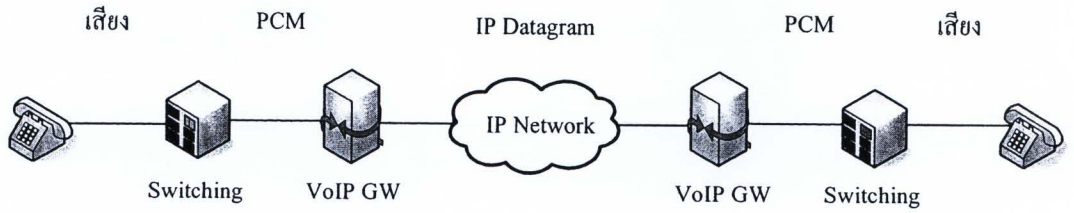
บทที่ 2
แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง

2.1 ความรู้เบื้องต้นเกี่ยวกับโทรศัพท์ไอพี (Minoli Daniel, 1998)

เนื่องจากเครือข่ายไอพีไม่ได้ถูกออกแบบมาให้สามารถรองรับการส่งข้อมูลในรูปแบบของงานประยุกต์ที่ไวต่อเวลาหน่วง (Delay Sensitive Application) ดังนั้นหากมีการออกแบบเครือข่ายไอพีที่ไม่ถูกต้องจะทำให้การส่งผ่านสัญญาณเสียงบนเครือข่ายไอพีไม่มีคุณภาพดีพอหรืออาจไม่สามารถใช้งานได้เลย

การส่งสัญญาณเสียงผ่านเครือข่ายไอพี เป็นระบบที่นำสัญญาณเสียงที่ผ่านการดิจิไตร์ (Digitize) มาบีบอัดแล้วบรรจุลงในแพ็กเก็ตไอพี (IP Packet) เพื่อทำการส่งผ่านทางเครือข่ายไอพี โดยสามารถใช้งานร่วมกับทราฟฟิกไอพี (IP Traffic) อื่นๆ ซึ่งการบีบอัดสัญญาณเสียงให้เล็กลง ทำให้ลดปริมาณการส่งสัญญาณ ลดความล่าช้าของสัญญาณ และลดช่องสัญญาณในการส่งสัญญาณ แต่คุณภาพเสียงที่ได้ก็จะลดลงเช่นกัน

การประยุกต์ส่งสัญญาณเสียงผ่านเครือข่ายไอพีสามารถกระทำได้โดยอาศัยอุปกรณ์ VoIP Gateway ทำหน้าที่แปลงข้อมูลสัญญาณเสียงที่อยู่ในรูปของ Pulse Code Modulation (PCM) ให้อยู่ในรูปของข้อมูลที่พร้อมจะบรรจุใน IP Datagram เพื่อให้สามารถส่งต่อไปในเครือข่ายไอพีดังแสดงในรูปที่ 2.1 ซึ่งเป็นรูปการเชื่อมต่อระหว่างอุปกรณ์ VoIP Gateway, PSTN Switching และเครือข่ายไอพีเข้าด้วยกัน



รูปที่ 2.1 การเชื่อมต่อของอุปกรณ์ในเครือข่ายการส่งสัญญาณเสียงบนไอพี (Minoli Daniel, 1998)

เครือขายไอพีมีรูปแบบการส่งข้อมูลที่เรียกว่า Connectionless ซึ่งเป็นรูปแบบการส่งที่ไม่ต้องมีการสร้างการเชื่อมต่อ (Connection) ระหว่างผู้ส่งและผู้รับกล่าว คือ ข้อมูล 2 ชุดที่ส่งจากผู้

ส่งไปยังผู้รับอาจเดินทางไปคนละเส้นทางจากผู้ส่งไปยังผู้รับก็ได้ และในขณะเดียวกันก็ไม่มีการควบการไหล (Flow Control) เพื่อควบคุมความน่าเชื่อถือของการส่งข้อมูลอันส่งผลให้การส่งข้อมูลแบบ Connectionlessไม่มีการรับประกันว่าข้อมูลสามารถส่งได้ถึงปลายทางหรือไม่ อาจมีการสูญหายของข้อมูล ส่งข้อมูลซ้ำซ้อนหรือส่งข้อมูลผิดลำดับ ซึ่งหากข้อมูลที่ถูกส่งต้องขึ้นอยู่กับเวลา (Delay Sensitive) เช่นเสียงพูด วีดีโอ การส่งแบบ Connectionless จะมีโอกาสทำให้เสียงหรือภาพที่ส่งขาดหายไปเป็นบางช่วงได้

รายละเอียดของเนื้อหาในบทนี้จะเกี่ยวข้องกับปัจจัยต่างๆ ที่จะส่งผลต่อคุณภาพการส่งสัญญาณเสียงบนเครือข่ายไอพี และแนวทางการออกแบบเครือข่ายไอพี เพื่อให้ส่งสัญญาณเสียงบนเครือข่ายไอพีได้อย่างมีคุณภาพ

2.1.1 องค์ประกอบของ VoIP (บงการ หอมนาน, 2547)

2.1.1.1 Software IP Telephony (Soft phone) หรือ โทรศัพท์ไอพี อาจจะเป็นเครื่องคอมพิวเตอร์ที่ได้รับการติดตั้งโปรแกรม หรืออุปกรณ์ที่ได้รับการออกแบบขึ้นมาสำหรับการใช้งานโทรศัพท์ผ่านอินเตอร์เน็ตโดยเฉพาะ

2.1.1.2 VoIP Gateway เป็นเครื่องเซิร์ฟเวอร์ที่ใช้งานสำหรับให้บริการโทรศัพท์ผ่านระบบอินเทอร์เน็ต เพื่อเป็นตัวกลางในการเชื่อมต่อเข้ากับเครื่องโทรศัพท์ตู้ชุมสายโทรศัพท์สาธารณะ PSTN (Public Switched Telephone Network) กับระบบเครือข่ายอินเตอร์เน็ตอย่างเครือข่ายไอพี ซึ่งการจะใช้งานโทรศัพท์ไอพีต้องอาศัยอุปกรณ์ตัวนี้เป็นตัวกลาง VoIP Gateway เป็นอุปกรณ์ในรูปแบบเราเตอร์ที่มีคุณสมบัติเช่นเดียวกับเราเตอร์ที่ใช้งานกันอยู่ แต่มีคุณสมบัติที่ถูกเพิ่มเติมให้รองรับโปรโตคอลการสื่อสารของ VoIP นั้นก็คือ โปรโตคอล H.323, SIP เป็นต้น

