ารหัสแบบ LPC

5.4.2 การเข้ารหัสเสียงแบบ CELP (Code-Book Excited Linear Prediction)

สำหรับวิธีการเข้ารหัสแบบ CELP นี้จะประกอบด้วยชุดสัญญาณเอกซ์ไซเทชันที่มีรูปแบบตายตัวจำนวนหนึ่งที่เรียกว่า code book โดยที่สัญญาณเอกซ์ไซเทชันเหล่านี้จะมีคุณลักษณะการกระจายเป็นแบบเกาส์ที่มีค่าเฉลี่ยเป็นศูนย์ ที่ภาคเข้ารหัสสัญญาณจะทำการค้นหาและเลือกสัญญาณเอกซ์ไซเทชันชุดที่เหมาะสมที่สุดสำหรับสัญญาณเสียงในแต่ละช่วงเวลาคือให้ได้คุณภาพเสียงที่ดีที่สุด จากนั้นภาคส่งก็จะทำการส่งดัชนีที่บ่งบอกถึงชุดสัญญาณเอกซ์ไซเทชันไปพร้อมๆกันกับชุดสัมประสิทธิ์ LPC ณ ที่ภาครับก็จะเลือกชุดสัญญาณเอกซ์ไซเทชันที่ภาคส่งระบุมาแล้วส่งผ่านวงจรฟิลเตอร์ LPC สำหรับทำการสังเคราะห์เสียงต่อไป การเข้ารหัสในลักษณะนี้จะใช้อัตราบิตของการเข้ารหัสที่ไม่สูงนักเช่นเพียง 4.8 Kbps แต่สามารถให้คุณภาพของสัญญาณเสียงในระดับที่ดีได้

ยกตัวอย่างเช่น ถ้าทำการแบ่งสัญญาณเสียงออกเป็นบล็อกๆ ที่มีขนาดบล็อกละ 5 ms มาทำการเข้ารหัส โดยใช้อัตราความถี่ของการลสุ่มสัญญาณที่ 8 KHz ในช่วงเวลาหนึ่งบล็อกจะมีแซมเปิลทั้งหมด 40 แซมเปิล หากเราใช้อัตราบิตสำหรับเข้ารหัสเฉพาะในส่วนของเอกซ์ไซเทชันเท่ากับ ¼ bit/sample จะได้ว่ามีบิตให้ใช้เพียง 10 บิตต่อสัญญาณเสียงหนึ่งบล็อก บิตจำนวน 10 บิตสามารถนำมาใช้เป็นดัชนีของชุดเอกซ์ไซเทชันที่แตกต่างกันได้ทั้งหมด $2^{10} = 1024$ ชุด เพราะฉะนั้นอัตราบิตที่ใช้สำหรับบ่งชี้ชุดเอกซ์ไซเทชันมีค่าเท่ากับ 10 bits/5 ms = 2 Kbps

ปัญหาที่สำคัญของวิธีการเข้ารหัสแบบนี้คือความซับซ้อนและเวลาที่ต้องใช้ในการค้นหาชุดสัญญาณเอกซ์ไซเทชันที่เหมาะสมจาก code book เนื่องจากคุณภาพของเสียงที่ได้ขึ้นอยู่กับจำนวนชุดสัญญาณเอกซ์ไซเทชันที่มีไว้ให้เลือกใช้ ดังนั้นการที่มีจำนวนชุดสัญญาณเอกซ์ไซเทชันมากขึ้น ก็ทำให้การค้นหาชุดสัญญาณเอกซ์ไซเทชันที่เหมาะสมต้องใช้เวลานานขึ้น ด้วยเหตุนี้งานวิจัยและพัฒนาในช่วงต่อมาของการเข้ารหัสประเภทนี้จึงมุ่งเน้นไปที่การค้นคว้าหาแนวทางหรือวิธีการเลือกชุดสัญญาณเอกซ์ไซเทชันที่เหมาะสมให้ได้รวดเร็ว

5.5 การวัดคุณภาพเสียง

โดยทั่วไปแล้วในการวัดคุณภาพของเสียงจำเป็นต้องวัดจากความรู้สึกของผู้ฟังต่อสัญญาณเสียงที่กำลังทดสอบอยู่โดยตรงเลย ซึ่งวิธีการทดสอบนี้มีชื่อเรียกว่า Subjective Test ซึ่งเป็นการทดสอบตามมาตรฐานของ ITU เช่น นำค่าเฉลี่ยที่ได้ไปใช้ ซึ่งมีชื่อเรียกว่า Mean Opinion Score (MOS) [5] ในระบบที่ใช้งานแต่ละระบบมีความต้องการคุณภาพของเสียง หรือค่า MOS ที่แตกต่างกันไป ซึ่งเราสามารถสรุปค่า MOS ที่เหมาะสมกับการใช้งานต่างๆ ได้ดังที่แสดงไว้ในตารางที่ 5.1

ตารางที่ 5.1 ค่า MOS ที่เหมาะสมกับการใช้งานในระบบต่างๆ

MOS	การใช้งาน
4.5 – 5.0	Broadcast Quality
4.0 – 4.5	Network or "Toll" Quality
3.5 – 4.0	Communication Quality
2.5 – 3.5	Synthetic Quality

5.6 การเปรียบเทียบคุณภาพเสียงของวิธีการเข้ารหัสแบบต่างๆ

จากตารางที่ 5.2 แสดงให้เห็นการเปรียบเทียบคุณภาพของเสียงที่ได้จากการเข้ารหัสด้วยวิธีการต่างๆ โดยวัดจากค่า MOS จะเห็นได้ว่า PCM ให้คุณภาพเสียงที่ดีที่สุดโดยได้คะแนน MOS อยู่ระหว่าง 4.1 ถึง 4.3 แต่การเข้ารหัสแบบ PCM นี้ต้องการอัตราบิตที่สูงสุดด้วยนั้นคือ 64 Kbps ส่วนการเข้ารหัสแบบ ADPCM นั้นสามารถลดอัตราบิตลดลงได้ถึงครึ่งหนึ่งคือ 32 Kbps โดยที่คุณภาพของเสียงยังคงใกล้เคียงกับการเข้ารหัสแบบ PCM นอกจากนี้ความซับซ้อนของการเข้ารหัสก็เพิ่มขึ้นไม่มากนัก

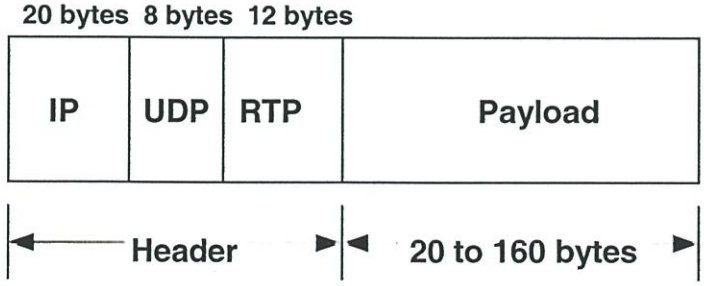
ตารางที่ 5.2 การเปรียบเทียบอัตราบิต MOS ของวิธีการเข้ารหัสสัญญาณเสียง

วิธีการเข้ารหัส	อัตราบิต (Kbps)	MOS Score
เสียงปกติตามธรรมชาติ	-	4.5
G.711 PCM	64	4.1
G726 ADPCM	32	3.85
G.728 LD-CELP	16	3.61
G.729 CS-ACELP	8	3.92
G.729 x2 Encodings	8	3.27
G.729 x3 Encodings	8	2.68
G.729a CS-ACELP	8	3.7
G.723.1 MP-MLQ	6.3	3.9
G.723.1 ACELP	5.3	3.65

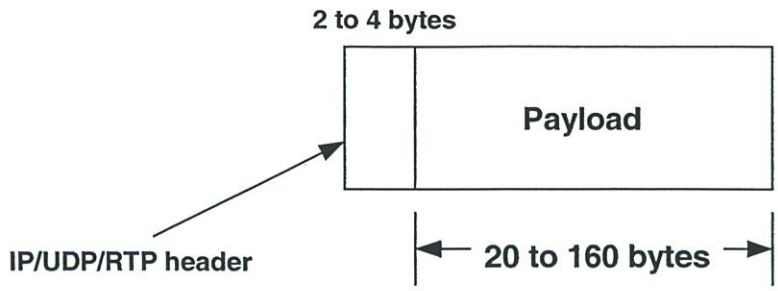
5.7 การบีบอัดข้อมูลส่วนหัวแบบ RTP

Real-Time Transport Protocol (RTP) [5] ใช้สำหรับนำพา Packet traffic ของเสียงบนเครือข่าย IP การบีบอัด ส่วนหัวของ RTP บีบอัด ส่วนหัว IP/UDP/RTP ใน RTP packet ของข้อมูลจาก 40 ไบท์ ไปเป็นประมาณ 2 – 4 ไบท์ ดังแสดงในรูป คุณสมบัติการบีบอัดจะเป็นประโยชน์ถ้าใช้ Voice over IP บน links ที่ช้า ใช้การบีบอัดบนสุดท้ายของแบนวิทด์ต่ำ สามารถที่ลด overhead ของเครือข่ายถ้ามี RTP traffic บน link ช้า

เป็นธรรมดา RTP packet จะมี payload โดยประมาณ 20 ถึง 160 bytes สำหรับ แอปลิเคชั่นของเสียงที่ใช้การบีบอัดที่ payload การบีบอัดส่วนหัวของ RTP เป็นผลดีเมื่อ ขนาดของ payload ของ RTP เล็กลง (ตามตัวอย่าง การบีบอัด payload ของเสียงระหว่าง 20 ถึง 50 bytes)



ภาพที่ 5.2 รูปแบบของ Frame ก่อนที่จะทำการบีบอัดส่วนหัวของ RTP

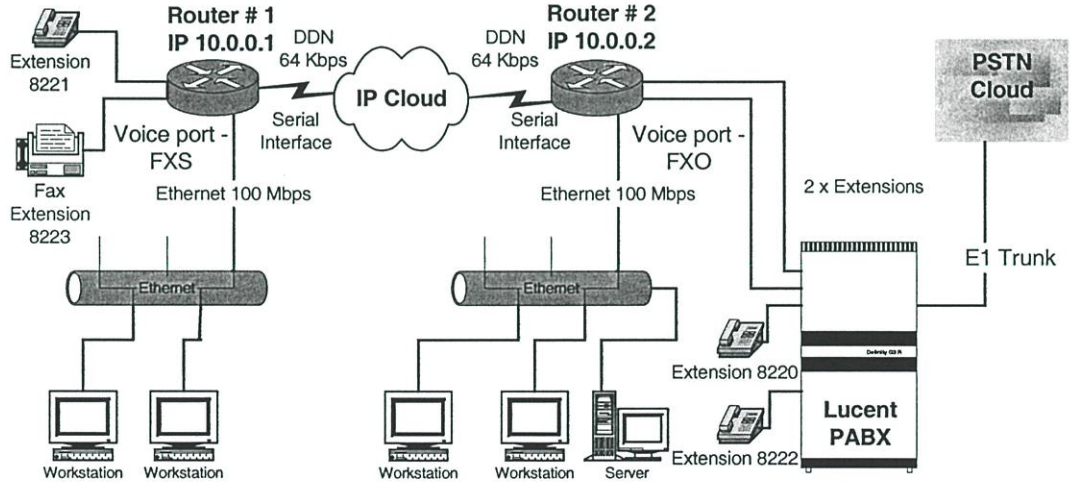


ภาพที่ 5.3 รูปแบบของ Frame หลังจากที่ทำการบีบอัดส่วนหัวของ RTP

บทที่ 6
แบบจำลองการทดสอบการส่งผ่าน Voice บนเครือข่าย IP

6.1 รูปแบบการเชื่อมโยงอุปกรณ์ที่ใช้ในการทดสอบ

จากคุณสมบัติของอุปกรณ์เครือข่ายที่มีเทคโนโลยีที่ทันสมัยมากขึ้น และสามารถสนับสนุนการใช้งานด้านข้อมูลเสียง (Voice Traffic) และจากความต้องการใช้งานเกี่ยวกับ Voice เพิ่มสูงขึ้นจึงทำให้ผู้เขียนวิทยานิพนธ์มุ่งเน้นที่จะทำการเพิ่มประสิทธิภาพของเครือข่าย โดยทำการจำลองและการทดสอบการส่งผ่าน Voice Traffic ไปบนเครือข่าย IP โดยยังคงการใช้งานของข้อมูลคอมพิวเตอร์ แอพพลิเคชั่นต่างๆ อยู่อย่างเดิม ทั้ง แอพพลิเคชั่นระบบ Retail banking, Lotus Note Mail และ Web Server โครงสร้างของรูปแบบจำลอง นั้นอ้างอิงกับระบบงานและอุปกรณ์ที่มีอยู่เดิม แต่เพิ่มประสิทธิภาพของการใช้งานของ Voice เข้าไป ซึ่งอุปกรณ์ที่นำมาทดสอบ คือ CISCO Router รุ่น 2600 [1] โดยการทดสอบครั้งนี้มุ่งวิเคราะห์การรองรับ และสนับสนุนการส่งผ่าน Voice Traffic ไปบนเครือข่าย โดยกำหนดรูปแบบจำลองดังภาพที่ 6.1



ภาพที่ 6.1 การจำลองการทดสอบการเชื่อมต่อระบบโทรศัพท์ส่งผ่านระบบเครือข่าย IP

ทำการกำหนดรูปแบบของแบบจำลองการทดสอบ โดยการเชื่อมโยงระหว่างอุปกรณ์ Router ที่สนับสนุนการทำงานของ Voice ด้วยกัน จำนวน 2 Units แบบ point-to-point โดยเชื่อมโยง Router ตัวที่ 1 ไปยัง Router ตัวที่ 2 โดยใช้สายสัญญาณมาตรฐาน V.35 แบบ DCE (V.35/DCE) และสายสัญญาณ V.35 แบบ DTE (V.35/DTE) ต่อที่ Interface Serial port 1/0 ของ

Router ทั้ง 2 จากนั้นทำการเชื่อมโยงสาย Interface V.35/DCE เข้ากับ Interface V.35/DTE สำหรับอุปกรณ์ Router ตัวที่ 2 ซึ่งมี Voice Interface ชนิด Foreign Exchange Office (FXO) อยู่จำนวน 2 Ports นั้น ทำการเชื่อมโยงสาย Voice Interface ไปยังระบบโทรศัพท์ตู้สาขาอัตโนมัติ (PABX) ที่มีสัญญาณโทรศัพท์สายภายในชนิด Analog จำนวน 2 เลขหมาย และทำการเชื่อมโยงสายชนิด Unshield Twisted Pair (UTP) จาก Interface Ethernet ที่ Router ตัวที่ 2 ไปยังอุปกรณ์คอมพิวเตอร์ Workstation และ Server เพื่อใช้งานในการส่งผ่านข้อมูล เช่น Lotus Note Mail เป็นต้น สำหรับอุปกรณ์ทดสอบ Router ตัวที่ 1 นั้น ทำการเชื่อมโยงสายสัญญาณโทรศัพท์จาก Voice Port ที่ 1/0/0 ซึ่งเป็นชนิด Foreign Exchange Station (FXS) [1] ของอุปกรณ์ Router ตัวที่ 1 ไปยังเครื่องโทรศัพท์ และจาก Voice Port ที่ 1/0/1 ไปยังเครื่องโทรสาร ส่วน Ethernet Interface นั้น ทำการเชื่อมสาย UTP จาก Router ตัวที่ 1 ไปยัง HUB/Switch เพื่อให้ สามารถต่อเครื่องคอมพิวเตอร์ให้ใช้งานได้หลายเครื่องพร้อมๆ กัน

กำหนด Function Configuring ของ Router ตัวที่ 1 และตัวที่ 2 โดยใช้ความเร็วในการเชื่อมโยงระหว่าง Router ซึ่งเป็นการเชื่อมต่อระบบเครือข่ายแบบ WAN ไว้ที่ 64 Kbps โดยใช้โพรโตคอล IP ในการเชื่อมต่อเครือข่าย กำหนดค่าพารามิเตอร์ให้กับ port ที่เชื่อมโยงระหว่าง Router จากนั้นทำการกำหนด IP Address ที่ Router ตัวที่ 1 เป็น 10.0.0.1 และ Router ตัวที่ 2 เป็น 10.0.0.2 ทำการกำหนด Configuration ของ Voice port ที่อุปกรณ์ Router ทั้ง 2 Units และนำอุปกรณ์วิเคราะห์ข้อมูล (Protocol Analyzer) มาเชื่อมต่อแบบคู่ขนานระหว่างการเชื่อมโยงของ Serial port เพื่อทำการตรวจจับข้อมูลระหว่างการทดลอง

ทำการทดลองส่งข้อมูลผ่านเครือข่ายโดยการเรียกใช้แอพพลิเคชั่น Lotus Note Mail และในขณะเดียวกันทำการยกหูโทรศัพท์ ด้าน Router ตัวที่ 1 หลังจากนั้นทำการวางโทรศัพท์ และทำการยกหูโทรศัพท์ใหม่ กดเลขหมายโทรศัพท์ปลายทาง คือ Extension หมายเลข 8220 และทำการรับสายที่หมายเลข Extension 8220 และทำการทดสอบเสียงจากการพูด จากนั้นทำการวางสายที่ Extension 8220 ก่อน และทำการบันทึกผลการทดลอง

6.2 รายละเอียดและการกำหนดพารามิเตอร์

จากรูปแบบการเชื่อมโยงที่ใช้ในการทดสอบ มีการกำหนดพารามิเตอร์ต่างๆเป็นดังต่อไปนี้

ตารางที่ 6.1 ค่าพารามิเตอร์ในการเชื่อมโยงระหว่าง Router#1 และ Router#2

Router#1	Router#2
interface Serial0/0	interface Serial0/0
description Router#1	description Router#2
bandwidth 64	bandwidth 64
ip address 10.0.0.1 255.255.255.0	ip address 10.0.0.2 255.255.255.0
encapsulation HDLC	encapsulation HDLC
interface FastEthernet0/0	interface FastEthernet0/0
router ospf 1	router ospf 1
network 10.0.0.0 0.0.0.255 area 2	network 10.0.0.0 0.0.0.255 area 2

ตารางที่ 6.2 ค่าพารามิเตอร์ของ Voice บนอุปกรณ์ Router ทั้ง 2 ตัว

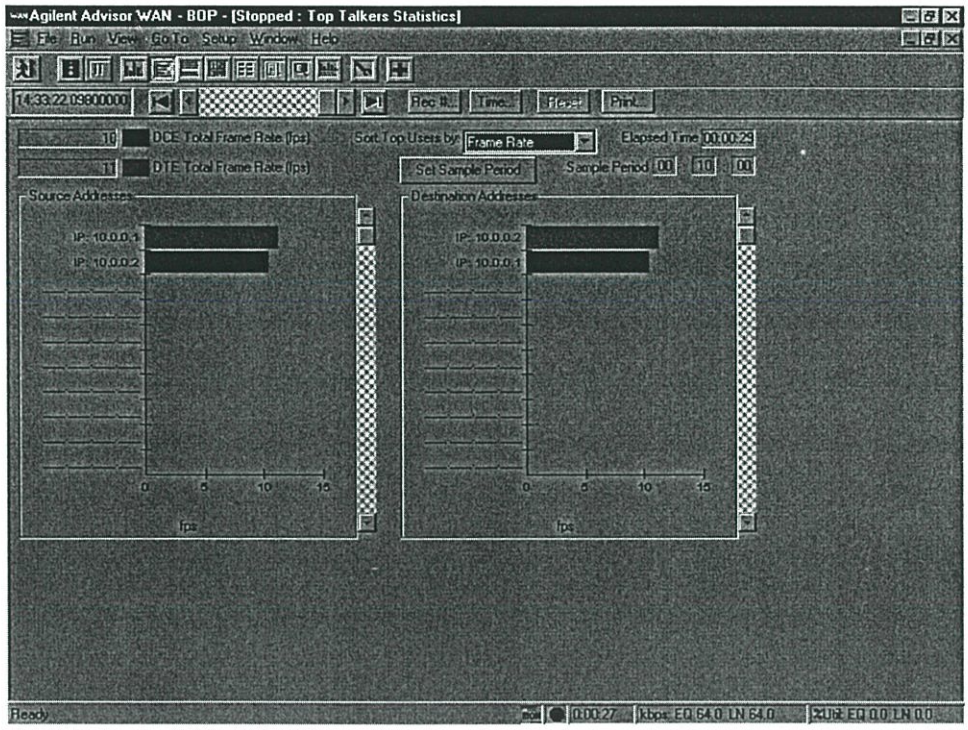
Router#1	Router#2
voice-port 1/0/0	voice-port 1/0/0
connection plar 9	connection plar 9
voice-port 1/0/1	voice-port 1/0/1
connection plar 9	connection plar 9
dial-peer cor custom	dial-peer cor custom
dial-peer voice 101 pots	dial-peer voice 101 pots
destination-pattern 9	destination-pattern 9
port 1/0/0	port 1/0/0
dial-peer voice 102 pots	dial-peer voice 102 pots
destination-pattern 9	destination-pattern 9
port 1/0/1	port 1/0/1
dial-peer voice 501 voip	dial-peer voice 501 voip
destination-pattern 9	destination-pattern 9
session target ipv4 ip 10.0.0.2	session target ipv4 ip 10.0.0.1

ตารางที่ 6.3 ค่าพารามิเตอร์ของ Voice บนอุปกรณ์ Router ที่ทำการบีบอัดข้อมูล

Router#1	Router#2
codec g729br8 bytes 30	codec g729br8 bytes 30
dial-peer voice 502 voip	dial-peer voice 502 voip
destination-pattern 9	destination-pattern 9
session target ipv4 ip 10.0.0.2	session target ipv4 ip 10.0.0.1
codec g729br8 bytes 30	codec g729br8 bytes 30

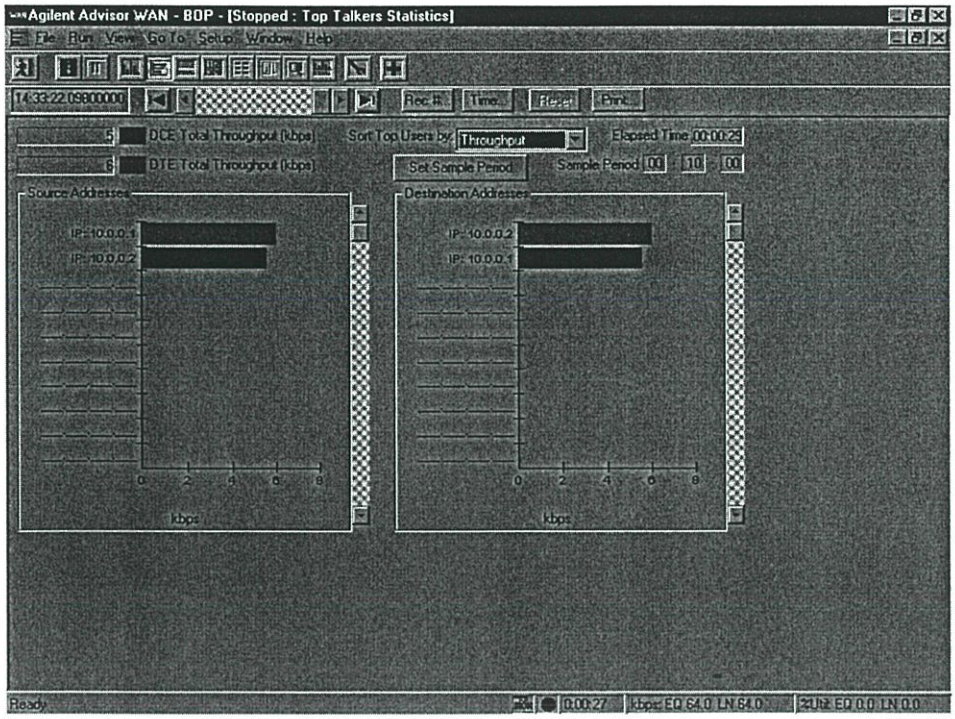
6.3 ผลการทดลองตามแบบจำลอง

จากการทดลองตามแบบจำลองเพื่อให้การส่งผ่าน Voice ไปบนเครือข่าย IP นั้น พบว่าหากทำการเชื่อมโยงเครือข่าย แบบ IP แล้วทำการกำหนดพารามิเตอร์ที่รองรับการส่งผ่าน Voice สามารถทำได้ ซึ่งข้อมูลที่เป็น แอพพลิเคชั่นเดิมสามารถใช้งานได้เป็นปกติ สามารถทำงานได้ไปพร้อมๆกัน แต่เมื่อทำการกำหนดพารามิเตอร์ใหม่ที่มีขบวนการบีบอัดข้อมูลไป เราสามารถเห็นการเปลี่ยนแปลงของ Instantaneous Utilization และปริมาณของ Voice Frames บนเครือข่ายที่ใช้โพรโตคอล IP และใช้คุณสมบัติของ Voice over IP ทำการส่งผ่านข้อมูลเสียงไปในเครือข่าย IP โดยใช้วิธีการบีบอัด เพื่อลด Header ของปริมาณเสียงที่ส่งผ่านไปในเครือข่าย ทำให้ปริมาณ ของ Instantaneous Utilization (%) นั้นลดลงเกือบ 20 % จึงทำให้การส่งผ่านข้อมูลปกติในเครือข่ายและส่งผ่านสัญญาณเสียงในเครือข่ายส่วนตัวสามารถทำได้อย่างมีประสิทธิภาพ ซึ่งแสดงในผลจากการนำอุปกรณ์ Protocol Analyzer มาทำการตรวจวัด ปริมาณของการส่งผ่านข้อมูลข้ามเครือข่ายโดยใช้อุปกรณ์ทดลอง Router ทั้ง 2 ตัว



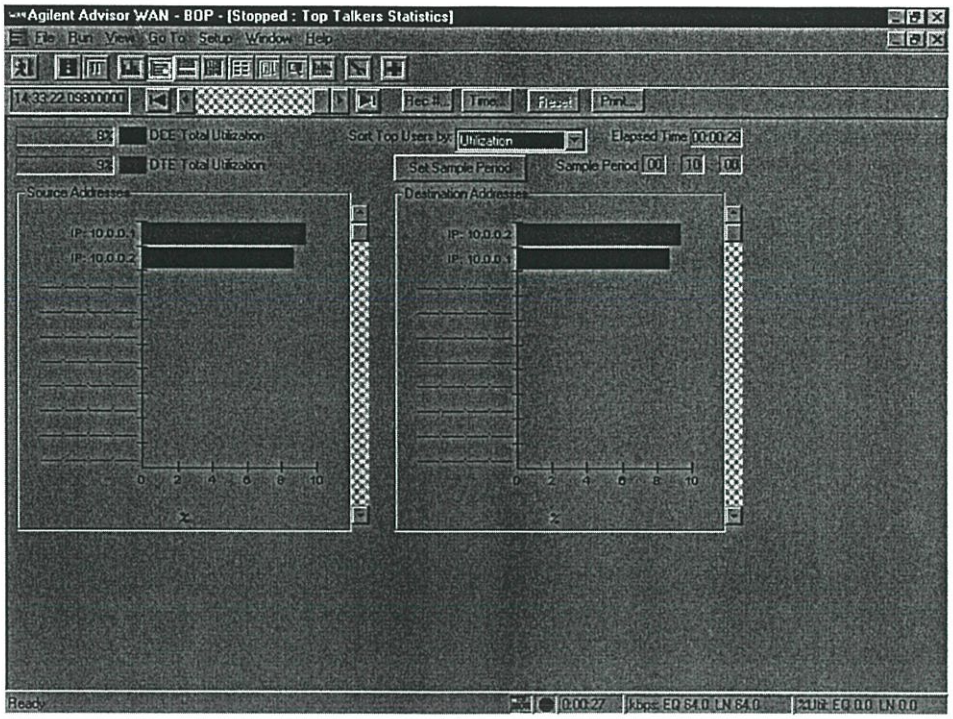
ภาพที่ 6.1 ปริมาณของ Voice Frame ในการส่งผ่านเครือข่าย IP

จากภาพที่ 6.1 แสดงให้เห็นถึงปริมาณของ Voice Frame ที่ต้นทางและปลายทาง อยู่ที่ 10 – 11 Frame per Second

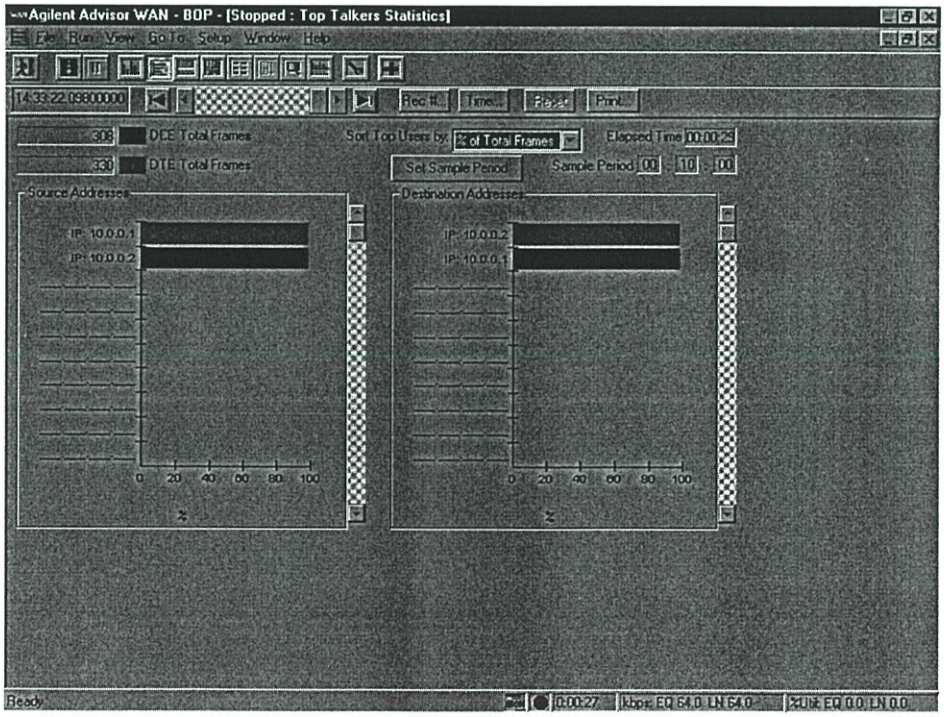


ภาพที่ 6.2 ปริมาณของ Voice Throughput

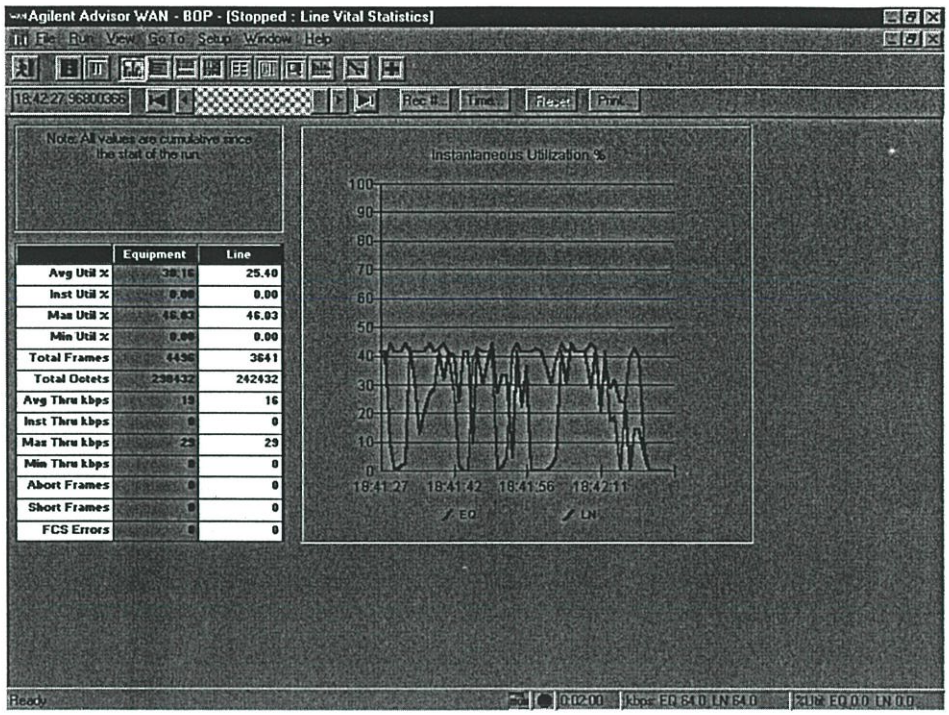
จากภาพที่ 6.2 จะเห็นปริมาณ Voice Throughput ที่ส่งผ่านไปในเครือข่ายจากต้นทางไปยังปลายทางเป็นจำนวน 5-6 Kbps