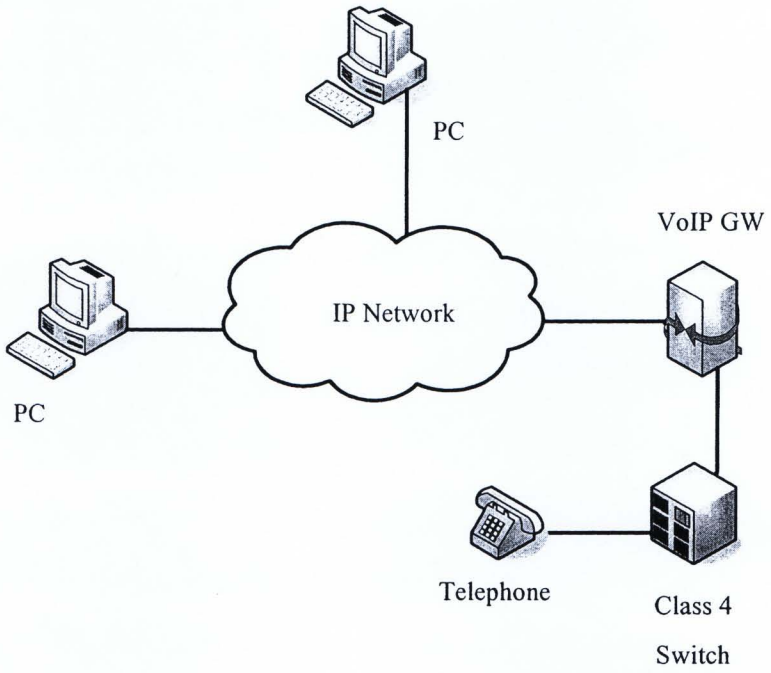
2.1.1.3 SIP Server/Gatekeeper เป็นเครื่องเซิร์ฟเวอร์ที่ถูกเชื่อมต่อเข้ากับระบบอินเทอร์เน็ต เป็นตัวกลางที่ใช้บริหารจัดการและควบคุมการให้บริการของ VoIP Gateway กับเครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมสำหรับใช้งานสื่อสาร VoIP หรือเครื่องโทรศัพท์แบบไอพี แบนด์วิดท์ที่ต้องการในการให้บริการ VoIP โดยทั่วไป แบนด์วิดท์ที่ต้องการขึ้นอยู่กับชนิดของการเข้ารหัสและบีบอัดระบบเสียง(Voice Codec)ซึ่ง VoIP Packet มีขนาดเล็กมากแต่แบนด์วิดท์ส่วนใหญ่จะถูกใช้ไปกับเฮดเดอร์ของ IP และ UDP ซึ่งมีขนาดใหญ่กว่ามาก

2.1.2 ลักษณะการให้บริการโดยทั่วไปของ VoIP

2.1.2.1 แบบเครื่องคอมพิวเตอร์กับเครื่องคอมพิวเตอร์ (PC-to-PC) รูปแบบการใช้งาน VoIP แบบนี้ส่วนใหญ่จะเป็นการพัฒนาต่อยอดจากโปรแกรมประเภท Chat หรือที่เรียกกันว่า Instant messaging ที่แต่เดิมเป็นการส่งข้อความเป็นตัวหนังสือ โดยเพิ่มฟังก์ชั่นในการพูดคุยด้วยเสียงเข้าไปเช่น Google Talk, MSN กล่าวง่ายๆ คือวิธีนี้จำเป็นต้องอาศัยเครื่องคอมพิวเตอร์

ทั้งที่ต้นทางและปลายทาง ซึ่งรูปแบบนี้เป็นวิธีการสื่อสารที่ไม่ต้องเสียค่าบริการโทรศัพท์แต่อย่างใด และต้องนัดแนะเวลาในการใช้อินเตอร์เน็ตในเวลาเดียวกัน ดังแสดงในรูปที่ 2.2

2.1.2.2 แบบเครื่องคอมพิวเตอร์สู่โทรศัพท์ (PC-to-Phone) การใช้งาน VoIP ประเภทนี้เครื่องคอมพิวเตอร์ต้องติดตั้งโปรแกรมที่เรียกว่า Soft phone ซึ่งเป็นโปรแกรมที่จำลองเครื่องโทรศัพท์บนคอมพิวเตอร์เพื่อให้ส่งข้อมูลเสียงไปยังปลายทางที่ไม่ใช่คอมพิวเตอร์ได้ ปัจจุบันมีผู้ให้บริการด้วย Soft phone หลายรายเช่น Skype, TRUE, CAT และ TOT โดยผู้ใช้บริการต้องเสียค่าบริการตามเวลาใช้งานจริง ดังแสดงในรูปที่ 2.2 (Franklin D. Ohrtman, Jr)

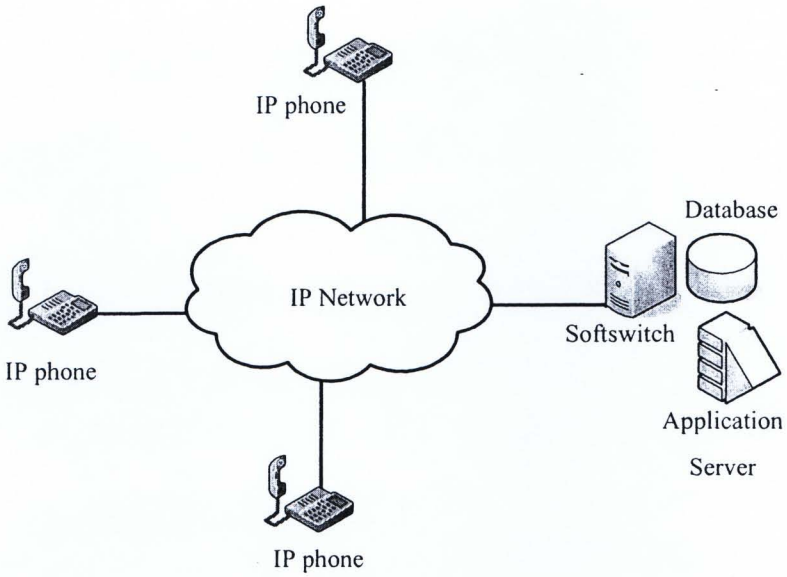


รูปที่ 2.2 การสื่อสารระหว่างเครื่องคอมพิวเตอร์กับเครื่องคอมพิวเตอร์และโทรศัพท์

2.1.2.3 แบบเครื่องโทรศัพท์กับเครื่องโทรศัพท์ (Phone-to-Phone) คือการใช้งาน VoIP แบบเครื่องโทรศัพท์หาเครื่องโทรศัพท์กันเองโดยโทรศัพท์ VoIP มีอยู่สองประเภทคือ

1) โทรศัพท์ปกติที่ต้องเชื่อมต่อกับ ATA (Analog Telephone Adapter) เนื่องจากโทรศัพท์ปกติที่ใช้งานในปัจจุบันไม่สามารถเชื่อมต่อกับโครงข่ายไอพีได้โดยตรง จึงต้องแปลงข้อมูลของเสียงเป็นข้อมูลดิจิตอลแพ็กเก็ตเสียก่อนโดยอาศัยอุปกรณ์ ATA (FXS Gateway) ซึ่งสามารถเชื่อมต่อ VoIP ทั้งโปรโตคอล SIP และ H.323 ผ่านหัวต่อ RJ-11 และ RJ-45 ได้

2) โทรศัพท์ที่สามารถใช้ติดต่อผ่านโครงข่ายไอพีได้เลย (IP Phone) เป็นวิธีที่สะดวกที่สุดในการใช้งาน ดังแสดงในรูปที่ 2.3 (Franklin D. Ohrtman, Jr)