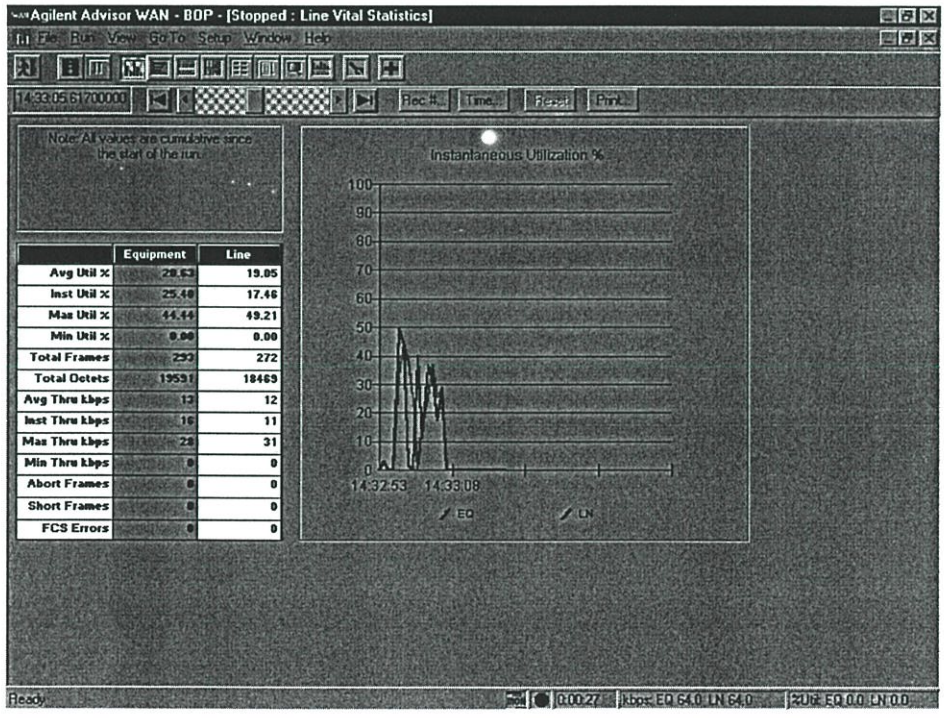
ภาพที่ 6.3 ปริมาณของ Utilization (%)



ภาพที่ 6.4 ปริมาณของ Total Frames (%)



ภาพที่ 6.5 ปริมาณของ Instantaneous Utilization (%) ก่อนที่จะทำการบีบอัด



ภาพที่ 6.6 ปริมาณของ Instantaneous Utilization (%) หลังจากที่ทำการบีบอัด

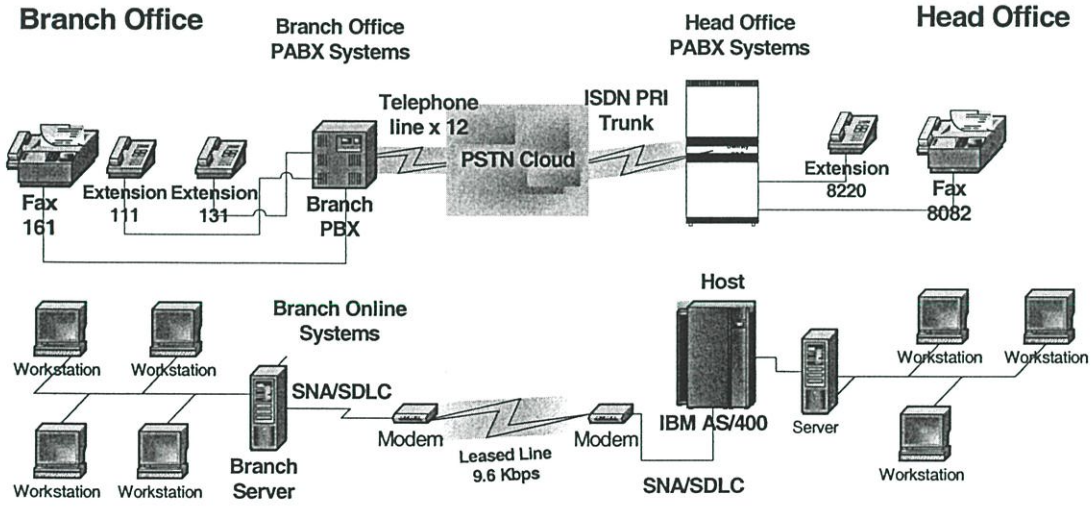
จากภาพที่ 6.5 จะเห็นว่า Maximum Utilization จะอยู่ที่ 46.03 % และค่า Average Utilization จะอยู่ที่ 30.16 % ส่วนค่า Average Throughput จะอยู่ที่ 19 Kbps และหากทำการบีบอัด

แล้วจะได้ผลดังภาพที่ 6.6 ดังนี้ ค่า Maximum Utilization จะอยู่ที่ 44.44 % และค่า Average Utilization จะอยู่ที่ 20.63 % ส่วนค่า Average Throughput จะอยู่ที่ 13 Kbps ซึ่งแสดงให้เห็นว่าหากทำการบีบอัดข้อมูลแล้วจะทำให้ Utilization จะลดลงทำให้ปริมาณข้อมูลที่ส่งผ่านในเครือข่ายไม่เกิดการแออัดคับคั่งก็จะทำให้เครือข่ายมีประสิทธิภาพ

บทที่ 7
รูปแบบการนำมาประยุกต์ใช้งาน

7.1 รูปแบบระบบเครือข่ายข้อมูลส่วนตัว

ปัจจุบันองค์กรต่างๆทั้งภาครัฐบาลและภาคเอกชนได้มีการใช้ระบบเครือข่ายคอมพิวเตอร์ที่เรียกว่าระบบเครือข่าย LAN (Local Area Network) เพื่อใช้สื่อสารกันระหว่างหน่วยงานของตนเองภายในองค์กร และหากการสื่อสารระหว่างกันเกินขอบเขตของระบบ LAN ซึ่งเป็นการสื่อสารที่ห่างไกลกัน ก็จะใช้ระบบเครือข่ายคอมพิวเตอร์ที่เรียกว่า WAN (Wide Area Network) ซึ่งแต่ละองค์กรก็จะใช้เทคโนโลยีการสื่อสารระยะไกลต่างกันไป และในแต่ละองค์กรอาจจะมีงบประมาณที่มากและน้อยต่างกันไป ซึ่งการใช้เทคโนโลยีนั้นมีหลากหลายวิธีเช่น Packet Switching, Circuit Switching, SNA/SDLC, BSC, X.25 และอื่นๆ เป็นต้น ซึ่งอาจจะมีข้อแตกต่างกันไป ลักษณะการนำเทคโนโลยีการสื่อสารข้อมูลมาประยุกต์ใช้กับระบบงานขององค์กร ก็สามารถที่จะเลือกให้เหมาะสมกับขนาดขององค์กรและวัตถุประสงค์หลักขององค์กร



ภาพที่ 7.1 การเชื่อมต่อของระบบโทรศัพท์ และระบบเครือข่ายที่แยกออกจากกัน

ในวิทยานิพนธ์ฉบับนี้ ผู้เขียนได้เสนอรูปแบบในการนำเทคโนโลยีของ IP (Internet Protocol) มาประยุกต์ใช้งานร่วมกับระบบโทรศัพท์ และระบบเครือข่ายที่มีอยู่เดิมของธนาคารสแตนดาร์ดชาร์เตอร์ดนครธน จำกัด (มหาชน) ซึ่งเรียกได้ว่าการนำระบบโทรศัพท์ประยุกต์ร่วม ระบบเครือข่ายข้อมูลส่วนตัว ระบบเครือข่ายข้อมูลใช้ระบบการเชื่อมโยงวงจรเช่า

(Leased Line) โดยเช่าจากองค์การโทรศัพท์แห่งประเทศไทย และวิ่งผ่านด้วยความเร็ว (Speed) 14.4 Kbps โดยใช้อุปกรณ์ MUX Modem (TDM) V.24 เชื่อมโยงซึ่งกันและกันระหว่างสาขามายังศูนย์คอมพิวเตอร์ ที่สำนักงานใหญ่ ซึ่งข้อมูลของระบบทั้งหมดจะถูกส่งผ่านมาบนคู่สาย 2 Wire Leased Line เพียงคู่เดียว

จากภาพที่ 7.1 เป็นระบบโครงข่ายคอมพิวเตอร์ที่มีอยู่เดิมขององค์กร ซึ่งมีทั้งระบบ Local Area Network (LAN) ที่ใช้ติดต่อสื่อสารระหว่างหน่วยงานต่างๆ ภายในอาคารสำนักงานใหญ่ และมีระบบสื่อสารที่อยู่ห่างไกล Wide Area Network (WAN) เพื่อเชื่อมโยงระบบงานไปยังสำนักงานสาขาต่างๆ อยู่ในเขตนครหลวง ซึ่งมีอยู่ประมาณ 32 สาขา และสาขาในเขตต่างจังหวัด ซึ่งมีอยู่ประมาณ 8 สาขา โดยมีการให้บริการแก่ลูกค้าในระบบ Online ระหว่างสาขาต่างๆ กับสำนักงานใหญ่คือ

7.1.1 ระบบ Online Retail Banking เป็นระบบที่ให้บริการ ฝาก และถอนเงินที่เคาเตอร์ของธนาคาร

7.1.2 ระบบ Self Service เป็นระบบที่สามารถทำรายการบนเครื่องอัตโนมัติต่างๆ ของธนาคาร แบ่งออกเป็นสังเขปดังนี้

7.1.2.1 การให้บริการในระบบ ATM (Automatic Teller Machine) ซึ่งให้บริการฝากและถอนเงิน ตลอดจนชำระบัตรเครดิต

7.1.2.2 การให้บริการในระบบบัตรเครดิต

7.1.2.3 การให้บริการเครื่องรับฝากเงิน

7.1.2.4 การให้บริการเครื่องบันทึกรายการอัตโนมัติ (Cash Deposit Machine)

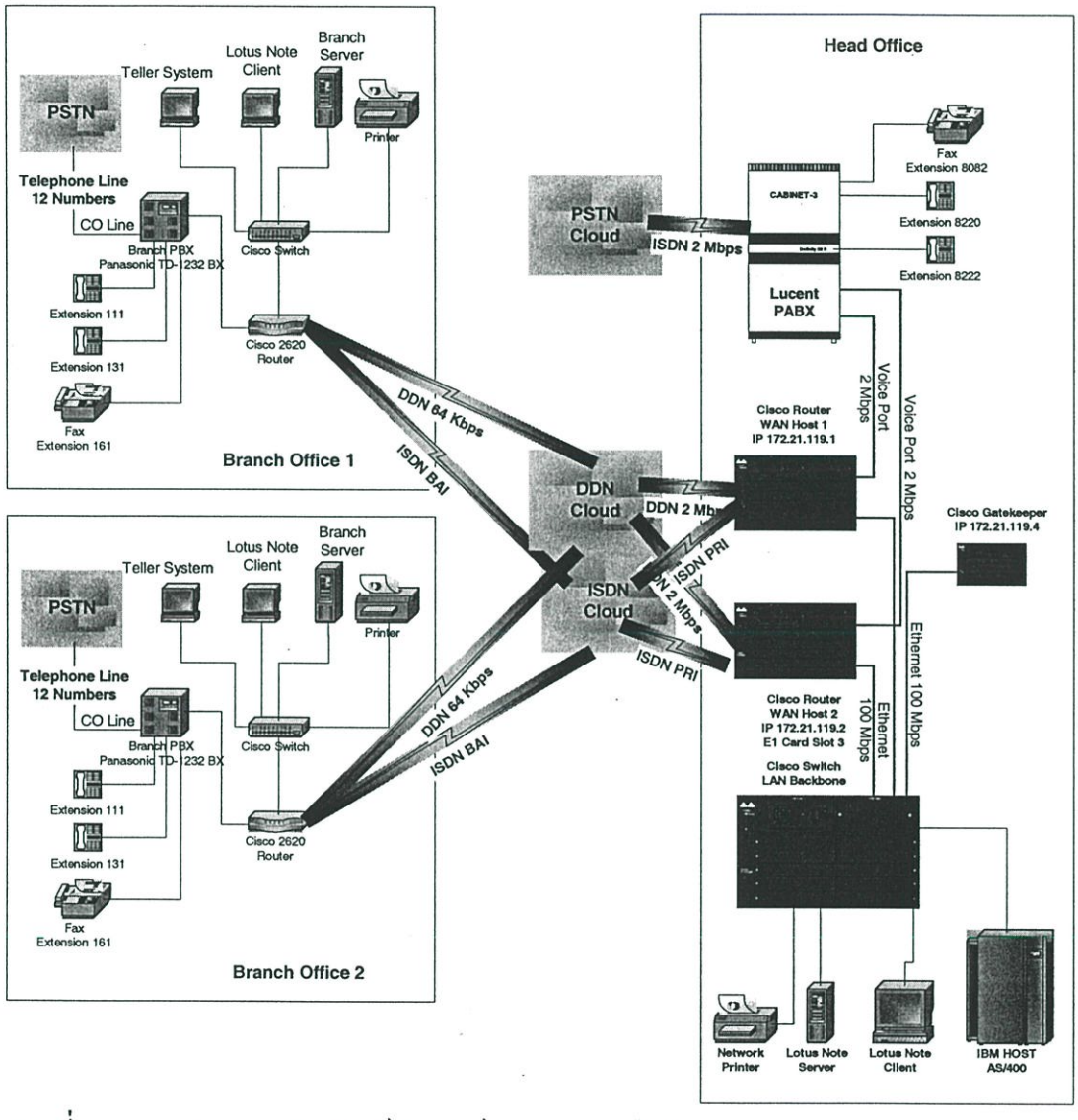
จากข้อมูลที่ได้กล่าวมาแล้วนั้น การให้บริการเป็นระบบ Online ดังนั้นจึงต้องมีระบบคอมพิวเตอร์และระบบโครงข่ายสื่อสารข้อมูล เพื่อใช้ในการติดต่อเชื่อมโยงและทำการส่งผ่านข้อมูลระหว่างสาขาต่างๆ ของธนาคาร กับศูนย์คอมพิวเตอร์ (Data Center) ที่สำนักงานใหญ่ ตลอดจนต้องมีระบบคอมพิวเตอร์ในการทำ Real Time Update Transaction

7.2 รูปแบบการนำระบบโทรศัพท์ ประยุกต์ร่วม ระบบเครือข่ายข้อมูลส่วนตัว

เนื่องจากระบบโทรศัพท์ตู้สาขาอัตโนมัติ (Private Automatic Branch Exchange : PABX) [4] ที่ธนาคารได้ใช้ที่อาคารสำนักงานใหญ่นั้นเป็นระบบโทรศัพท์ที่สามารถสนับสนุนการใช้งานได้หลากหลายกอปรกับความต้องการใช้งานด้านโทรศัพท์ของธนาคารนั้นมีเป็นจำนวนมาก และระบบโทรศัพท์ตู้สาขาอัตโนมัติ ที่ติดตั้งตามสาขาต่างๆของธนาคารนั้นเป็นระบบโทรศัพท์ตู้สาขาอัตโนมัติ ขนาดเล็ก มีจำนวนสายสัญญาณโทรศัพท์ที่ต่อเข้ามายังตู้สาขาอัตโนมัติ จำนวน 12 สาย และสายภายใน (Extension) จำนวน 24 สาย และเนื่องจากปริมาณการใช้โทรศัพท์ติดต่อระหว่างสาขาและสำนักงานใหญ่ และจากสาขาไปยังสาขามีปริมาณเพิ่มขึ้น ดังนั้นจึงทำให้ผู้เขียน

วิทยานิพนธ์จึงมีความสนใจที่จะศึกษาการใช้งานระบบโทรศัพท์ ร่วมกับระบบเครือข่ายข้อมูลส่วนตัว

รูปแบบในการนำระบบโทรศัพท์ ประยุกต์ร่วม ระบบเครือข่ายของธนาคาร สแตนดาร์ดชาร์เตอร์ดนครธน จำกัด(มหาชน) จะมีรายละเอียดดังภาพที่ 7.2



ภาพที่ 7.2 การนำระบบโทรศัพท์ประยุกต์ร่วม ระบบเครือข่ายของธนาคาร สแตนดาร์ดชาร์เตอร์ดนครธน จำกัด(มหาชน)

จากภาพที่ 7.2 เป็นการนำระบบโทรศัพท์ประยุกต์ใช้ร่วมกับระบบสื่อสารข้อมูลโดยมีขั้นตอนประยุกต์พอสังเขปดังนี้

7.2.1 ติดตั้งอุปกรณ์เชื่อมโยงระหว่างสาขาไปยังสำนักงานใหญ่จาก Leased Line Analog มาเป็นระบบ Leased Line Digital Data Network (DDN) โดยใช้อัตราในการส่งผ่าน

ความเร็วที่ 64 Kbps โดยเช่าวงจรจากผู้ให้บริการวงจรเช่า บริษัท เทเลคอมเอเซีย คอร์ปอเรชั่น จำกัด (มหาชน)

7.2.2 ติดตั้งอุปกรณ์เราท์เตอร์ ที่แต่ละสาขา โดยอุปกรณ์เราท์เตอร์นี้ต้องสนับสนุนรูปแบบโปรโตคอลต่างๆ ได้เช่น Ethernet (IEEE 802.3) และIEEE 802.2 LLC2 (Local Link Control 2) ตลอดจนสนับสนุนการส่งผ่านของเสียงที่ได้มาตรฐานในการเชื่อมต่อกับระบบตู้สาขาอัตโนมัติได้

7.2.3 ติดตั้งอุปกรณ์เราท์เตอร์ที่สำนักงานใหญ่โดยอุปกรณ์นี้ต้องสนับสนุนรูปแบบของโปรโตคอลต่างๆ ที่กล่าวมาแล้วในอุปกรณ์เราท์เตอร์ และมีอัตราในการส่งผ่านข้อมูลได้ถึง 2.048 Mbps (ตามมาตรฐาน E1) ตลอดจนสามารถเชื่อมต่อกับระบบโทรศัพท์ตู้สาขาอัตโนมัติ ที่มาตรฐาน E1 (30 Channels) ได้ทั้งนี้เพื่อใช้คุณสมบัติของ เครือข่าย IP ในการส่งผ่านเสียง (Voice Over IP) โดยจะทำให้สามารถประหยัดค่าใช้จ่ายเกี่ยวกับการโทรศัพท์ของธนาคารได้อย่างมาก

7.2.4 ติดตั้งอุปกรณ์เชื่อมต่อบนระบบโทรศัพท์ตู้สาขาอัตโนมัติ ที่สาขาโดยทำการต่อสายสัญญาณโทรศัพท์ที่เป็น Extension จำนวน 2 สายสัญญาณ ไปยังอุปกรณ์เราท์เตอร์ โดยเชื่อมต่อที่ Voice Port ของอุปกรณ์เราท์เตอร์

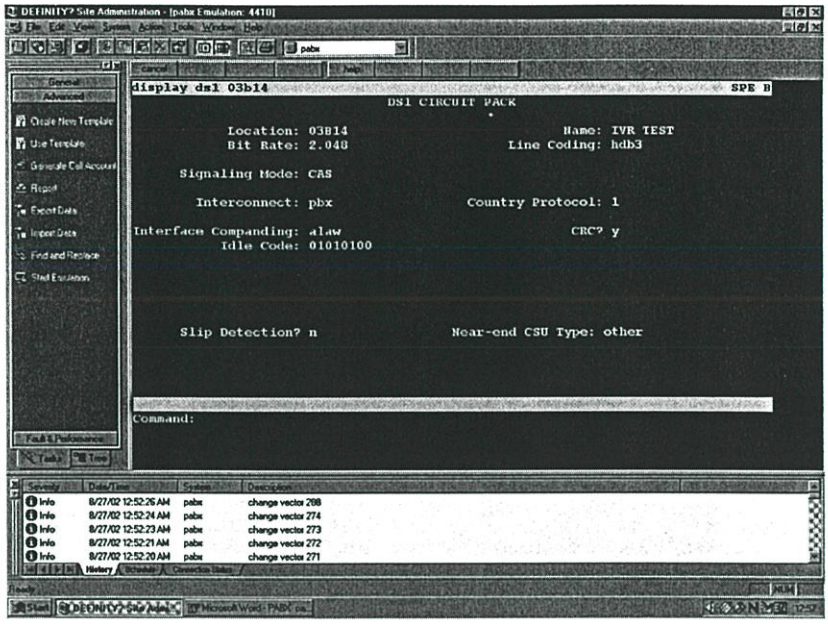
7.2.5 ทำการติดตั้ง Interface Digital Signal Level 1 (DS1 Interface) จำนวน 2 Cards เข้ากับ ตู้สาขาอัตโนมัติ ทีสำนักงานใหญ่ โดยทำการกำหนดพารามิเตอร์เป็น E1 Trunk [4] ชนิด Tie เพื่อทำการเชื่อมต่อกับอุปกรณ์เราท์เตอร์ ที่มี Voice Interface ชนิดที่สนับสนุนการเชื่อมต่อที่ 2.048 Mbps

7.3 การกำหนดค่าพารามิเตอร์บนระบบโทรศัพท์

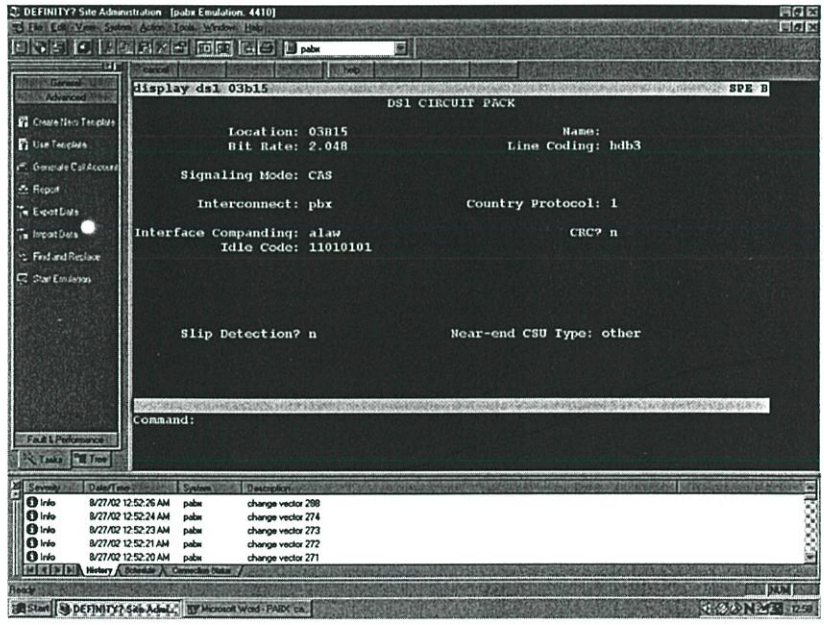
เมื่อทำการเชื่อมต่อระบบตู้สาขาอัตโนมัติ ทีสำนักงานใหญ่เข้ากับอุปกรณ์ Router ที่สำนักงานใหญ่เรียบร้อยแล้ว การกำหนดค่าพารามิเตอร์บนตู้สาขาอัตโนมัติมีรายละเอียดดังต่อไปนี้

จากภาพที่ 7.3 เป็นการดูสถานะของค่าพารามิเตอร์ของ Digital Signal Level 1 ที่ได้ทำการกำหนดไว้ให้เป็นการเชื่อมต่อที่ 2.048 Mbps และใช้ line Coding แบบ High Density Bipolar 3-bit (HDB3) และ Signaling เป็นแบบ Channel-Associated Signaling (CAS) โดยมี Interface Companding เป็น A law

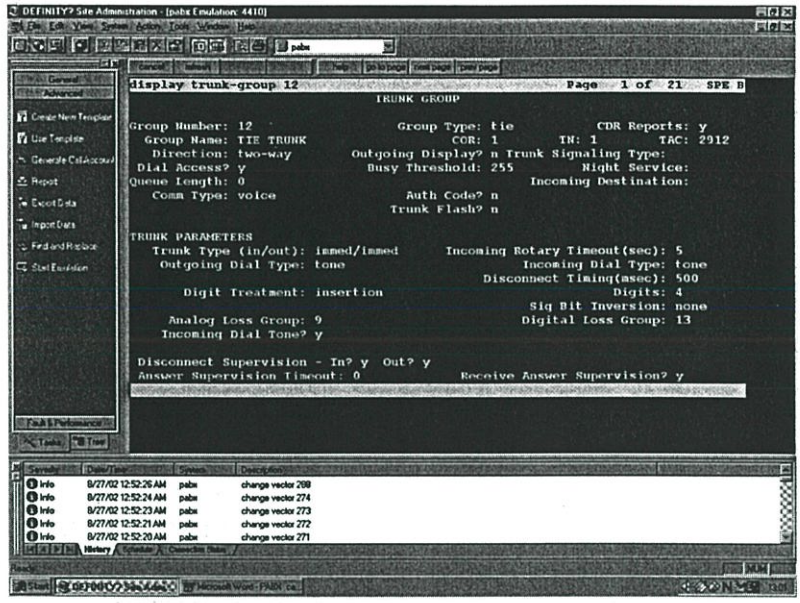
เนื่องจากที่สำนักงานใหญ่นั้นได้ใช้ตู้ชุมสายอัตโนมัติ ของ Avaya Definity G3V8r ซึ่งมีโปรแกรมที่สามารถใช้ควบคุมการทำงาน แก้ไข และดูสถานะของตู้ชุมสายได้ เรียกว่า Avaya Site Administration ซึ่งทำงานในรูปแบบกราฟฟิก ซึ่งทำให้ผู้ทำวิทยานิพนธ์สามารถนำมาแสดงให้เห็นชัดเจนขึ้นดังแสดงในรูปดังนี้



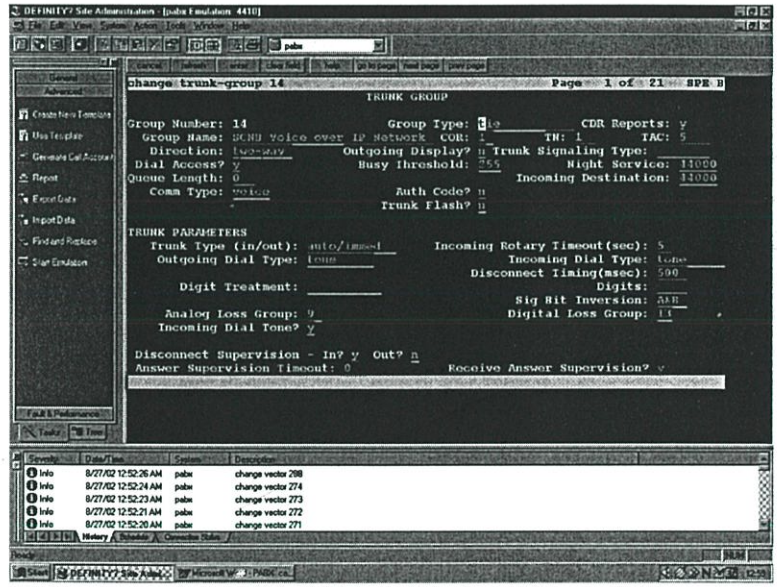
ภาพที่ 7.3 ค่าพารามิเตอร์ของ DS1 Interface Card ที่ 1 ด้วย Bit Rate เท่ากับ 2.048 Mbps



ภาพที่ 7.4 ค่าพารามิเตอร์ของ DS1 Interface Card ที่ 2 ด้วย Bit Rate เท่ากับ 2.048 Mbps

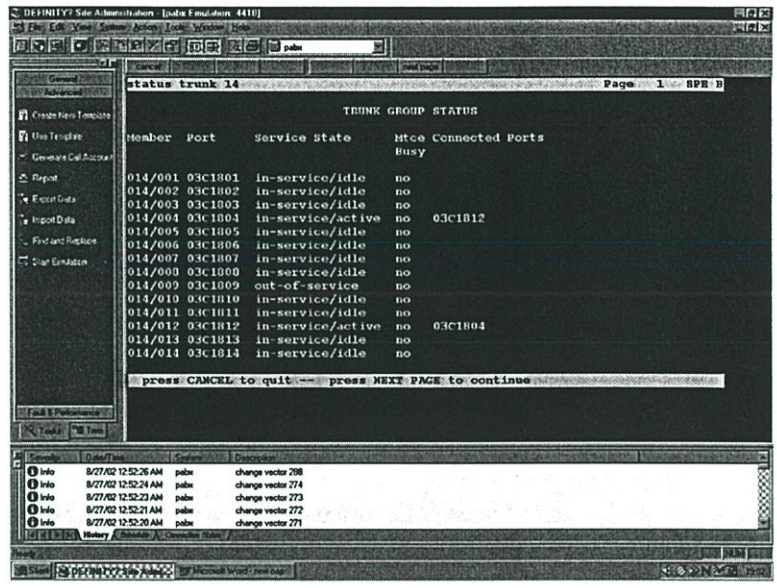


ภาพที่ 7.5 ค่าพารามิเตอร์ของ Trunk ชนิด Tie Trunk

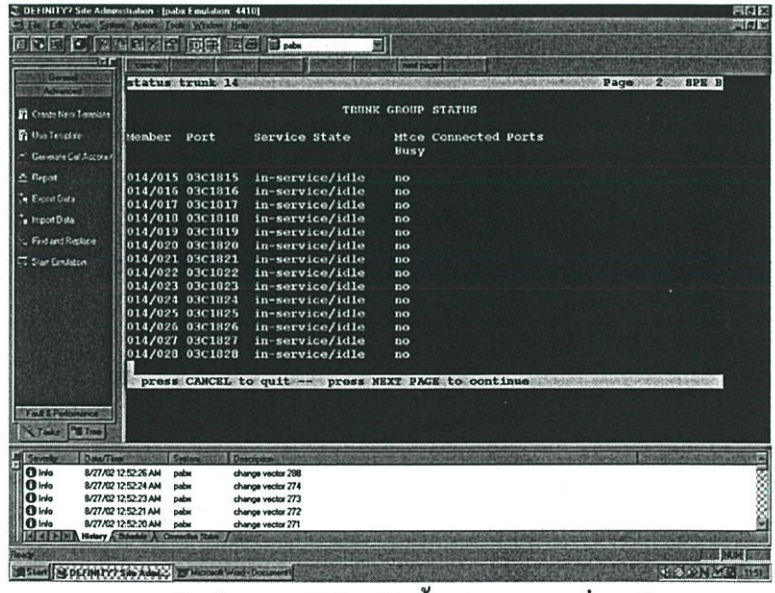


ภาพที่ 7.6 การเปลี่ยนค่าพารามิเตอร์ของ Trunk ในตู้ชุมสายอัตโนมัติ

หลังจากทำการกำหนดค่าพารามิเตอร์ต่างๆในระบบโทรศัพท์ตู้ชุมสายอัตโนมัติ ของสำนักงานใหญ่เรียบร้อยแล้ว จึงทำการตรวจสอบสถานะของ Trunk ที่ทำการสร้างขึ้นโดยที่กำหนดหมายเลขของ Trunk ไว้ที่หมายเลข 14 โดยใช้คำสั่งดูสถานะของ Trunk ดังนี้ คือ Status Trunk 14

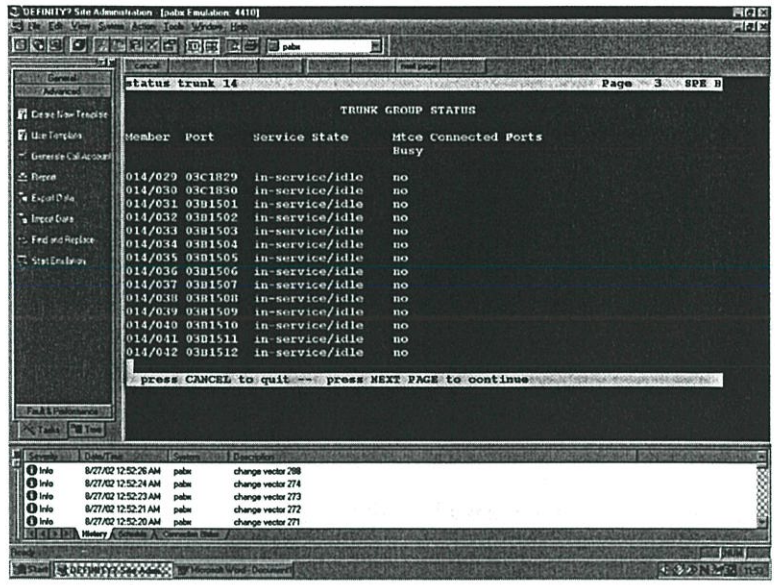


ภาพที่ 7.7 สถานะของ Trunk ในตู้ชุมสายอัตโนมัติ ตั้งแต่ channel ที่ 1 ถึง 14

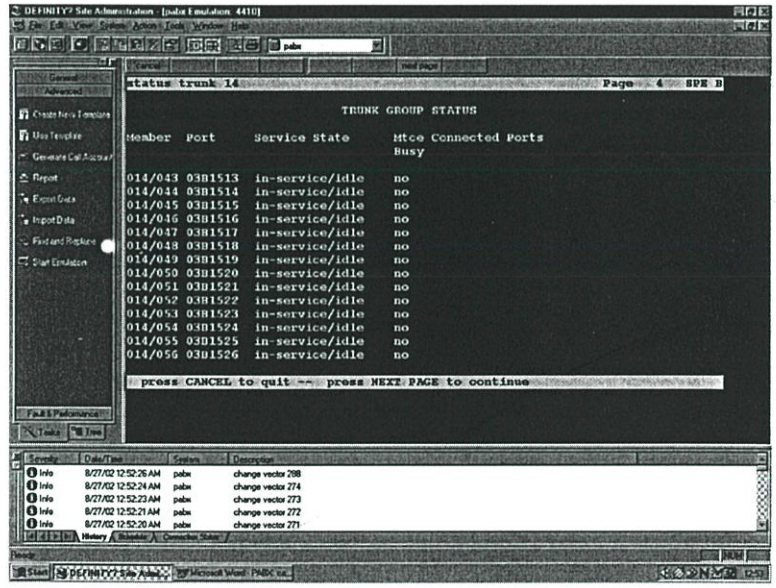


ภาพที่ 7.8 สถานะของ Trunk ในตู้ชุมสายอัตโนมัติ ตั้งแต่ channel ที่ 15 ถึง 28

จากภาพที่ 7.7 ถึง 7.11 เป็นการแสดงให้เห็นถึงสถานะของ Voice Status ของ Trunk Port ที่เชื่อมต่อกับอุปกรณ์เราท์เตอร์ โดย Member 014/001 หมายถึง Trunk หมายเลขที่ 14 และเป็น Channel ที่ 1 ส่วน Port 03C1801 หมายถึง ตำแหน่งของ Card และ Port บนตู้โทรศัพท์