รูปที่ 2.3 การสื่อสารแบบโทรศัพท์กับโทรศัพท์

2.1.3 ขั้นตอนการทำงานของ VoIP

เมื่อผู้พูดโทรศัพท์จากเครื่องโทรศัพท์ธรรมดา หรือพูดผ่านไมโครโฟนที่ถูกต่อเข้ากับการ์ดเสียงของเครื่องคอมพิวเตอร์คลื่นสัญญาณเสียงแบบอนาล็อคก็จะได้รับการแปลงเป็นสัญญาณดิจิตอลจากนั้นจะถูกบีบอัดด้วยตัวอุปกรณ์ VoIP Gateway และเมื่อผ่าน VoIP Gateway แล้วก็จะถูกส่งต่อไปยัง Gatekeeper เพื่อค้นหาเครื่องปลายทางที่จะติดต่อแล้วจะแปลงเป็นแพ็กเกจข้อมูลส่งออกไปบนเครือข่ายอินเตอร์เน็ตเมื่อถึงปลายทางก็จะถูก VoIP Gateway ปลายทางก็จะทำการย้อนกระบวนการทั้งหมดเพื่อให้ฝั่งรับปลายทางต่อไป

2.2 โปรโตคอลที่เกี่ยวข้องกับ VoIP (สาธิตพงษ์ พุทธิประเสริฐและคณะ, 2544)

2.2.1 โปรโตคอล H.323 เป็น VoIP โปรโตคอลตัวแรกที่ได้รับความนิยมกันอย่างแพร่หลาย โดยเริ่มแรกได้รับการพัฒนามาจาก ITU-T's (International Telecommunications Union) standard เพื่อให้บริการ Multimedia conferencing บนโครงข่าย LAN และได้พัฒนาต่อมาเพื่อให้รองรับบริการ VoIP โดย H.323 เวอร์ชั่น แรกได้ประกาศในปี 1996 และตลอกเวลามากกว่า 10 ปี H.323 โปรโตคอลได้มีการแก้ไขเพิ่มเติมเพื่อให้มีบริการเสริมหลากหลายมากขึ้น มีความเสถียรสูงและรองรับการขยายโครงข่ายในอนาคตได้ดีขึ้น ซึ่งในปัจจุบัน H.323โปรโตคอลได้พัฒนาอยู่ที่ Version 5.

ลักษณะของโปรโตคอล H.323

1) เป็น Peer-to-Peer โปรโตคอล ซึ่งหมายถึงอุปกรณ์ปลายทางทั้งสองฝั่งมีความเท่าเทียมกัน(ซึ่งจะแตกต่างจาก MGCP/H.248 โปรโตคอลซึ่งเป็น Master / Slave โปรโตคอล) ดังแสดงในรูปที่ 2.4 (สำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ, 2550)

2) โปรโตคอล H.323 เป็น VoIP protocol suite, หมายถึงภายใต้ H.323 จะมีโปรโตคอลย่อยอื่นๆ เพื่อระบุรายละเอียดการทำงานในแต่ละส่วนเพื่อให้สามารถให้บริการได้ตัวอย่างโปรโตคอลย่อยที่สำคัญของ H.323 ได้แก่ H.225 RAS signaling, H.225.0 Call signaling, H.245 Control signaling, Media coding, H.246 for Interworking issues and etc.

3) มีการ Coding แบบ ASN.1 (binary form)

4) อุปกรณ์หลักใน โปรโตคอล H.323 ประกอบด้วย

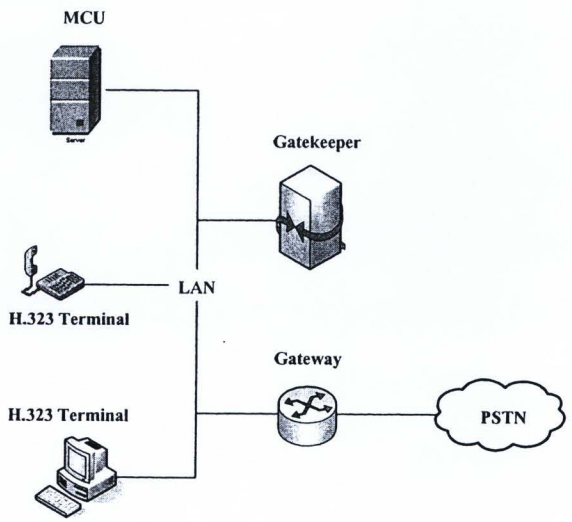
4.1) Terminal เป็นอุปกรณ์ปลายทางของผู้ใช้งาน

4.2) Gatekeeper เป็นอุปกรณ์ควบคุมการเชื่อมต่อของอุปกรณ์ต่างๆ ภายในโครงข่าย H.323

4.3) Gateway เป็นอุปกรณ์ใช้เชื่อมต่อไปยังโครงข่ายอื่นๆ เช่น โครงข่ายโทรศัพท์พื้นฐาน (Fixed Network)

4.4) MCU (Multi Point Control Units) เป็นอุปกรณ์เชื่อมต่อระหว่างผู้ใช้บริการหลายๆ คนให้สามารถ Conferencing ร่วมกันได้

4.5) PSTN (Public Switch Telephone Network) หรือ เครือข่ายโทรศัพท์พื้นฐาน หรือเรียกง่ายๆว่าเครือข่ายโทรศัพท์บ้าน



รูปที่ 2.4 แสดงอุปกรณ์ต่างๆ ในโครงข่าย H.323

2.2.2 โปรโตคอลSIP (Session Initial Protocol) เป็นโปรโตคอลที่ใช้งานสำหรับ IP Telephony แบบ Peer-to-Peer เช่นเดียวกับ H.323 พัฒนาโดย IETF's standard (Internet Engineering Task Force) โดย SIP เป็นโปรโตคอลในชั้นแอพพลิเคชั่นซึ่งทำหน้าที่ในการสร้าง สิ้นสุดและเปลี่ยนแปลงแก้ไขเซสชั่นของพหุสื่อ (Multimedia session) หรือการเรียก ซึ่งรวมถึง Internet Telephony การประชุมแบบพหุสื่อ (Multimedia conference) และแอพพลิเคชั่นอื่นที่คล้ายคลึงกัน SIP เป็นโปรโตคอลไคล์แอนท์-เซิร์ฟเวอร์ (client-server) โดยการใช้ส่งข้อมูลในรูปของตัวอักษร (text based) เช่นเดียวกับโปรโตคอล HTTP (Hypertext Transfer Protocol) รวมทั้งยังมีกลไกที่คล้ายคลึงกัน ทำให้สามารถใช้เฮดเดอร์และกลไกที่มีอยู่บางอย่างของ HTTP ได้โดยรองรับได้มากกว่าหนึ่งอุปกรณ์ในคราวเดียวกัน โดยบริการที่รองรับได้ไม่จำกัดเฉพาะ VoIP session เท่านั้น แต่ SIP โปรโตคอลยังสามารถรองรับบริการอื่นได้อีกเช่น Instant Massaging ,Presence และอื่นๆ

โดย IETF ประกาศมาตรฐาน SIP ครั้งแรกในปี 1999 และได้มีการพัฒนาเพิ่มเติมมาเรื่อย ดังตัวอย่างต่อไปนี้

1) ในปี 1999 ได้ออกแบบ มาตรฐาน SIP RFC 2543, 153 ASCII pages

2) ในปี 2000 3GPP(Third generation mobile) ได้เลือก SIP โปรโตคอลเป็นมาตรฐานในการสื่อสารบนโครงข่ายโมบาย ซึ่งในอนาคตจะส่งผลให้ โปรโตคอล SIP เป็นที่นิยมอย่างแพร่หลายมากขึ้นและมีข้อกำหนดเกี่ยวกับโปรโตคอล SIP อื่นๆเพิ่มเติมอีกหลายตัวเพื่อให้โปรโตคอล SIP สามารถใช้ในโครงข่ายโมบายได้อย่างมีประสิทธิภาพ