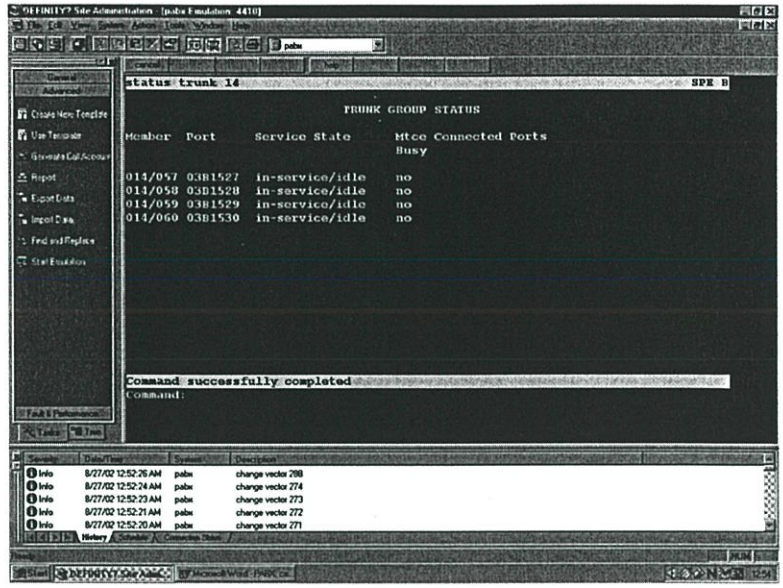


ภาพที่ 7.9 สถานะของ Trunk ในตู้ชุมสายอัตโนมัติ ตั้งแต่ channel ที่ 19 ถึง 42



ภาพที่ 7.10 สถานะของ Trunk ในตู้ชุมสายอัตโนมัติ ตั้งแต่ channel ที่ 43 ถึง 56

สำหรับ Service State หากแสดง in-service/idle หมายถึงสถานะพร้อมที่จะทำงาน หากเป็น in-service/active แสดงว่ามีการใช้งานอยู่ และจะมีการแสดงให้เห็นถึง port ที่ใช้งานอยู่ โดยดูได้จาก Connected Ports คือ 03C1812 เป็นต้น และหากขึ้น out-of-service แสดงว่า channel นั้นใช้งานไม่ได้



ภาพที่ 7.11 สถานะของ Trunk ในตู้ชุมสายอัตโนมัติ ตั้งแต่ channel ที่ 57 ถึง 60

จากภาพที่ 7.6 ถึง 7.9 เป็นการตรวจสอบสถานะของ Trunk 14 ที่เราทำการกำหนดค่าพารามิเตอร์เป็น Trunk และเชื่อมต่อกับอุปกรณ์ Router จำนวน 2 ตัว โดยแบ่งการเชื่อมต่อกับ Digital Signal Level 1 ต่อ Router 1 ตัว จึงทำให้มี Voice channel ได้ทั้งหมด 60 channels โดยในการกำหนดหมายเลขที่ต้องการให้ออกที่ Trunk 14 นี้นั้นได้กำหนดเป็นเลข 5 เมื่อทำการกดหมายเลข 5 ระบบตู้สาขาอัตโนมัติ ก็จะทำการชี้มาที่ Trunk 14 ที่เราทำการกำหนดพารามิเตอร์ให้เชื่อมต่อกับอุปกรณ์ Router ทันที่ หลังจากนั้น จำนวนหมายเลข 2 หลักหลัง จะถูกจัดการโดยอุปกรณ์ Router ที่เรียกว่า Routing ที่มีอยู่บน Route นั่นเอง

7.4 การกำหนดค่าพารามิเตอร์บนอุปกรณ์ Router

ตามที่เราได้ทำการกำหนดค่าพารามิเตอร์ต่างๆที่ระบบตู้สาขาอัตโนมัติไปแล้วนั้น ในขั้นตอนนี้จะกล่าวถึงการกำหนดค่าพารามิเตอร์บนอุปกรณ์ Router ซึ่งเป็นส่วนสำคัญในการนำพาระบบเสียงผ่านไปยังเครือข่ายส่วนตัวได้อย่างมีประสิทธิภาพ โดยมีรายละเอียดดังต่อไปนี้

ตารางที่ 7.1 ค่าพารามิเตอร์ของ WAN port Interface

Head Office	Branch Office
interface Serial5/0:7	interface Serial0/0
description ### Chaengwatthana-WAN	bandwidth 64
Interface CCT: B03337 ###	no ip address
bandwidth 64	encapsulation ppp
no ip address	ppp authentication chap
encapsulation ppp	ppp multilink
ppp authentication chap	multilink-group 10
ppp multilink	
multilink-group 17	

ตารางที่ 7.2 ค่าพารามิเตอร์ของ Routing

Head Office	Branch Office
router ospf 1	router ospf 1
log-adjacency-changes	log-adjacency-changes
area 1 range 172.21.128.0 255.255.240.0	network 172.21.135.128 0.0.0.3 area 1
network 172.21.103.0 0.0.0.255 area 0	network 172.21.135.133 0.0.0.0 area 1
network 172.21.119.1 0.0.0.0 area 1	network 172.21.135.192 0.0.0.63 area 1
network 172.21.135.0 0.0.0.3 area 1	!

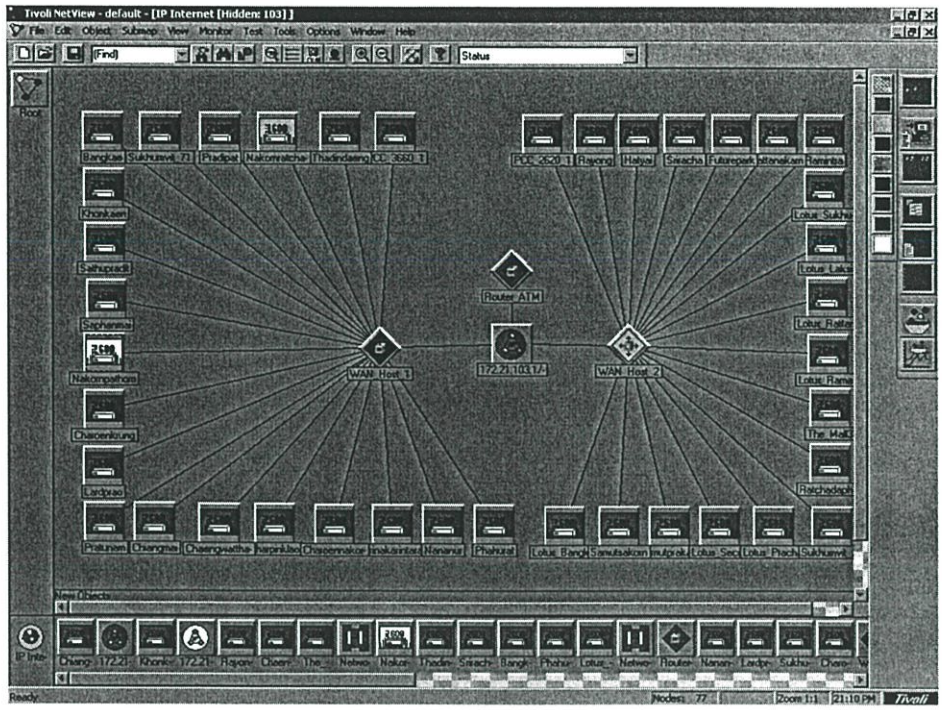
ตารางที่ 7.3 ค่าพารามิเตอร์ของ Voice Interface

Head Office	Branch Office
voice-card 3 class-map match-all voice match ip rtp 16384 16383 policy-map qos class app-dlsw bandwidth 10 class voice priority 20 class class-default fair-queue controller E1 3/0 framing NO-CRC4 ds0-group 0 timeslots 1-15,17-31 type e&m-immediate-start interface Loopback1 ip address 172.21.119.11 255.255.255.255 h323-gateway voip interface h323-gateway voip id zoneHeadOffice ipaddr 172.21.119.4 1718 h323-gateway voip h323-id WAN_Host_1 h323-gateway voip tech-prefix 1#	encapsulation ppp ip tcp header-compression iphc-format ip rtp header-compression iphc-format voice-port 1/0/0 voice-port 1/0/1 dial-peer cor custom

ตารางที่ 7.4 ค่าพารามิเตอร์ของการเข้ารหัสและDial Plan

Head Office	Branch Office
voice-port 3/0:0 dial-peer voice 503 voip destination-pattern 19 session target ipv4:172.21.132.5 codec g729br8 ip precedence 5	dial-peer voice 101 pots destination-pattern 31 port 1/0/0 ! dial-peer voice 102 pots destination-pattern 31 port 1/0/1 dial-peer voice 501 voip destination-pattern 9 session target ras codec g729br8 bytes 30 ip precedence 5 ! dial-peer voice 502 voip destination-pattern .. session target ras codec g729br8 bytes 30

หลังจากทำการกำหนดค่าพารามิเตอร์ต่างๆ ในอุปกรณ์เราท์เตอร์ จนครบทั้งหมดจะได้เครือข่ายที่มีคุณสมบัติตามที่ต้องการคือเป็นเครือข่ายอินเตอร์เน็ต โพรโตคอล มี อุปกรณ์เราท์เตอร์ที่ตั้งชื่อ WAN Host 1 และ WAN Host 2 เป็นอุปกรณ์หลักของเครือข่าย และมีอุปกรณ์เราท์เตอร์ ที่ทำหน้าที่เป็น gatekeeper ที่ช่วยจัดการด้าน Voice และจาก WAN Host 1 & 2 นั้นก็เชื่อมต่อไปยังอุปกรณ์เราท์เตอร์ ที่สำนักงานสาขาต่างๆ ด้วยการเชื่อมต่อแบบ Leased Line ชนิด Digital Data Network (DDN) ความเร็ว 64 Kbps โดยลักษณะการเชื่อมต่อเป็นแบบ Star คือทุกๆสำนักงานสาขาเชื่อมโยงตรงมายังสำนักงานใหญ่ และที่สำนักงานใหญ่ จะถูกเชื่อมต่อแบบ Channel E1 จำนวน 2 E1 ซึ่งถูกแยกเชื่อมต่อที่ WAN Host 1 และ WAN Host 2 ตามลำดับ โดยสามารถดูภาพโดยรวมดังแสดงภาพที่ 7.12



ภาพที่ 7.12 เครือข่ายที่มีการประยุกต์ใช้งาน

จากภาพที่ 7.12 เป็นการแสดงให้เห็นถึงเครือข่ายที่ทำการประยุกต์ใช้งาน โดยการนำระบบโทรศัพท์ ส่งผ่านไปในระบบเครือข่าย ซึ่งทำให้เห็นถึงระบบการเชื่อมโยงจากสำนักงานใหญ่ไปยังสำนักงานสาขาได้อย่างชัดเจน โดยเป็นการแยกออกเป็น 2 กลุ่ม ซึ่งการออกแบบเครือข่ายนี้ได้มุ่งเน้นการแบ่ง Load และลดความเสี่ยงในระบบเมื่อเกิดปัญหาในระบบเครือข่ายขึ้นมา

จากการดูสถานะของ Voice Port ที่อุปกรณ์ Router ตัวที่ 1 ได้ผลดังนี้

```
WAN_Host_1# sh voice port sum
```

					IN	OUT	
PORT	CH	SIG-TYPE	ADMIN	OPER	STATUS	STATUS	EC
3/0:0	1	e&m-imd	up	dorm	idle	idle	y
3/0:0	2	e&m-imd	up	dorm	idle	idle	y
3/0:0	3	e&m-imd	up	dorm	idle	idle	y
3/0:0	4	e&m-imd	up	up	seized	seized	y
3/0:0	5	e&m-imd	up	dorm	idle	idle	y
3/0:0	6	e&m-imd	up	dorm	idle	idle	y
3/0:0	7	e&m-imd	up	dorm	idle	idle	y
3/0:0	8	e&m-imd	up	dorm	idle	idle	y
3/0:0	9	e&m-imd	up	dorm	idle	idle	y
3/0:0	10	e&m-imd	up	dorm	idle	idle	y
3/0:0	11	e&m-imd	up	dorm	idle	idle	y
3/0:0	12	e&m-imd	up	up	seized	seized	y
3/0:0	13	e&m-imd	up	dorm	idle	idle	y
3/0:0	14	e&m-imd	up	dorm	idle	idle	y
3/0:0	15	e&m-imd	up	dorm	idle	idle	y
3/0:0	17	e&m-imd	up	dorm	idle	idle	y
3/0:0	18	e&m-imd	up	dorm	idle	idle	y
3/0:0	19	e&m-imd	up	dorm	idle	idle	y
3/0:0	20	e&m-imd	up	dorm	idle	idle	y
3/0:0	21	e&m-imd	up	dorm	idle	idle	y
3/0:0	22	e&m-imd	up	dorm	idle	idle	y
3/0:0	23	e&m-imd	up	dorm	idle	idle	y
3/0:0	24	e&m-imd	up	dorm	idle	idle	y
3/0:0	25	e&m-imd	up	dorm	idle	idle	y
3/0:0	26	e&m-imd	up	dorm	idle	idle	y
3/0:0	27	e&m-imd	up	dorm	idle	idle	y
3/0:0	28	e&m-imd	up	dorm	idle	idle	y
3/0:0	29	e&m-imd	up	dorm	idle	idle	y
3/0:0	30	e&m-imd	up	dorm	idle	idle	y
3/0:0	31	e&m-imd	up	dorm	idle	idle	y

จากสถานะของ Voice Port ที่อุปกรณ์ Router ข้างต้นนั้น จะแสดง Interface Port และจำนวน Channel เริ่มตั้งแต่ Channel ที่ 1 ถึง 31 ซึ่ง Channel ที่ 15 จะไม่ได้ถูกใช้งาน เนื่องจากเป็น D Channel และ Status เป็น idle หมายถึงสถานะพร้อมทำงาน หากเป็น seized ก็หมายถึง Channel ถูกใช้งานอยู่ ณ ขณะนั้น

วิธีการโทรจากสำนักงานใหญ่ไปยังสำนักงานสาขาโดยทำการกดหมายเลข 5 แล้วตามด้วยหมายเลข จำนวน 2 หลัก ซึ่งในที่นี้ได้ทำการกำหนดหมายเลข 2 หลัก เป็นหมายเลขประจำสำนักงานสาขานั้นๆอยู่แต่เดิมเพื่อให้สะดวกในการจำดังมีรายละเอียดตามตารางที่ 7.4

ตารางที่ 7.5 หมายเลขโทรศัพท์ที่ทำการกำหนดให้ใช้งานโดยผ่านเครือข่ายส่วนตัวจากสำนักงานใหญ่

Calling from HQ. to Branch offices Method

			Access Code⟹wait until get dialtone+ Br. Extension			
			H.Q. Ext to Br.	Br. Extension		
No.	Br.No.	Branch		BM	CSM	PFC
1	1	Thadindaeng	5 01			
2	4	Sampeng	5 04			
3	6	Nakornratchasima	5 06			
4	7	Pradipat	5 07			
5	9	Sukhumvit71	5 09			
6	12	Mahanak	5 12			
7	13	Bangkae	5 13			
8	14	Khonkaen	5 14			
9	15	Surawong	5 15			
10	18	Sathupradit	5 18			
11	23	Saphanmai	5 23			
12	24	Nakhonpathom	5 24			
13	25	Charoenkrung	5 25			
14	26	Lardprao	5 26			
15	27	Pratunam	5 27			
16	28	Chiangmai	5 28			
17	31	Chaengwatthana	5 31			
18	33	Phrapinklao	5 33			
19	34	Charoennakorn	5 34			
20	37	Srinakarintara	5 37	111	131	121-125
21	39	Nananua	5 39			
22	40	Rayong	5 40			
23	42	Phahurat	5 42			
24	46	Samutsakhon	5 46			
25	47	Sriracha	5 47			
26	49	Hatyai	5 49			
27	51	Ratchadaphisek	5 51			
28	52	Sukhumvit24	5 52			
29	55	Future Park Rangsit	5 55			
30	63	Samutprakarn	5 63			
31	65	Pattanakan	5 65			
32	67	Ramintra	5 67			
33	68	Lotus Sukhumvit50	5 68			
34	69	Lotus Laksi	5 69			
35	70	Lotus Rattanatibeth	5 70			
36	71	Lotus Rama3	5 71			
37	72	The Mall3 Ramkhumhaeng	5 72			
38	73	Lotus Prachachuen	5 73			
39	74	Lotus Seacon	5 74			

Sample : From H.Q.extension press5 XX (2 Digits of Br.No.) wait until get dial tone press Br.Ext. 3 digits XXX

Remark: BM : Branch Manager
CSM : Customer Service Manager
PFC : Personal Financial Consultant

วิธีการโทรจากสำนักงานสาขาไปยังสำนักงานใหญ่ทำได้โดยทำการกดหมายเลข 5 แล้วตามด้วยหมายเลข จำนวน 1 หลัก ซึ่งในที่นี้ได้ทำการกำหนดหมายเลข 1 หลัก เป็นหมายเลข 9 เสมือนว่าตัดสายนอก ซึ่งหลังจากกดหมายเลข 5 9 เป็นที่เรียบร้อยแล้วจะได้ยินเสียงประกาศจากตู้สาขาอัตโนมัติเพื่อให้กดหมายเลขโทรศัพท์ภายในต่อไป ดังมีรายละเอียดตามตารางที่ 7.5

ตารางที่ 7.6 แสดงหมายเลขโทรศัพท์ที่ทำการกำหนดให้ใช้งานโดยผ่านเครือข่ายส่วนตัว จากสำนักงานสาขา

No.	Br.No.	Branch	Br. call to H.Q.	H.Q Extension*
1	1	Thadindaeng	5 9	
2	4	Sampeng	5 9	
3	6	Nakornratchasima	5 9	
4	7	Pradipat	5 9	
5	9	Sukhumvit 71	5 9	
6	12	Mahanak	5 9	
7	13	Bangkae	5 9	
8	14	Khonkaen	5 9	
9	15	Surawong	5 9	
10	18	Sathupradit	5 9	
11	23	Saphanmai	5 9	
12	24	Nakhonpathom	5 9	
13	25	Charoenkrung	5 9	
14	26	Lardprao	5 9	
15	27	Pratunam	5 9	
16	28	Chiangmai	5 9	
17	31	Chaengwatthana	5 9	
18	33	Phrapinklao	5 9	
19	34	Charoennakorn	5 9	
20	37	Srinakarintara	5 9	4XXXX
21	39	Nananua	5 9	
22	40	Rayong	5 9	
23	42	Phahurat	5 9	
24	46	Samutsakhon	5 9	
25	47	Sriracha	5 9	
26	49	Hatyai	5 9	
27	51	Ratchadaphisek	5 9	
28	52	Sukhumvit 24	5 9	
29	55	Future Park Rangsit	5 9	
30	63	Samutprakarn	5 9	
31	65	Pattanakan	5 9	
32	67	Ramintra	5 9	
33	68	Lotus Sukhumvit 50	5 9	
34	69	Lotus Laksi	5 9	
35	70	Lotus Rattanatibeth	5 9	
36	71	Lotus Rama 3	5 9	
37	72	The Mall 3 Ramkhumhaeng	5 9	
38	73	Lotus Prachachuen	5 9	
39	74	Lotus Seacon	5 9	

Sample : From Branches extension press 59 (get auto greeting) press 4XXXX

ในขณะเดียวกันหากสำนักงานสาขาต้องการติดต่อไปยังสำนักงานสาขาด้วยกันก็สามารถทำได้โดยใช้วิธีการกดหมายเลขโทรศัพท์ หมายเลข 5 แล้วตามด้วย 2 หลักของหมายเลขประจำสำนักงานสาขานั้นๆดังแสดงตามตารางที่ 7.6 ซึ่งทำให้สำนักงานสาขาติดต่อกันได้โดยตรงโดยไม่ต้องใช้ระบบตู้ชุมสายอัตโนมัติที่สำนักงานใหญ่

ตารางที่ 7.7 หมายเลขโทรศัพท์ที่ทำการกำหนดให้ใช้งานโดยผ่านเครือข่ายส่วนตัว จากสำนักงานสาขาไปยังสำนักงานสาขา

No.	Br.No.	Branch	Br. Ext to Br. Ext	Br. Extension		
				BM	CSM	PFC
1	1	Thadindaeng	5 01			
2	4	Sampeng	5 04			
3	6	Nakornratchasima	5 06			
4	7	Pradipat	5 07			
5	9	Sukhumvit71	5 09			
6	12	Mahanak	5 12			
7	13	Bangkae	5 13			
8	14	Khonkaen	5 14			
9	15	Surawong	5 15			
10	18	Sathupradit	5 18			
11	23	Saphanmai	5 23			
12	24	Nakhonpathom	5 24			
13	25	Charoenkrung	5 25			
14	26	Lardprao	5 26			
15	27	Pratunam	5 27			
16	28	Chiangmai	5 28			
17	31	Chaengwatthana	5 31			
18	33	Phrapinklao	5 33			
19	34	Charoennakorn	5 34			
20	37	Srinakarintara	5 37	111	131	121-125
21	39	Nananua	5 39			
22	40	Rayong	5 40			
23	42	Phahurat	5 42			
24	46	Samutsakhon	5 46			
25	47	Sriracha	5 47			
26	49	Hatyai	5 49			
27	51	Ratchadaphisek	5 51			
28	52	Sukhumvit24	5 52			
29	55	Future Park Rangsit	5 55			
30	63	Samutprakarn	5 63			
31	65	Pattanakan	5 65			
32	67	Ramintra	5 67			
33	68	Lotus Sukhumvit50	5 68			
34	69	Lotus Laksi	5 69			
35	70	Lotus Rattanatibeth	5 70			
36	71	Lotus Rama3	5 71			
37	72	The Mall3 Ramkhumhaeng	5 72			
38	73	Lotus Prachachuen	5 73			
39	74	Lotus Seacon	5 74			

7.5 สรุปผลการทดสอบและข้อเสนอแนะ

วิทยานิพนธ์นี้ได้เสนอผลงานวิจัย โครงสร้างของโพรโตคอล เพื่อการจัดการเครือข่ายอินเตอร์เน็ต โพรโตคอล มาประยุกต์ใช้งานโดยที่ทำหน้าที่หลัก และนำข้อมูลชนิดต่างๆ เช่น สัญญาณเสียง และข้อมูล ส่งรวมกันไปบนเครือข่ายได้ โดยทดลองใช้วิธีการบีบอัดซึ่งเป็นส่วนสำคัญในการส่งผ่านข้อมูลเสียงในรูปแบบของอินเตอร์เน็ต โพรโตคอล อีกทั้งสามารถตรวจวัดปริมาณของ utilization และปริมาณของ Voice Frames บนเครือข่าย ที่ถูกใช้ผ่านเครือข่ายด้วย สำหรับการทดสอบครั้งนี้ผู้ทำวิทยานิพนธ์ได้ทำการเชื่อมต่อระบบโทรศัพท์ของสำนักงานใหญ่เข้ากับเครือข่ายอินเตอร์เน็ต โพรโตคอล ที่เป็นเครือข่ายข้อมูลส่วนตัวขององค์กร และเชื่อมต่อไปยังสำนักงานสาขาต่างๆ และจากนั้นก็เชื่อมต่อไปยัง Station Port ของตู้ชุมสายอัตโนมัติ

ซึ่งเป็นตู้ชุมสายอัตโนมัติขนาดเล็ก ซึ่งในการทดสอบนี้ได้ใช้ทั้งวิธีการบีบอัดข้อมูลและไม่ใช้วิธีการบีบอัด ซึ่งก็ได้ผลการทดสอบดังที่กล่าวไว้ในบทที่ 6 แล้วนั้น การส่งสัญญาณเสียง และข้อมูล รวมกันไปบนเครือข่ายชนิดอินเตอร์เน็ต โพรโตคอลนั้น เป็นการใช้ช่องทางการสื่อสารข้อมูลอย่างคุ้มค่า และมีประสิทธิภาพ ซึ่งรูปแบบในการวิจัยนี้พิสูจน์ให้เห็นในวัตถุประสงค์หลักของประโยชน์การนำโครงสร้างหรือคุณสมบัติที่เกี่ยวข้องของโพรโตคอลและวิธีการบีบอัด ซึ่งเป็นส่วนสำคัญในการส่งผ่านข้อมูลเสียงไปบนช่องทางหรือวงจรที่ยังคงมีแบนด์วิดท์เดียวกัน และนำระบบโทรศัพท์ มาประยุกต์ใช้งานร่วมไปในเครือข่าย

ดังนั้นสิ่งที่ต้องวิเคราะห์และพิจารณาจึงได้แก่ วิธีการบีบอัด การส่งสัญญาณเสียงไปบนเครือข่ายชนิดอินเตอร์เน็ต โพรโตคอล การเชื่อมต่อและจุดเชื่อมต่อ รวมไปถึงโพรโตคอลที่นำมาประยุกต์ใช้งานว่าเหมาะสมเพียงใด โดยในงานวิจัยฉบับนี้จะเป็นแนวทางในการสร้างแนวความคิดในการประยุกต์ใช้งาน

บรรณานุกรม

[1] Cisco Systems, Inc. 1998. **Voice over IP for the Cisco 2600 and Cisco 3600 Series Software Configuration Guide.** San Jose : Cisco Press.

[2] J. Davidson and J.Peters, 2000. **Voice over IP Fundamentals.** Indianapolis : Cisco Press.

[3] K. Siyan, 1997. **Inside TCP/IP.** Indiannapolis : New Riders Publishing.

[4] R. Getter et. al., 2000. **Definity System's Little Instruction Book.** Indianapolis : Lucent Technologies

[5] S. Keagy, 2000. **Integrating Voice and Data Networks.** Indianapolis : Cisco Press.

ภาคผนวก

ภาคผนวก

ตัวอย่างการกำหนด Configure Parameter ที่อุปกรณ์ Router (CISCO 3600) ที่เชื่อมต่อกับตู้ชุมสายอัตโนมัติ ชนิด E1 Channel