3) ในปี 2002 ได้ออก มาตรฐาน SIP ตัวใหม่ RFC 3261, 270 ASCII pages

4) จนถึงปัจจุบันก็ยังคงมีข้อกำหนดอื่นๆเกี่ยวกับโปรโตคอล SIP ออกมาอยู่เรื่อยๆ

2.2.2.1 ลักษณะของโปรโตคอล SIP

1) เป็นโปรโตคอล Peer-to-Peer เช่นเดียวกับโปรโตคอล H.323 และดูจะเหมือนว่าจะมาทดแทน โปรโตคอล H.323 ในอนาคตอันใกล้นี้

2) มีการ Coding แบบ ISO UTF-8 (Text based) สามารถอ่านข้อมูลในโปรโตคอลได้ง่าย

3) รูปแบบข้อมูลมีลักษณะใกล้เคียงที่ใช้ใน Internet protocol (HTTP syntax) มีความยืดหยุ่นสูง

4) การระบุปลายทาง (addressing scheme) ใช้ ULR ซึ่งทำให้สามารถรองรับได้ทั้ง phone number, IP address และ e-mail address

5) อุปกรณ์หลักใน SIP โปรโตคอลดังแสดงในรูปที่ 2.5 (สำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ, 2550) ซึ่งจะประกอบด้วย

2.2.2.1.1 User Agents เป็นอุปกรณ์ปลายทางสำหรับผู้ใช้ (SIP user) สามารถแบ่งได้ 2 ประเภท

1) User Agent Client (UAC) โดย UAC จะเป็นผู้เริ่มต้นร้องขอ SIP request

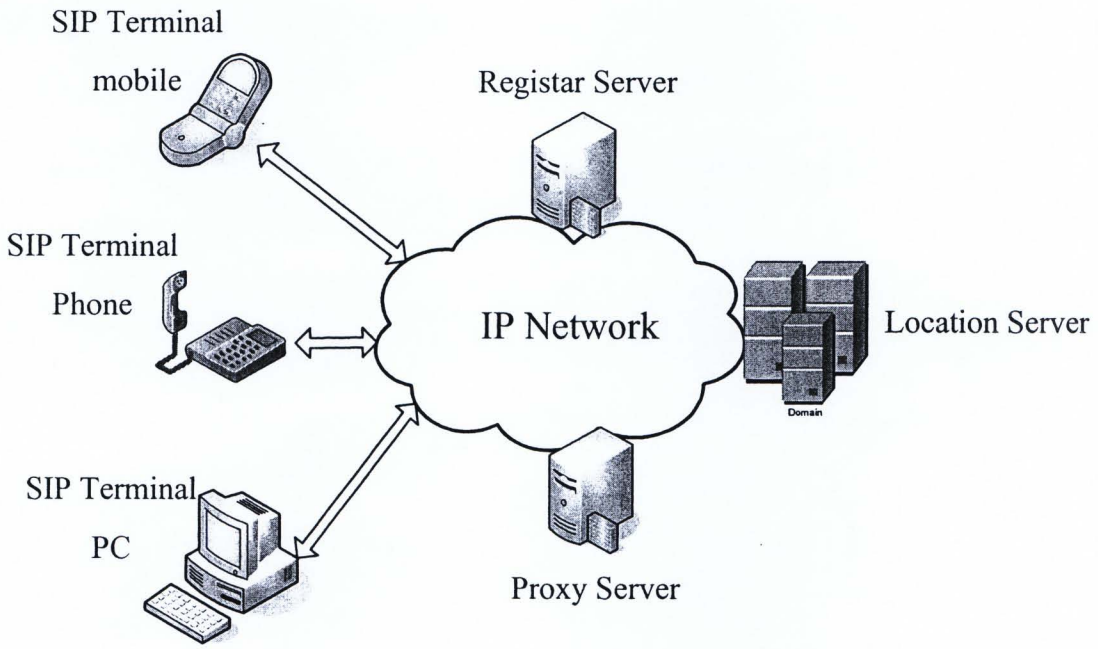
2) User Agent Server (UAS) โดย UAS จะเป็นผู้รับ SIP request และตอบกลับ

2.2.2.1.2 Network Servers เป็นอุปกรณ์ในโครงข่ายมีอยู่ 3 ประเภทด้วยกันคือ

1) Registrar server ทำหน้าที่รองรับการลงทะเบียนของผู้ใช้บริการ (SIP user)

2) proxy server ทำหน้าที่รองรับการส่งต่อข้อมูลไปยัง server ถัดไป

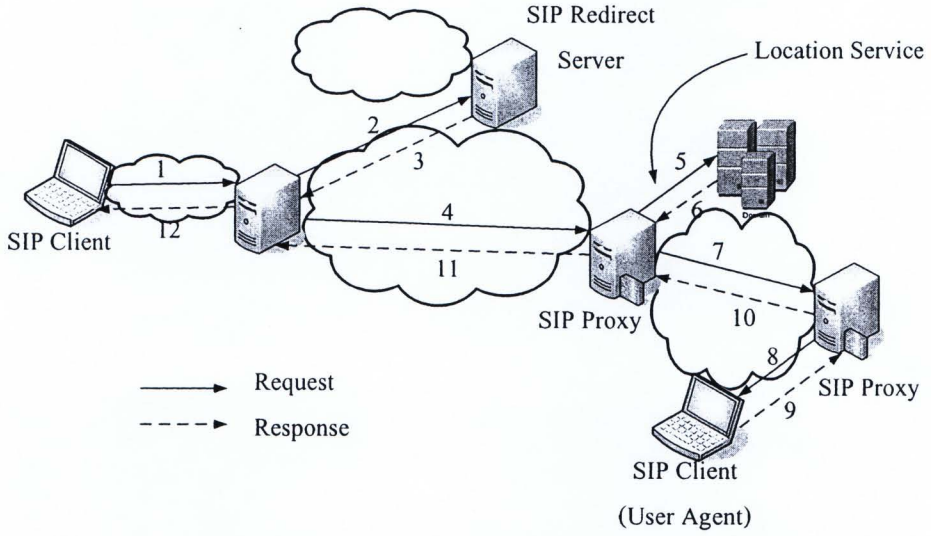
3) redirection server ทำหน้าที่รองรับ ตัดสินใจระบุทิศทางและที่อยู่ของ server ถัดไป



รูปที่ 2.5 แสดงอุปกรณ์ต่างๆ ในโครงข่ายโปรโตคอล SIP

2.2.2.2 สถาปัตยกรรมและองค์ประกอบของโปรโตคอล SIP (SIP Architecture & Components) โดย SIP เป็นโปรโตคอลไคลเอนท์-เซิร์ฟเวอร์ ไคลเอนท์จะทำหน้าที่ส่งคำร้องขอให้กับเซิร์ฟเวอร์เพื่อทำการประมวลผลแล้วจึงตอบสนองมายังไคลเอนท์ ในการส่งข้อมูลร้องขอแมสเสจ

อาจจะถูกส่งผ่านเซิร์ฟเวอร์หลายตัว จนกระทั่งถึงเซิร์ฟเวอร์ที่สามารถตอบสนองคำร้องของไคลเอนท์ได้ในระบบ SIP จะมีองค์ประกอบที่ทำหน้าที่ของไคลเอนท์และเซิร์ฟวอร์ องค์ ประกอบเหล่านี้จะทำการติดต่อสื่อสารกันโดยตรงโดยใช้แมสเสจ SIP ซึ่งมีสถาปัตยกรรมดังรูปที่ 2.6 (สาธิต พงษ์ พุทธิประเสริฐและคณะ, 2544)



รูปที่ 2.6 สถาปัตยกรรมของ SIP

ใน SIP จะแบ่งองค์ประกอบเป็น 2 ชนิดหลักคือ user agent และ network agent ดังรายละเอียดดังต่อไปนี้

2.2.2.2.1 User Agent เป็น endpoint ที่ทำหน้าที่แทนผู้ใช้ในการติดต่อสื่อสาร เนื่องจากว่าผู้ใช้ต้องสามารถเริ่ม การเรียก หรือตอบสนองต่อการเรียกที่เข้ามา ดังนั้น user agent ควรจะสามารถทำหน้าที่เป็นได้ทั้งไคลเอนท์และเซิร์ฟเวอร์ในกรณีที่มีการเริ่ม การเรียก ผู้ใช้จะทำหน้าที่เป็นไคลเอนท์เพื่อทำการร้องขอการสื่อสารไปยังผู้ถูกเรียกซึ่งจะทำหน้าที่เป็นเซิร์ฟเวอร์ในการตอบสนองการร้องขอ โดยทั่วไป user agent จึงประกอบด้วยส่วนที่ทำหน้าที่เป็นไคลเอนท์และเซิร์ฟเวอร์ดังนี้

1) ผู้ใช้ฝั่งไคลเอนท์ (User Agent Client: UAC) จะทำหน้าที่ในการเริ่ม การเรียก โดยการส่งแมสเสจร้องขอไปยังผู้ถูกเรียกโดยผ่านทางเซิร์ฟเวอร์เครือข่าย

2) ผู้ใช้ฝั่งเซิร์ฟเวอร์ (User Agent Server: UAS) จะทำหน้าที่ในการรับคำร้องขอและตอบสนองต่อคำร้องขอโดยจะรอการตอบสนองจากผู้ใช้ ซึ่งการตอบสนองอาจจะ

เป็นการยอมรับหรือปฏิเสธ การเรียก ในกรณีที่ผู้ใช้มีการใช้เทอร์มินัลหลายตัว ผู้ใช้ยังอาจจะกำหนดให้ UAS ทำการส่งต่อการเรียก (redirect)ไปยังที่ UAS อื่น ที่ผู้ใช้ใช้งานอยู่จริง

2.2.2.2.2 Network server เป็นเซิร์ฟเวอร์ภายในเครือข่ายซึ่งจะทำหน้าที่ในการจัดการกับแมสเสจที่ได้รับ โดยอาจจะได้รับจาก user agent หรือ network server อื่นๆการจัดการกับแมสเสจจะขึ้นกับชนิดของเซิร์ฟเวอร์ ซึ่งมี 2 ชนิด

1) พร็อกซี่เซิร์ฟเวอร์ (Proxy server) จะทำการกำหนดเอนทิตี้ที่ได้รับข้อมูลต่อไป โดยอาจจะเป็น UAS หรือ network server ก็ได้ จากนั้นเซิร์ฟเวอร์จะเป็นผู้ทำการร้องขอไปยังเอนทิตี้นั้น พร้อมกับข้อมูลตอบสนองให้กับ UAC (หรืออาจจะเป็น network server อื่นที่ส่งข้อมูลร้องขอมา) เพื่อระบุว่ากำลังรอการตอบสนองจากผู้ถูกเรียก เมื่อเซิร์ฟเวอร์ได้รับการตอบเสนองจากผู้ถูกเรียกหรือ UAS เซิร์ฟเวอร์จึงจะส่งแมสเสจตอบสนองต่อกลับไปให้กับ UAC ดังรูปที่ 2.6 เซิร์ฟเวอร์ชนิดนี้จะทำหน้าที่เป็นทั้งไคลเอนท์และเซิร์ฟเวอร์ ในกรณีที่ส่งแมสเสจร้องขอจะเป็นไคลเอนท์ส่วนในกรณีที่ส่งข้อมูลตอบสนองจะเป็นเซิร์ฟเวอร์

2) รีไดเร็ก เซิร์ฟเวอร์ (Redirect server) เมื่อเซิร์ฟเวอร์ได้รับแมสเสจร้องขอแล้วจะกำหนดแอนทิตี้ที่จะรับข้อมูลต่อไป จากนั้นเซิร์ฟเวอร์ก็จะส่งแอดรสของแอนทิตี้นั้นไปให้กับUAC หรือnetwork server ที่ส่งข้อมูลร้องขอมา เมื่อUAC (network server) ได้รับแอดเดรสแล้วจึงจะส่งคำร้องไปยังเซิร์ฟเวอร์นั้นด้วยตนเองดังรูปที่ 2.6

เนื่องจากว่าผู้ใช้อาจจะมีการเปลี่ยนแปลเทอร์มินัลที่ใช้งานได้ ดังนั้น network server จึงจะต้องสามารถกำหนดเอนทิตี้ที่รับข้อมูลเพื่อให้สามารถส่งแมสเสจให้กับผู้ถูกเรียกได้ โดย network server จะทำการติดต่อกับ location server เพื่อทำการกำหนดเอนทิตี้ต่อไปที่จะรับแมสเสจ location server จะทำหน้าที่ในการหาตำแหน่งปัจจุบันของผู้ถูกเรียกโดยการกำหนดเอนทิตี้ที่จะรับแมสเสจต่อไป แล้วส่งแอดเดรสของเอนทิตี้ให้กับ network server ข้อมูลของ location server จะได้รับจาก registrar ซึ่งทำหน้าที่ในการรับข้อมูลเกี่ยวกับตำแหน่งของผู้ใช้ แล้วส่งข้อมูลนี้ให้กับ location server ในการให้ข้อมูลของผู้ใช้กับ registrar จะทำได้โดยการใช้แมสเสจ REGISTER เพื่อบอกตำแหน่งที่อยู่ของผู้ใช้ โดยทั่วไปแล้ว registrar จะถูกรวมเข้ากับ network server

2.2.2.3 ชื่อและแอดเดรส (Addressing & Naming) ในระบบ SIP การส่งแมสเสจระหว่างเอนทิตี้จะต้องระบุ SIP URL เพื่อใช้อ้างอิงถึงผู้ใช้ SIP URL จะประกอบด้วย SIP Address รูปแบบของแอดเดรสจะอยู่ในรูปของ name@domain โดยอาจจะเป็น user@domain user@address phone-number@gateway และ user@host แอดเดรสนี้จะถูกใช้อ้างอิงถึงผู้ใช้ทั้งผู้เรียกและผู้ถูกเรียกในการส่งแมสเสจ ตัวอย่างของ SIP URL เช่น SIP ://j.doe@example.com โดยที่ URL นี้จะอยู่ในส่วนของแอดเดอร์ของแมสเสจ ในการส่งแมสเสจไปยัง SIP URL ที่ระบุไว้จะต้องมีการแปลง SIP

แอดเดรสให้อยู่ในรูปของ user@host โดยอาจจะผ่านการแปลงมากกว่าหนึ่งครั้งจนกระทั่งได้ตำแหน่งที่อยู่ของผู้ใช้ ในการแปลงแอสเดรสอาจจะใช้ DNS (Domain Name Server) หรือ LDAP (Lightweight Driectory Access Protocol)