WAN Host 1
WAN_Host_1#sh run
Building configuration...
Current configuration : 28591 bytes
!
! Last configuration change at 13:54:15 UTC Sat Nov 2 2002
! NVRAM config last updated at 21:46:42 UTC Mon Oct 21 2002
!
version 12.2
service timestamps debug uptime
service timestamps log datetime msec
service password-encryption
!
hostname WAN_Host_1
!
logging buffered 65535 debugging
enable secret 5 1h4LE$xgO4LUfHb8VZXGGyv0VRq1
enable password 7 00071A150754
!
username PCC_TANDEM password 7 0017100806
username WAN_Host_1 password 7 06150C2F4E
username Thadindaeng password 7 095F4D071B
username Nakornratchasima password 7 111A1A0B15
username Bangkae password 7 06150C2F4E
username Sathupradit password 7 044808080D
username Saphaımai password 7 140411050E
username Charoenkrung password 7 1316141C09

```
username Lardprao password 7 0215075509
username Pratunam password 7 111A1A0B15
username Chiangmai password 7 06150C2F4E
username Chaengwatthana password 7 1316141C09
username Charoennakorn password 7 140411050E
username Nananur password 7 0100050A59
username Phahurat password 7 0317580504
username scnbtelecom privilege 10 password 7 1058001C12181C0715
username scnbadmin privilege 15 password 7 00071B03165400030A
username Panjathani_1 password 7 095F4D071B
username Pan password 7 0452090B
username Surawong password 7 0017100806
username Sampeng password 7 0317580504
username Pradipat password 7 140411050E
username Sukhumvit_71 password 7 0317580504
username Khonkaen password 7 105D0A1707
username Nakornpathom password 7 0017100806
username Phrapinklao password 7 140411050E
username Srinakarintara password 7 0017100806
username DRC_Empire password 7 0502150B2F
username ISDN_Nakornratchasima password 7 0502150B2F
username ISDN_Khonkaen password 7 020F175F05
username ISDN_Thadindaeng password 7 0452180201
username ISDN_Bangkae password 7 09455D0D17
username ISDN_Sathupradit password 7 09455D0D17
username ISDN_Saphanmai password 7 0706324840
username ISDN_Charoenkrung password 7 0502150B2F
username ISDN_Lardprao password 7 151B18080A
username ISDN_Pratunam password 7 020F175F05
username ISDN_Chiangmai password 7 0502150B2F
username ISDN_Chaengwatthana password 7 130C041605
username ISDN_Charoennakorn password 7 11000A0119
```

```
username ISDN_Nananur password 7 011A150055
username ISDN_Phahurat password 7 0502150B2F
username ISDN_Surawong password 7 130C041605
username ISDN_Sampeng password 7 121016131C
username ISDN_Pradipat password 7 000D00020A
username ISDN_Sukhumvit_71 password 7 030D480F08
username ISDN_Mahanak password 7 141E010F02
username ISDN_Nakornpathom password 7 121016131C
username ISDN_Phrapinklao password 7 151B18080A
username ISDN_Srinakarintara password 7 030D480F08
username ISDN_DRC_Empire password 7 011A150055
username Mahanak password 7 1316141C09
username ISDN_Test_Empire password 7 011A150055
voice-card 3
!
ip subnet-zero
!
!
ip ftp username coredump
ip ftp password 7 02050B490E021A2C5C
no ip domain-lookup
ip host CALLED_1 4040 172.21.188.5
!
virtual-profile virtual-template 1
!
class-map match-all voice
 match ip rtp 16384 16383
!
!
policy-map qos
 class voice
  priority 24
```

```
 class class-default
  fair-queue
!
isdn switch-type primary-net5
call rsvp-sync
!
!
!
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
controller E1 3/0
 framing NO-CRC4
 ds0-group 0 timeslots 1-15,17-31 type e&m-immediate-start
!
controller E1 5/0
 framing NO-CRC4
 channel-group 0 timeslots 1
 channel-group 1 timeslots 2
 channel-group 2 timeslots 3
 channel-group 3 timeslots 4
 channel-group 4 timeslots 5
 channel-group 5 timeslots 6
 channel-group 6 timeslots 7
 channel-group 7 timeslots 8
 channel-group 8 timeslots 9
 channel-group 9 timeslots 10
 channel-group 10 timeslots 11
 channel-group 11 timeslots 12
 channel-group 12 timeslots 13
```

```
 channel-group 13 timeslots 14
 channel-group 14 timeslots 15
 channel-group 15 timeslots 16
 channel-group 16 timeslots 17
 channel-group 17 timeslots 18
 channel-group 18 timeslots 19
 channel-group 19 timeslots 20
 channel-group 20 timeslots 21
 channel-group 21 timeslots 22
 channel-group 22 timeslots 23
 channel-group 23 timeslots 24
 channel-group 24 timeslots 25
 channel-group 25 timeslots 26
 channel-group 26 timeslots 27
 channel-group 27 timeslots 28
 channel-group 28 timeslots 29
 channel-group 29 timeslots 30
 channel-group 30 timeslots 31
!
controller E1 5/1
 pri-group timeslots 1-31
!
!
!
stun peer-name 172.21.119.1
stun protocol-group 1 basic
stun protocol-group 3 basic
stun protocol-group 4 basic
dlsw local-peer peer-id 172.21.119.1
dlsw remote-peer 0 tcp 172.21.130.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.131.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.188.5 lsap-output-list 200
```

```
dlsw remote-peer 0 tcp 172.21.135.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.128.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.188.37 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.136.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.133.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.138.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.137.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.140.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.141.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.142.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.129.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.133.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.138.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.135.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.190.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.140.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.136.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.132.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.132.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.129.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.131.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.137.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.141.5 lsap-output-list 200
dlsw bridge-group 1
!
bstun peer-name 172.21.119.1
bstun protocol-group 1 bsc
bstun protocol-group 2 bsc
bstun protocol-group 3 bsc
!
interface Loopback0
ip address 172.21.119.1 255.255.255.255
```

```
!
interface Loopback1
 ip address 172.21.119.11 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip id zoneHeadOffice ipaddr 172.21.119.4 1718
 h323-gateway voip h323-id WAN_Host_1
 h323-gateway voip tech-prefix 1#
!
interface Multilink1
 description -> MLPPP Connection to Panjathani_1 S4/0 CCT:
 ip address 172.21.190.1 255.255.255.252
 ip tcp header-compression iphc-format
 no ip mroute-cache
 load-interval 30
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 1
 ip rtp header-compression iphc-format
!
interface Multilink13
description ->MLPPP Connection to Charoenkrung S5/0:3 CCT:B03507
 bandwidth 64
 ip address 172.21.132.129 255.255.255.252
 ip tcp header-compression iphc-format
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 13
 ip rtp header-compression iphc-format
```

```
!
interface Multilink14
 description ->MLPPP Connection to Lardprao S5/0:4 CCT:B03659
 bandwidth 64
 ip address 172.21.133.1 255.255.255.252
 ip tcp header-compression iphc-format
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 14
 ip rtp header-compression iphc-format
!
 interface Multilink15
 description ->MLPPP Conection to Chiangmai S5/0:5 CCT:B03436
 bandwidth 64
 ip address 172.21.133.129 255.255.255.252
 ip tcp header-compression iphc-format
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 15
 ip rtp header-compression iphc-format
!
interface Multilink16
 description -> MLPPP Connection to Pratunam S5/0:6 CCT:B03596
 bandwidth 64
 ip address 172.21.135.1 255.255.255.252
 ip tcp header-compression iphc-format
 no cdp enable
 ppp multilink
```

```
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 16
 ip rtp header-compression iphc-format
!
interface Multilink17
 description -> MLPPP Connection to Chaengwatthana S5/0:07 CCT:B03337
 bandwidth 64
 ip address 172.21.135.129 255.255.255.252
 ip tcp header-compression iphc-format
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 17
 ip rtp header-compression iphc-format
!
interface Multilink18
 description ->MLPPP Connection to Charoennakorn S5/0:8 CCT:B03510
 bandwidth 64
 ip address 172.21.136.1 255.255.255.252
 ip tcp header-compression iphc-format
 no ip mroute-cache
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 18
 ip rtp header-compression iphc-format
!
interface Multilink19
 description -> MLPPP Connection to Thadindaeng S5/0:9 CCT:B02243
```

```
 bandwidth 64
 ip address 172.21.136.129 255.255.255.252
 ip tcp header-compression iphc-format
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 19
 ip rtp header-compression iphc-format
!
interface Multilink21
 description -> MLPPP Connection to Sathupradit S5/0:11 CCT:B03554
 bandwidth 64
 ip address 172.21.138.1 255.255.255.252
 ip tcp header-compression iphc-format
 no ip mroute-cache
 no cdp enable
 ppp multilink
ppp multilink interleave
 multilink-group 21
 ip rtp header-compression iphc-format
!
interface Multilink22
 description -> MLPPP Connection to Saphanmai S5/0:12 CCT:B03511
 bandwidth 64
 ip address 172.21.138.129 255.255.255.252
 ip tcp header-compression iphc-format
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 22
```

```
 ip rtp header-compression iphc-format
!
interface Multilink23
 description -> MLPPP Connection to Nananur S5/0:13 CCT:B03339
 bandwidth 64
 ip address 172.21.140.1 255.255.255.252
 ip tcp header-compression iphc-format
 no cdp enable
 ppp multilink
ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 23
 ip rtp header-compression iphc-format
!
interface Multilink24
 description -> MLPPP Connection to Phahurat S5/0:14 CCT:B03513
 bandwidth 64
 ip address 172.21.140.129 255.255.255.252
 ip tcp header-compression iphc-format
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 24
 ip rtp header-compression iphc-format
!
interface Multilink26
 description -> MLPPP Connection to Pradipat S5/0:16 CCT:B01311
 bandwidth 64
 ip address 172.21.130.129 255.255.255.252
 ip tcp header-compression iphc-format
 no cdp enable
```

```
ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 26
 ip rtp header-compression iphc-format
!
interface Multilink27
 description -> MLPPP Connection to Sukhumvit_71 S5/0:17 CCT: B02256
 bandwidth 64
 ip address 172.21.131.1 255.255.255.252
 ip tcp header-compression iphc-format
 no ip mroute-cache
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 27
 ip rtp header-compression iphc-format
!
interface Multilink29
 description MLPP Connection to Nakornpathom S5/0:19 CCT:B02586
 bandwidth 64
 ip address 172.21.141.1 255.255.255.252
 ip tcp header-compression iphc-format
 no ip mroute-cache
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 29
 ip rtp header-compression iphc-format
!
```

```
interface Multilink30
 description -> MLPPP Connection to Phrapinklao S5/0:20 CCT:B03160
 bandwidth 64
 ip address 172.21.141.129 255.255.255.252
 ip tcp header-compression iphc-format
 no ip mroute-cache
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 30
 ip rtp header-compression iphc-format
!
interface Multilink31
description -> MLppp Connection to Srinakarintara S5/0:21 CCT:B03545
 bandwidth 64
 ip address 172.21.142.1 255.255.255.252
 ip tcp header-compression iphc-format
 no ip mroute-cache
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 31
 ip rtp header-compression iphc-format
!
interface Multilink32
 description -> MLPPP Connection to Khonkaen S5/0:22 CCT:B02571
 bandwidth 64
 ip address 172.21.129.1 255.255.255.252
 ip tcp header-compression iphc-format
 no ip mroute-cache
```

```
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 32
 ip rtp header-compression iphc-format
!
interface FastEthernet0/0
 description Ethernet 0/0 LAN BB
 ip address 172.21.103.249 255.255.255.0
 no ip mroute-cache
 ip policy route-map 64only
 duplex auto
 speed auto
 no cdp enable
 bridge-group 1
!
interface FastEthernet0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
interface Serial1/0
 description ### TA-Link to PCC_3660 128Kbps S1/0 CCT:B03474 ###
 ip address 172.21.188.1 255.255.255.252
 no ip mroute-cache
!
interface Serial1/1
 description ### TA-Link to PCC_3660 64Kbps S1/1 CCT:B03475 ###
```

```
 bandwidth 64
 ip address 172.21.188.21 255.255.255.252
 ip access-group 101 in
!
interface Serial1/2
 description ## MASTER CARD ##
 mtu 512
 no ip address
 encapsulation bstun
 no keepalive
 bstun group 1
 bsc contention 1
 bstun route all tcp 172.21.188.5
!
interface Serial1/3
 description ### AS/400-3 to Empire for EFT Testing ###
 mtu 2104
 bandwidth 9
 no ip address
 encapsulation stun
 shutdown
 clockrate 9600
 stun group 4
!
interface Serial1/4
 description ### Master Card Test ###
 no ip address
 encapsulation bstun
 no keepalive
 bstun group 2
 bsc contention 2
 bstun route all tcp 172.21.188.37
```

```
!
interface Serial1/5
 description ### Link to Empire ###
 ip address 172.21.188.33 255.255.255.252
 no ip mroute-cache
!
interface Serial1/6
 description ### ATM Test PCC T202 ###
 no ip address
 encapsulation sdlc
 no ip mroute-cache
 no keepalive
 sdlc role primary
 sdlc vmac 5000.0008.0500
 sdlc address C2
 sdlc xid C2 0A800101
 sdlc partner 4900.0008.0502 C2
 sdlc dlsw C2
!
interface Serial1/7
 description ### ATM Test PCC T207 ###
 no ip address
 encapsulation sdlc
 no ip mroute-cache
 no keepalive
 sdlc role primary
 sdlc vmac 5000.0008.0500
 sdlc address C7
 sdlc xid C7 0A800204
 sdlc partner 4900.0008.0507 C7
 sdlc dlsw C7
!
```

```
interface Serial2/0
 description ### AS/400-3 to Test_Empire for Testing ###
 mtu 2104
 no ip address
 encapsulation stun
 no ip mroute-cache
 shutdown
 clockrate 9600
!
interface Serial2/1
 description ### Link to AS/400 ###
 mtu 2104
 no ip address
 encapsulation stun
 no ip mroute-cache
 clockrate 128000
 stun group 1
 stun route all tcp 172.21.188.5
!
interface Serial2/2
 description ###ATM TEST SCB to SCNB ST3FL2 ###
 no ip address
 encapsulation sdlc
 no ip mroute-cache
 no keepalive
 sdlc role primary
 sdlc vmac 5000.0008.0500
 sdlc address 30
 sdlc xid 30 0A800557
 sdlc partner 4900.0008.0557 30
 sdlc dlsw 30
!
```

```
interface Serial2/3
 description TEST LARDPRAO
 no ip address
 encapsulation sdlc
 no ip mroute-cache
 no keepalive
 shutdown
 sdlc role primary
 sdlc vmac 5000.0001.0200
 sdlc address 1C
 sdlc xid 1C 0A100229
 sdlc partner 4900.0001.0229 1C
 sdlc dlsw 1C
!
interface Serial2/4
 no ip address
 no ip mroute-cache
!
interface Serial2/5
 description ### Bangkae-WAN Interface CCT: 0-2238-4898 ###
 mtu 500
 bandwidth 64
 ip address 172.21.137.1 255.255.255.252
 no ip mroute-cache
 no cdp enable
!
interface Serial2/6
 no ip address
!
interface Serial2/7
 no ip address
 shutdown
```

```
!
interface Serial4/0
 description ### Panjathani_1 Port 1/0 TOT-Link CCT:234A876 ###
 bandwidth 2048
 no ip address
 encapsulation ppp
serial restart-delay 0
 ppp authentication chap
 ppp multilink
 multilink-group 1
!
interface Serial4/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial4/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial4/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial5/0:0
 description ### Nakornratchasima-WAN Interface CCT: B03600 ###
 mtu 500
 ip address 172.21.128.1 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
```

```
!
interface Serial5/0:1
 description ### Chonburi-WAN Interface CCT: B03633 ###
 mtu 500
 ip address 172.21.129.129 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:2
 no ip address
 no fair-queue
!
interface Serial5/0:3
 description ### Charoenkrung-WAN Interface CCT: B03507 ###
 bandwidth 64
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 13
 !
interface Serial5/0:4
 description ### Lardprao-WAN Interface CCT: B03659 ###
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 14
!
interface Serial5/0:5
 description ### Chiangmai-WAN Interface CCT: B03436 ###
 bandwidth 64
```

```
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 15
!
interface Serial5/0:6
 description ### Pratunam-WAN Interface CCT: B03596 ###
 bandwidth 64
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 16
!
interface Serial5/0:7
 description ### Chaengwatthana-WAN Interface CCT: B03337 ###
 bandwidth 64
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 17
!
interface Serial5/0:8
 description ### Charoennakorn-Wan Interface CCT: B03510 ###
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 18
!
```

```
interface Serial5/0:9
 description ### Thadindaeng-WAN Interface CCT: B02243 ###
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 19
!
interface Serial5/0:10
 description ### Surawong -Wan Interface CCT:B00045 ###
 mtu 500
 ip address 172.21.137.129 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:11
 description ### Sathupradit-WAN Interface CCT: B03554 ###
 bandwidth 64
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 21
!
interface Serial5/0:12
 description ### Saphanmai-WAN Interface CCT: B03511 ###
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 22
!
```

```
interface Serial5/0:13
 description ### Nananur-WAN Interface CCT: B03339 ###
 bandwidth 64
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 23
!
interface Serial5/0:14
 description ### Phahurat-WAN Interface CCT: B03513 ###
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 24
 !
interface Serial5/0:15
 description ### Sampeng-WAN INterface CCT:B03136 ###
 mtu 500
 ip address 172.21.130.1 255.255.255.252
 random-detect
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:16
 description ### Pradipat-WAN Interface CCT: B01311  ###
 bandwidth 64
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
```

```
 multilink-group 26
!
interface Serial5/0:17
 description ### Sukhumvit 71-WAN Interface CCT:B02256  ###
 bandwidth 64
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 27
!
interface Serial5/0:18
 description ### Mahanak-WAN Interface CCT:B03263 ###
 mtu 500
 ip address 172.21.131.129 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:19
 description ### Nakornpathom-WAN Interface CCT:B02586 ###
 bandwidth 64
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 29
!
interface Serial5/0:20
 description ### Phrapinklao CCT:B03160 ###
 bandwidth 64
 no ip address
 encapsulation ppp
```

```
 ppp authentication chap
 ppp multilink
 multilink-group 30
!
interface Serial5/0:21
 description ### Srinakarintra-WAN Interface CCT:B03545 ###
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 31
!
interface Serial5/0:22
 description ### Khonkaen-WAN Interface CCT:B02571 ###
 bandwidth 64
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 32
!
 interface Serial5/0:23
 no ip address
!
interface Serial5/0:24
 no ip address
!
interface Serial5/0:25
 no ip address
!
interface Serial5/0:26
 no ip address
```

```
!
interface Serial5/0:27
 no ip address
!
interface Serial5/0:28
 no ip address
!
interface Serial5/0:29
 no ip address
!
interface Serial5/0:30
 no ip address
 !
interface Serial5/1:15
 ip unnumbered Loopback0
 encapsulation ppp
 ip tcp header-compression iphc-format
 ip ospf cost 1562
 dialer idle-timeout 2000000
 dialer-group 1
 isdn switch-type primary-net5
 ppp authentication chap
 ppp chap hostname Host1
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 ip rtp header-compression iphc-format
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ip tcp header-compression iphc-format
 ip ospf cost 1562
```

```
 ppp authentication chap
 ppp chap hostname Host1
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 ip rtp header-compression iphc-format
!
router ospf 1
 log-adjacency-changes
 area 1 range 172.21.128.0 255.255.240.0
 network 172.21.103.0 0.0.0.255 area 0
 network 172.21.119.1 0.0.0.0 area 1
 network 172.21.119.11 0.0.0.0 area 1
 network 172.21.128.0 0.0.0.3 area 1
 network 172.21.129.0 0.0.0.3 area 1
 network 172.21.129.128 0.0.0.3 area 1
 network 172.21.130.0 0.0.0.3 area 1
 network 172.21.130.128 0.0.0.3 area 1
 network 172.21.131.0 0.0.0.3 area 1
 network 172.21.131.128 0.0.0.3 area 1
 network 172.21.132.0 0.0.0.3 area 1
 network 172.21.132.128 0.0.0.3 area 1
 network 172.21.133.0 0.0.0.3 area 1
 network 172.21.133.128 0.0.0.3 area 1
 network 172.21.135.0 0.0.0.3 area 1
 network 172.21.135.128 0.0.0.3 area 1
 network 172.21.136.0 0.0.0.3 area 1
 network 172.21.136.128 0.0.0.3 area 1
 network 172.21.137.0 0.0.0.3 area 1
 network 172.21.137.8 0.0.0.3 area 1
 network 172.21.137.128 0.0.0.3 area 1
 network 172.21.138.0 0.0.0.3 area 1
```

```
network 172.21.138.128 0.0.0.3 area 1
network 172.21.140.0 0.0.0.3 area 1
network 172.21.140.128 0.0.0.3 area 1
network 172.21.141.0 0.0.0.3 area 1
network 172.21.141.128 0.0.0.3 area 1
network 172.21.142.0 0.0.0.3 area 1
network 172.21.188.0 0.0.0.3 area 3
network 172.21.188.20 0.0.0.3 area 3
network 172.21.188.32 0.0.0.3 area 3
network 172.21.190.0 0.0.0.3 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.21.103.1
ip route 172.21.180.0 255.255.255.0 172.21.103.254
ip route 172.30.0.3 255.255.255.255 172.21.188.2
ip route 192.168.0.8 255.255.255.255 172.21.188.2
ip route 203.155.210.237 255.255.255.255 172.21.188.2
 no ip http server
ip pim bidir-enable
!
!
ip access-list extended app-dlsw
 permit tcp any any eq 2065
 permit tcp any eq 2065 any
logging trap debugging
logging 11.10.1.101
access-list 11 permit 11.10.0.0 0.0.255.255
access-list 11 permit 172.21.101.0 0.0.0.255
access-list 101 deny   tcp any any eq telnet
access-list 101 deny   tcp any any eq ftp
access-list 101 permit ip any any
access-list 110 permit ip any 192.168.0.0 0.0.255.255
```

```
access-list 200 permit 0x0000 0x0D0D
access-list 200 deny   0x0000 0xFFFF
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
route-map 64only permit 10
 match ip address 110
 set ip next-hop 172.21.188.22
!
 snmp-server community scnbmon RO
snmp-server community scnbsup RW
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps ipmulticast
snmp-server enable traps syslog
snmp-server enable traps dlsw
snmp-server enable traps dial
snmp-server enable traps dsp card-status
snmp-server enable traps voice poor-qov
snmp-server host 11.10.1.101 scnbmon
snmp-server host 172.21.103.243 scnbmon
snmp-server host 172.21.103.244 scnbmon
bridge 1 protocol ieee
!
 voice-port 3/0:0
```

```
!
voice-port 6/0/0
 shutdown
!
voice-port 6/0/1
 shutdown
!
voice-port 6/1/0
 shutdown
!
voice-port 6/1/1
 shutdown
!
dial-peer cor custom
!
!
!
dial-peer voice 101 pots
 destination-pattern 9
 port 6/0/0
!
dial-peer voice 102 pots
 destination-pattern 9
 port 6/0/1
!
dial-peer voice 103 pots
 destination-pattern 9
 port 6/1/0
!
dial-peer voice 104 pots
 destination-pattern 9
 port 6/1/1
```

```
!
dial-peer voice 501 voip
 destination-pattern 06
 session target ipv4:172.21.128.5
 codec g729br8
 ip precedence 5
!
dial-peer voice 502 voip
 destination-pattern 10
 session target ipv4:172.21.129.133
 codec g729br8
 ip precedence 5
!
 dial-peer voice 503 voip
 destination-pattern 19
 session target ipv4:172.21.132.5
 codec g729br8
 ip precedence 5
!
dial-peer voice 506 voip
 destination-pattern 28
 session target ipv4:172.21.133.133
 codec g729br8
 ip precedence 5
!
dial-peer voice 508 voip
 destination-pattern 31
 session target ipv4:172.21.135.133
 codec g729br8
 ip precedence 5
!
dial-peer voice 509 voip
```

```
 destination-pattern 34
 session target ipv4:172.21.136.5
 codec g729br8
 ip precedence 5
 !
dial-peer voice 510 voip
 destination-pattern 01
 session target ipv4:172.21.136.133
 codec g729br8
 ip precedence 5
!
dial-peer voice 511 voip
 destination-pattern 13
 session target ipv4:172.21.137.5
 codec g729br8
 ip precedence 5
!
dial-peer voice 512 voip
 destination-pattern 16
 session target ipv4:172.21.137.133
 codec g729br8
 ip precedence 5
!
dial-peer voice 514 voip
 destination-pattern 23
 session target ipv4:172.21.138.133
 codec g729br8
 ip precedence 5
!
dial-peer voice 515 voip
 destination-pattern 39
 session target ipv4:172.21.140.5
```

```
 codec g729br8
 ip precedence 5
!
dial-peer voice 516 voip
 destination-pattern 42
 session target ipv4:172.21.140.133
 codec g729br8
 ip precedence 5
!
dial-peer voice 601 voip
 destination-pattern 49
 session target ipv4:172.21.144.5
 codec g729br8
 ip precedence 5
!
dial-peer voice 602 voip
 destination-pattern 55
 session target ipv4:172.21.145.133
 codec g729br8
 ip precedence 5
!
dial-peer voice 604 voip
 destination-pattern 67
 session target ipv4:172.21.146.133
 codec g729br8
 ip precedence 5
!
dial-peer voice 605 voip
 destination-pattern 68
 session target ipv4:172.21.147.5
 codec g729br8
 ip precedence 5
```

```
!
dial-peer voice 606 voip
 destination-pattern 69
 session target ipv4:172.21.147.133
 codec g729br8
 ip precedence 5
!
dial-peer voice 607 voip
 destination-pattern 70
 session target ipv4:172.21.148.5
 codec g729br8
 ip precedence 5
!
dial-peer voice 608 voip
 destination-pattern 71
 session target ipv4:172.21.148.133
 codec g729br8
!
dial-peer voice 609 voip
 destination-pattern 72
 session target ipv4:172.21.149.5
 codec g729br8
 ip precedence 5
!
dial-peer voice 610 voip
 destination-pattern 51
 session target ipv4:172.21.149.133
 codec g729br8
 ip precedence 5
!
dial-peer voice 611 voip
 destination-pattern 52
```

```
 session target ipv4:172.21.150.5
 codec g729br8
 ip precedence 5
!
dial-peer voice 612 voip
 destination-pattern 73
 session target ipv4:172.21.150.133
 codec g729br8
 ip precedence 5
!
dial-peer voice 613 voip
 destination-pattern 74
 session target ipv4:172.21.151.5
 codec g729br8
 ip precedence 5
!
dial-peer voice 105 pots
 destination-pattern 9
 port 3/0:0
!
dial-peer voice 106 voip
 destination-pattern 88
 session target ipv4:172.21.190.5
 codec g729br8 bytes 30
!
dial-peer voice 615 voip
 destination-pattern 63
 session target ipv4:172.21.151.133
 codec g729br8 bytes 30
!
dial-peer voice 616 voip
 destination-pattern 14
```

```
 session target ipv4:172.21.129.5
 codec g729br8
!
dial-peer voice 201 voip
 destination-pattern ..
 session target ras
 codec g729br8 bytes 30
!
dial-peer voice 614 voip
 destination-pattern 76
 session target ipv4:172.21.153.133
 codec g729br8
 ip precedence 5
!
 gateway
!
privilege exec level 10 show startup-config
!
line con 0
 exec-timeout 0 0
 password 7 094F471A1A0A
 logging synchronous
line aux 0
 no motd-banner
 no exec-banner
 exec-timeout 0 0
 no flush-at-activation
 no activation-character
 no vacant-message
 modem InOut
 autocommand  telnet CALLED_1 /stream
 transport preferred telnet
```

```
transport output pad v120 telnet rlogin
 escape-character NONE
 databits 7
 parity even
 stopbits 1
 flowcontrol hardware
line vty 0 4
 password 7 110A1016141D
 login
!
exception protocol ftp
exception dump 172.21.103.243
ntp clock-period 17180313
ntp server 11.10.1.1 prefer
end


WAN_Host_1#
WAN_Host_1#
```