2.2.2.4 Locating Server ในการส่งแมสเสจจะใช้ SIP URL อ้างอิงถึงในการส่ง โดยจะต้องมีการแปลงส่วนโดเมนของ SIP แอสเดรสไปเป็นหมายเลขไอพี ซึ่งเป็นแอสเดรสของ SIP Server ที่สามารถค้นหาตำแหน่งของผู้ใช้ต่อไปได้ การแปลง SIP แอสเดรสอาจทำโดย UAC หรือ UAC จะส่งแมสเสจให้กับเซิร์ฟเวอร์ที่กำหนดซึ่งเซิร์ฟเวอร์จะเป็นผู้ที่ทำหน้าที่ในการแปลง SIP แอดเดรสแทน ในการแปลง SIP แอดเดรสนี้สามารถใช้ DNS เข้ามาช่วยได้

2.2.2.5 Locate User จากข้างต้น เมื่อได้ตำแหน่งของเซิร์ฟเวอร์ที่ส่งข้อมูลมาให้กับผู้ถูกเรียกแล้วต่อไปจะเป็นการหาตำแหน่งของผู้ถูกเรียก เมื่อ SIP Server ได้รับแมสเสจร้องขอแล้วเซิร์ฟเวอร์จะต้องการค้นหาผู้ใช้ที่อ้างอิงถึงใน SIP แอสเดรส โดยการร้องขอข้อมูลไปยัง Location server ซึ่งจะตอบกลับด้วยรายการตำแหน่งที่เป็นไปได้ของผู้ถูกเรียก เมื่อ SIP server ได้ข้อมูลเกี่ยวกับตำแหน่งของผู้ถูกเรียกแล้ว ถ้าเป็น proxy server จะทำการส่งแมสเสจร้องขอต่อไปยังตำแหน่งต่างๆ ตามรายการที่ได้รับการ location serverไว้ โดยอาจจะส่งแบบ sequential หรือ parallel ส่วนถ้าเป็น redirect server จะส่งรายการตำแหน่งของผู้ถูกเรียกไปให้ผู้เรียกผ่านโดยการใช้เฮดเดอร์ contact เพื่อให้ผู้เรียกส่งแมสเสจร้องขอไปเอง สำหรับตำแหน่งของผู้ใช้จะต้องทำการลงทะเบียนกับ registrar โดยใช้เฮดเดอร์ REGISTER รวมทั้งยังอาจจะอัพโหลด script ของผู้ใช้งานเองเพื่อเก็บไว้ที่เซิร์ฟเวอร์สำหรับจัดการกับการเรียกตามความต้องการของผู้ใช้

2.2.2.6 ความน่าเชื่อถือ (Reliabillity) ในระบบ SIP จะมีกลไกเรื่องความเชื่อถือได้ไม่ว่าจะใช้โปรโตคอล UDP หรือ TCP โดยการใช้เมธอด Ack ไคล์เอนท์จะส่งแมสเสจร้องขอใหม่ตามช่วงเวลาที่กำหนดจนกระทั่งได้รับแมสเสจตอบจากเซิร์ฟเวอร์ ทางด้านเซิร์ฟเวอร์ก็จะส่งแมสเสจตอบจนกระทั่งได้รับแมสเสจ Ack จากไคล์เอนท์จึงทำให้การร้องขอที่สมบูรณ์ต้องใช้การแลกเปลี่ยนแมสเสจ 3 แมสเสจ เซิร์ฟเวอร์อาจจะตอบสนองต่อ Ack ในการส่งแมสเสจตอบสุดท้ายไปให้กับไคลเอนท์ซึ่งอาจจะไม่จำเป็นต้องมีก็ได้ สำหรับการส่งมีเดียสตรีมเซิร์ฟเวอร์จะยอมจะมีการส่งเมื่อได้รับ Ack จากไคล์เอนท์เท่านั้นด้วยกลไกนี้จึงทำให้เกิดความน่าเชื่อถือได้ในการแลกเปลี่ยนแมสเสจโดยไม่จำเป็นต้องอาศัยกลไกของโปรโตคอลในชั้นต่ำกว่า เช่น TCP

2.2.2.7 ความสามารถในการขยาย (Protocol extension) SIP สามารถรองรับคุณลักษณะใหม่ที่เพิ่มเติมขึ้นสำหรับเมธอด เฮดเดอร์ และ status code ดังนี้

1) เมธอด เซิร์ฟเวอร์จะส่งแมสเสจแสดงความผิดพลาด (Error message) กลับมาให้ไคลเอนท์ถ้าเมธอดที่ร้องขอมาเซิร์ฟเวอร์ไม่เข้าใจและจะบอกเมธอดที่เซิร์ฟเวอร์เข้าใจโดยใช้

เฮดเดอร์ Public และ Allow ไคล์เอนท์อาจจะส่งแมสเสจร้องขอเพื่อขอทราบเมธอดที่เซิร์ฟเวอร์สนับสนุนโดยใช้ตัวเลือกที่เฮดเดอร์ (header option)

2) เฮดเดอร์ เมื่อเอนทิตี้ได้รับเฮดเดอร์ที่ไม่เข้าใจก็จะละทิ้งเฮดเดอร์นั้นในกรณีที่ไคลเอ้นท์จำเป็นต้องการใช้เฮดเดอร์บางเฮดเดอร์ไคล์แอนท์จะส่งแมสเมสจเพื่อร้องขอเฮดเดอร์ที่จำเป็นต้องใช้ไปโดยระบุบในเฮดเดอร์ Require หากมีเฮดเดอร์ที่เซิร์ฟเวอร์ไม่สามารถให้การสนับสนุนได้เซิร์ฟเวอร์จะตอบปฏิเสธกลับมา

3) Status code ได้แบ่งเป็นคลาสต่างๆ เช่นเดียวกับ Response code ของโปรโตคอล HTTP ซึ่งไคล์เอนท์ต้องเข้าใจในความหมายในแต่ละคลาสเพื่อที่จะได้ทราบผลของการร้องขอว่าสำเร็จหรือไม่ สำหรับ status code ในแมสเสจตอบจะมีข้อความต่อหลังซึ่งจะเป็นความหมายของ code ซึ่งสามารถอ่านเข้าใจได้ โดยถ้าไคล์เอ้นท์ไม่ใจในรายละเอียดของ code ทั้งหมด ไคล์เอนท์จะตีความหมายเป็น XOO เมื่อ X เป็นตัวเลขตัวแรกของ status code และนอกจากนี้อาจจะนำ PEP (Protocol extention protocol) มาปรับปรุงใช้งานกับ SIPได้

ในกรณีมีการส่งแมสเสจผ่านเซิร์ฟเวอร์หลายตัวจะใช้เฮดเดอร์ Via เพื่อระบุบเซิร์ฟเวอร์ที่เป็นทางผ่านของแมสเสจทั้งหมด สำหรับใช้ในการส่งแมสเสจตอบสนองจะมีการตอบตกลงเกี่ยวกับพารามิเตอร์ของเซสชั่นด้วย ซึ่งรายละเอียดจะอยู่ในส่วนของ message body เช่นในกรณีของการสื่อสารโดยใช้เสียง พารามิเตอร์จะเป็น IP Address พอร์ตสำหรับ RTP และการเข้า/ถอดรหัสเสียงหลังจากการสร้าง การเรียก เสร็จสมบูรณ์ ช่องสัญญาณสำหรับ RTP จะถูกสร้างขึ้นทำให้ทั้งสองฝ่ายสามารถสื่อสารกันได้รวมทั้งยังอาจจะเชิญผู้อื่นมาเข้าร่วมในเซสชั่นนี้ได้ ในกรณีที่ต้องการเปลี่ยนพารามิเตอร์ของเซสชั่นสามารถทำได้โดยส่งแมสเสจร้องของใหม่อีกครั้งโดยใช้วิธีการ invite ซึ่งมี call-id เดิม ไปยังผู้ร่วมเซสชั่นพร้อมทั้งค่าพารามิเตอร์ของเซสชั่นใหม่ที่ต้องการใช้รายละเอียดในส่วนนี้จะอยู่ในส่วนของ message body ซึ่งโดยทั่วไปจะใช้โปรโตคอล SDP (Session Description Protocol) ในการอธิบายความหมาย

2.2.3 เปรียบเทียบ H.323 กับ SIP โปรโตคอล เนื่องจากการพัฒนา H.323 โปรโตคอลได้ถูกพัฒนาโดยมีพื้นฐานมาจาก ATM และ ISDN จึงทำให้ H.323 โปรโตคอลยังมีข้อจำกัดอยู่หลายประการในการให้บริการ VoIP โดยเฉพาะเมื่อเปรียบเทียบกับ SIP โปรโตคอล ซึ่งถูกพัฒนาโดยพื้นฐานของ Internet โดยตรง H.323 โปรโตคอลจึงมีความยืดหยุ่นต่ำ รองรับกาขยายตัวของโครงข่ายต่ำ และมีความซับซ้อนสูงเมื่อเทียบกับ SIP โปรโตคอล เช่น H.323 โปรโตคอลได้มีการกำหนด element ต่างๆ นับร้อยในขณะที่ SIP โปรโตคอลมีแค่ 37 headers โดยจะแสดงข้อแต่ต่างในตารางที่ 2.1 (สำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ, 2550)

ตารางที่ 2.1 ข้อเปรียบเทียบระหว่าง H.323 โปรโตคอลกับ SIP โปรโตคอล

หัวข้อ	H.323	SIP
ความซับซ้อน	สูง	ต่ำ
จำนวน Message set	มาก	น้อย
การ Debug	ต้องการอุปกรณ์เสริมที่มีความซับซ้อน	ต้องการอุปกรณ์เสริมไม่ซับซ้อน
การรองรับการขยายตัวในอนาคต	ต่ำ	สูง
ความยืดหยุ่นเพื่อรองรับบริการอื่น	ต่ำ	สูง
รองรับ Telephone service	เชื่อถือได้	เชื่อถือได้
ความสิ้นเปลืองใน Processor/Memory usage	สูง	ต่ำ
ความแพร่หลาย	สูง แต่คาดว่าจะถูกแทนที่โดย SIP ในอนาคตอันใกล้นี้	สูง และคาดว่าจะเป็นโปรโตคอลหลัก แทนที่ H.323

ฉะนั้นจึงพอสรุปได้ว่า SIP จะเป็นโปรโตคอลที่จะใช้ทดแทน H.323 โปรโตคอลในอนาคตอันใกล้ทั้งในส่วนโครงข่าย Fixed และ Mobile

2.2.3 เรียวทามโปรโตคอล (Real Time Protocol : RTP) (Schlzrinne H, 1996)

Real Time Protocol (RTP) ถูกออกแบบมาเพื่อใช้สนับสนุนการส่งข้อมูลแบบเวลาจริง (Real Time Traffic) ที่ต้องการส่งข้อมูลและรับข้อมูลในช่วงเวลาที่สั้นมากๆ ตัวอย่างการส่งข้อมูลแบบเวลาจริงเช่น การส่งข้อมูลเสียงของการสนทนาระหว่างคู่สนทนา การส่งภาพของภาพยนตร์จากเครื่องส่งไปยังผู้รับหรือผู้ชมปลายทาง

RTP เป็นโปรโตคอลที่ทำงานในระดับ Transport Layer โดยการทำงานร่วมกับ UDP กล่าวคือ ข้อมูลสัญญาณเสียงที่ถูกส่งมาจากระดับชั้นบนจะถูกใส่ข้อมูลส่วนหัวของ RTP ก่อนที่จะส่งต่อให้ UDP ซึ่งอยู่ในระดับ Transport Layer เช่นเดียวกับ RTP จากนั้นข้อมูลจะถูกส่งต่อไปยัง Network Layer (IP) ต่อไป RTP ถูกออกแบบมาให้มีส่วนของการกำกับเวลา (Time Stamp) ในส่วนหัวของ RTP แพ็คเก็ต เพื่อใช้เป็นข้อมูลในการเข้าจังหวะข้อมูลสำหรับผู้รับปลายทาง เพื่อให้มีความมั่นใจ ได้ว่าลำดับของข้อมูลที่ได้รับมาแล้วที่ถูกส่งต่อขึ้นไปให้ชั้นที่สูงกว่ามีความถูกต้อง และถูกลำดับแน่นอน ดังนั้นรูปแบบการทำงานของ RTP จึงมี 2 หน้าที่หลักคือ

1) RTP ทำหน้าที่เป็น Translator แปลง Syntax ของข้อมูลที่ได้รับเข้ามา ให้เป็นข้อมูลส่งออกที่มี Syntax อีกแบบที่เหมาะสมกับเครื่องคอมพิวเตอร์ปลายทาง

2) RTP ทำหน้าที่เป็น Mixer รวมข้อมูลที่มาจากต้นทางหลายๆ แหล่ง ให้เป็นข้อมูลส่งออกที่รวมกันเป็นข้อมูลสายเดียวกัน

2.3 ความรู้เบื้องต้นเกี่ยวกับ Voice Codec (วาริน เล้าสกุล, 2544)

VoIP จะมีการแปลงสัญญาณเสียงที่อยู่ในรูปแบบของ PCM ให้เป็นรูปแบบใหม่ เพื่อใช้ส่งไปในเครือข่ายไอพีนั้น จะต้องแปลงสัญญาณเสียงให้อยู่ในรูปแบบของดิจิตอล (CODEC) โดยรูปแบบของ CODEC ที่นิยมใช้กันในปัจจุบันคือ G.711, G.729 และ GSM

หน้าที่ของตัวแปลงสัญญาณเสียงที่ต้นทางคือ การเข้ารหัสข้อมูล PCM ของสัญญาณเสียงที่ได้รับมาให้อยู่ในรูปของข้อมูลแบบใหม่ที่มีขนาดเล็กลง และที่ปลายทางอุปกรณ์ตัวแปลงสัญญาณเสียง ก็จะทำหน้าที่ในการถอดรหัสข้อมูลที่ได้รับมาให้กลับมาอยู่ในรูปแบบของข้อมูล PCM ของสัญญาณเสียงเหมือนเดิม จากนั้นจึงจะเป็นหน้าที่ของอุปกรณ์อื่นต่อไปที่จะทำหน้าที่แปลงข้อมูล PCM ให้เป็นสัญญาณเสียงแล้วส่งต่อไปยังผู้รับปลายทาง

รายละเอียดการเปรียบเทียบคุณสมบัติด้านต่างๆ ของการแปลงสัญญาณเสียงในมาตรฐานต่างๆ สามารถแสดงดังในตารางที่ 2.2

ตารางที่ 2.2 เปรียบเทียบคุณสมบัติของการแปลงสัญญาณเสียงของมาตรฐานต่างๆ

ชนิดของ CODEC	Data Rate	MOS
G.711	64 kbps	4.20
GSM	13.2 kbps	3.57
G.729	8 kbps	3.91

ที่มา: วินโด ไอทีโปร (Windows IT Pro), 2542.