ตัวอย่างการกำหนด Configure Parameter ที่อุปกรณ์ Router (CISCO 2600) ที่เชื่อมต่อกับตู้ชุมสายอัตโนมัติ ชนิด Station Port

Branch Office (Phahurat)
Phahurat#sh run Building configuration...   Current configuration : 5113 bytes ! version 12.2 service timestamps debug uptime service timestamps log datetime no service password-encryption ! hostname Phahurat ! logging buffered 65535 debugging aaa new-model aaa authentication login default local aaa authentication login loginauthen group tacacs+ local aaa authentication enable default group tacacs+ enable aaa authentication ppp default local aaa authorization exec default local aaa authorization exec execauthor group tacacs+ if-authenticated local aaa accounting exec execacc start-stop group tacacs+ enable secret 5 1TaAC$NIHrt.U.33PqGW5l82h5O. enable password 7 104D000A0618 ! username scnbadmin privilege 15 password 0 u7tyrg username Host1 password 0 isdn

```
username WAN_Host_1 password 0 scnb
username scnbtelecom privilege 12 password 0 viewonly
ip subnet-zero
!
!
no ip domain-lookup
ip dhcp excluded-address 172.21.140.193 172.21.140.212
!
ip dhcp pool Phahurat
  network 172.21.140.192 255.255.255.192
  default-router 172.21.140.193
  domain-name th.standardchartered.com
  netbios-name-server 172.21.96.8 172.21.103.10
  dns-server 172.21.103.49 10.32.68.49 172.21.96.28
!
virtual-profile virtual-template 1
isdn switch-type basic-net3
call rsvp-sync
!
!
!
dlsw local-peer peer-id 172.21.140.133
dlsw remote-peer 0 tcp 172.21.119.1 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.139.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.188.5 lsap-output-list 200
dlsw bridge-group 1
!
interface Loopback0
 ip address 172.21.140.133 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip id zonePhahurat ipaddr 172.21.119.4 1718
 h323-gateway voip h323-id Phahurat
```

```
h323-gateway voip tech-prefix 1#
!
interface Multilink10
 bandwidth 64
 ip address 172.21.140.130 255.255.255.252
 ip tcp header-compression iphc-format
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 10
 ip rtp header-compression iphc-format
!
interface FastEthernet0/0
 ip address 172.21.140.193 255.255.255.192
 duplex auto
 speed 100
 bridge-group 1
!
interface Serial0/0
 bandwidth 64
 backup delay 300 120
 backup interface BRI0/0
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 multilink-group 10
!
interface BRI0/0
 ip unnumbered Loopback0
 encapsulation ppp
```

```
 ip tcp header-compression iphc-format
 no ip mroute-cache
 dialer string 022069940
 dialer-group 1
 isdn switch-type basic-net3
 ppp authentication chap
 ppp chap hostname ISDN_Phahurat
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 ip rtp header-compression iphc-format
!
interface Serial0/1
 no ip address
 encapsulation sdlc
 no ip mroute-cache
 no keepalive
 sdlc role primary
 sdlc vmac 5000.0001.0200
 sdlc address 0D
 sdlc xid 0D 0A100213
 sdlc partner 4900.0001.0213 0D
 sdlc dlsw D
 !
interface Virtual-Template1
 ip unnumbered Loopback0
 ip tcp header-compression iphc-format
 ip ospf cost 1562
 ppp authentication chap
 ppp chap hostname ISDN_Phahurat
 ppp multilink
 ppp multilink fragment-delay 20
```

```
 ppp multilink interleave
 ip rtp header-compression iphc-format
!
router ospf 1
 log-adjacency-changes
 network 172.21.140.128 0.0.0.3 area 1
 network 172.21.140.133 0.0.0.0 area 1
 network 172.21.140.192 0.0.0.63 area 1
!
ip classless
ip tacacs source-interface Loopback0
no ip http server
ip pim bidir-enable
!
 logging trap debugging
logging 11.10.1.101
access-list 200 permit 0x0000 0x0D0D
access-list 200 deny   0x0000 0xFFFF
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
tacacs-server host 11.10.1.103
tacacs-server key scnbl0ck
snmp-server community scnbmon RO
snmp-server community scnbsup RW
snmp-server trap-source Loopback0
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps dlsw
```

```
snmp-server enable traps dial
snmp-server enable traps voice poor-qov
snmp-server host 11.10.1.101 scnbmon
bridge 1 protocol ieee
!
 voice-port 1/0/0
!
voice-port 1/0/1
!
dial-peer cor custom
!
!
dial-peer voice 101 pots
 destination-pattern 42
 port 1/0/0
!
dial-peer voice 102 pots
 shutdown
 destination-pattern 42
 port 1/0/1
!
dial-peer voice 501 voip
 destination-pattern 9
 session target ras
 codec g729br8 bytes 30
 ip precedence 5
!
 dial-peer voice 502 voip
 destination-pattern ..
 session target ras
 codec g729br8 bytes 30
!
```

```
gateway
!
banner exec ^C
AUTHORIZED ACCESS ONLY
THIS SYSTEM IS THE PROPERTY OF SCNB
DISCONNECT IMMEDIATEDLY IF YOUR ARE NOT AN AUTHORIZED USER !
^C
banner login ^C
AUTHORIZED ACCESS ONLY
THIS SYSTEM IS THE PROPERTY OF SCNB
DISCONNECT IMMEDIATEDLY IF YOUR ARE NOT AN AUTHORIZED USER !
^C
privilege exec level 12 show startup-config
privilege exec level 8 show isdn active
!
line con 0
line aux 0
 modem InOut
 autocommand  udptn 255.255.255.255
 transport output udptn
line vty 0 4
 password 7 045802150C2E
 authorization exec execauthor
 accounting exec execacc
 login authentication loginauthen
!
end


Phahurat#
```

ตัวอย่างการกำหนด Configure Parameter ที่อุปกรณ์ Router (CISCO 2600) ที่เชื่อมต่อกับระบบเครือข่ายระยะไกล้ (LAN) และทำหน้าที่เป็น Gatekeeper

Gatekeeper
Gatekeeper#
Gatekeeper#sh run
Building configuration...
Current configuration : 3941 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log datetime
no service password-encryption
!
hostname Gatekeeper
!
logging buffered 4096 debugging
enable password cisco
!
ip subnet-zero
!
!
!
!
interface Loopback0
ip address 172.21.119.4 255.255.255.255
!
interface FastEthernet0/0
ip address 172.21.103.246 255.255.255.0
duplex auto
speed auto

```
!
router ospf 1
 log-adjacency-changes
 network 172.21.103.0 0.0.0.255 area 0
 network 172.21.119.4 0.0.0.0 area 0
!
ip classless
no ip http server
ip pim bidir-enable
!
!
dial-peer cor custom
!
!
!
gatekeeper
 zone local zonePanjathani scnb.co.th 172.21.119.4
 zone local zonebranch-1 scnb.co.th
 zone local zonebranch-2 scnb.co.th
 zone local zonePhrapinklao scnb.co.th
 zone local zonePradipat scnb.co.th
 zone local zoneNakornratchasima scnb.co.th
 zone local zoneSampeng scnb.co.th
 zone local zoneSukhumvit_71 scnb.co.th
 zone local zoneMahanak scnb.co.th
 zone local zoneCharoenkrung scnb.co.th
 zone local zoneLardprao scnb.co.th
 zone local zoneChiangmai scnb.co.th
 zone local zonePratunam scnb.co.th
 zone local zoneChaengwatthana scnb.co.th
 zone local zoneCharoennakorn scnb.co.th
 zone local zoneThadindaeng scnb.co.th
```

```
zone local zoneBangkae scnb.co.th
zone local zoneSurawong scnb.co.th
zone local zoneSathupradit scnb.co.th
zone local zoneSaphanmai scnb.co.th
zone local zoneNananur scnb.co.th
zone local zonePhahurat scnb.co.th
zone local zoneNakornpathom scnb.co.th
zone local zoneSrinakarintara scnb.co.th
zone local zoneHatyai scnb.co.th
zone local zoneSamutsakorn scnb.co.th
zone local zoneFuturepark scnb.co.th
zone local zonePattanakarn scnb.co.th
zone local zoneRamintra scnb.co.th
zone local zoneLotus_Sukhumvit50 scnb.co.th
zone local zoneLotus_Laksi scnb.co.th
zone local zoneLotus_Rattanatibet scnb.co.th
zone local zoneLotus_Rama3 scnb.co.th
zone local zoneThe_Mall3 scnb.co.th
zone local zoneRatchadaphisek scnb.co.th
zone local zoneSukhumvit_24 scnb.co.th
zone local zoneSamutprakarn scnb.co.th
zone local zoneRayong scnb.co.th
zone local zoneSriracha scnb.co.th
zone local zoneHeadOffice scnb.co.th
zone local zoneKhonkaen scnb.co.th
zone local zoneLotus_Secon scnb.co.th
zone local zoneLotus_Prachachuen scnb.co.th
zone local zoneLotus_Bangkapi scnb.co.th
zone prefix zoneThadindaeng 01*
zone prefix zoneSampeng 04*
zone prefix zoneNakornratchasima 06*
zone prefix zonePradipat 07*
```

```
zone prefix zoneSukhumvit_71 09*
zone prefix zoneMahanak 12*
zone prefix zoneBangkae 13*
zone prefix zoneKhonkaen 14*
zone prefix zoneSurawong 15*
zone prefix zoneSathupradit 18*
zone prefix zoneSaphanmai 23*
zone prefix zoneNakornpathom 24*
zone prefix zoneCharoenkrung 25*
zone prefix zoneLardprao 26*
zone prefix zonePratunam 27*
zone prefix zoneChiangmai 28*
zone prefix zoneChaengwatthana 31*
zone prefix zonePhrapinklao 33*
zone prefix zoneCharoennakorn 34*
zone prefix zoneSrinakarintara 37*
zone prefix zoneNananur 39*
zone prefix zoneRayong 40*
zone prefix zonePhahurat 42*
zone prefix zoneSamutsakorn 46*
zone prefix zoneSriracha 47*
zone prefix zoneHatyai 49*
zone prefix zoneRatchadaphisek 51*
zone prefix zoneSukhumvit_24 52*
zone prefix zoneFuturepark 55*
zone prefix zoneSamutprakarn 63*
zone prefix zonePattanakarn 65*
zone prefix zoneRamintra 67*
zone prefix zoneLotus_Sukhumvit50 68*
zone prefix zoneLotus_Laksi 69*
zone prefix zoneLotus_Rattanatibet 70*
zone prefix zoneLotus_Rama3 71*
```

```
zone prefix zoneThe_Mall3 72*
zone prefix zoneLotus_Prachachuen 73*
zone prefix zoneLotus_Secon 74*
zone prefix zoneLotus_Bangkapi 75*
zone prefix zonePanjathani 88*
zone prefix zoneHeadOffice 9*
gw-type-prefix 1#* default-technology
bandwidth interzone zone zonebranch-1 128
bandwidth interzone zone zonePradipat 128
bandwidth interzone zone zoneLardprao 128
no shutdown
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 password cisco
 login
!
end

Gatekeeper#
Gatekeeper#
```

ผลงานที่ได้รับการตีพิมพ์

1. กมล กลัดคร้าม กอบชัย เดชหาญ และชาลิน สุวรรณวงศ์, "การนำระบบเครือข่าย ATM ประยุกต์ใช้งานร่วมกับระบบ LAN โดยใช้ LAN Emulation," วิศวสารลาดกระบัง ปีที่ 16 ฉบับที่ 1 เดือนมีนาคม 2542
2. กมล กลัดคร้าม กอบชัย เดชหาญ และชาลิน สุวรรณวงศ์, "การนำระบบโทรศัพท์ประยุกต์ร่วม ระบบเครือข่ายข้อมูลส่วนตัว," วิศวสารลาดกระบัง ปีที่ 18 ฉบับที่ 4 เดือนธันวาคม 2544

ประวัติผู้เขียน

นายกมล กลัดคร้าม เกิดเมื่อวันที่ 28 พฤษภาคม 2507 ที่จังหวัดอ่างทอง สำเร็จการศึกษา ครุศาสตร์อุตสาหกรรมบัณฑิต (วิศวกรรมโทรคมนาคม) จากสถาบันเทคโนโลยีราชมงคล ปีการศึกษา 2538 เข้าทำงานตำแหน่งวิศวกรข่ายสื่อสารข้อมูล (Network Engineer) ที่ธนาคารกรุงเทพ จำกัด (มหาชน) ปี พ.ศ. 2528 – 2540 และเข้าทำงานตำแหน่ง Data Communication Engineer ที่ธนาคารนครธน จำกัด (มหาชน) ปัจจุบันตำแหน่ง Technical Specialist สังกัด Global Technology Service Delivery – Network Services ธนาคารสแตนดาร์ดชาร์เตอร์ดนครธน จำกัด (มหาชน)