2.4 คุณลักษณะของเครือข่ายที่มีผลกระทบต่อคุณภาพเสียง (พรภัทร ภัทรจารี, 2548)

QoS (Quality of Service) เป็นการจัดลำดับความสำคัญของข้อมูลในระดับ Application โดยที่การทำงานของเทคโนโลยี Quality of Service (QoS) นั้น จะเป็นการจัดแบ่งประเภทของข้อมูล Application ออกเป็นหมวดหมู่ และมีการจัดลำดับความสำคัญของข้อมูล Application ในแต่ละหมวดหมู่นั้นๆ ซึ่งจะทำให้เราสามารถที่จะควบคุม Bandwidth ในระบบเครือข่ายของเราให้ใช้ประโยชน์ได้สูงสุดตาม Application ต่างๆ ที่เราต้องการ

QoS (Quality of Service) เข้ามาช่วยเป็นเกณฑ์มาตรฐานที่ใช้ในการวัดการรับส่งข้อมูล และการยอมรับในเรื่องคุณภาพของการให้บริการต่างๆ ซึ่งการยอมรับในเรื่องคุณภาพเป็นระดับที่ยากแก่การกำหนดว่า มาตรฐานคุณภาพในเครือข่ายสื่อสารเป็นอย่างไร ซึ่งผลกระทบทีมีต่อคุณภาพของเสียงบนเครือข่ายไอพีมีดังนี้

2.4.1 ความล่าช้า (Delay) ในการส่งสัญญาณข้อมูลเสียงแบบแพ็คเก็ตเกิดจากการรวบรวมสัญญาณที่สุ่มตัวอย่างจากสัญญาณเสียง เวลาในการเข้ารหัส/ถอดรหัส เวลาในการเข้าแพ็คเก็ต Jitter buffer delay และความล่าช้าของเน็ตเวิร์ค ปัญหาที่เกิดจากความล่าช้าของสัญญาณจากปลายสายหนึ่งถึงอีกปลายสายหนึ่งในเครือข่ายสัญญาณเสียงคือ เสียงสะท้อน และผู้พูดพูดซ้อนกัน จะเกิดเสียงสะท้อน(echo)ขึ้นเมื่อความล่าช้าของเสียงที่เดินทาง 1 รอบมีค่ามากกว่า 50 ms ระบบ VoIP จำเป็นจะต้องมีการความคุมเสียงสะท้อนและโปรแกรมกำจัดเสียงสะท้อน การที่ผู้พูดพูดซ้อนกัน (talker overlap) จะเป็นปัญหาสำคัญเมื่อความล่าช้าของสัญญาณเสียงทิศทางเดียว (one way delay) มีค่ามากกว่า 150 ms

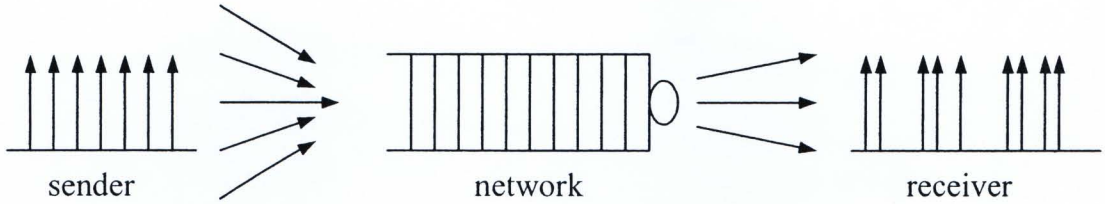
ค่าของดีเลย์ที่วัดจากต้นทางกับปลายทางที่เกิดขึ้นจริงจะประกอบด้วย 3 อย่างด้วยกัน คือ

1) Propagation delay : เป็นเวลาที่ข้อมูลเดินทางผ่านเครือข่ายจากต้นทางไปยังปลายทาง เช่น ดีเลย์ที่เกิดจากต้นทางอยู่กรุงเทพฯ ปลายทางอยู่มาเลเซีย ย่อมมีดีเลย์น้อยกว่า ที่ต้นทางอยู่กรุงเทพฯ แต่ปลายทางอยู่อเมริกา มีหน่วยเป็นมิลลิวินาที (ms)

2) Transport delay : เป็นดีเลย์ที่เกิดจากอัตราการส่งข้อมูล ค่านี้จะมีความสัมพันธ์กับแบนด์วิดธ์ คือ ถ้าค่าแบนด์วิดธ์กว้าง ดีเลย์ก็จะน้อย มีหน่วยเป็นมิลลิวินาที (ms)

3) Packetization delay เป็นเวลาที่ Codec แปลงสัญญาณอนาล็อคไปสู่การสร้างเฟรมและแปลงกลับเมื่อถึงปลายทาง เช่น Codec G.729 จะใช้เวลาในการแปลงเป็นแพ็กเก็ตที่สูงกว่า Codec G.711 เพราะว่าต้องใช้เวลาในการบีบอัดข้อมูลที่มากกว่า

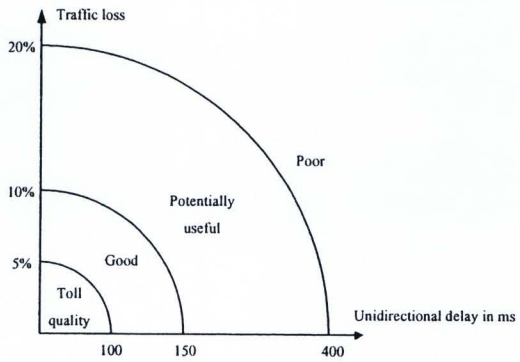
2.4.2 ความผันแปรเฉลี่ยของระยะเวลาดีเลย์ที่เกิดขึ้นกับแต่ละแพ็ค (Jitter) ในการส่งข้อมูลเสียงผ่านเครือข่ายอินเตอร์เน็ต ข้อมูลเสียงแต่ละแพ็กเก็ตจะใช้เวลาในการเดินทางจากต้นทางไปยังปลายทางไม่เท่ากัน ซึ่งทำให้ข้อมูลที่ปลายทางได้รับนั้นมี Jitter เกิดขึ้น และถ้านำข้อมูลเสียงมาถอดรหัสทันทีจะทำให้เกิดความไม่ต่อเนื่องของเสียงได้ การลด Jitter สามารถทำได้โดยการนำข้อมูลเสียงที่ได้รับจากต้นทางมาเก็บไว้ในบัฟเฟอร์ก่อนช่วงเวลาหนึ่งแล้วค่อยนำข้อมูลเสียงนั้นไปถอดรหัสดังแสดงในรูป 2.7 โดยถ้าบัฟเฟอร์ข้อมูลเสียงมากก็จะลด Jitter ได้มาก แต่ข้อมูลเสียงจะเกิดการประวิงทางเวลามากเช่นกัน ดังนั้นการเลือกขนาดของบัฟเฟอร์จึงเป็นสิ่งสำคัญต่อคุณภาพเสียงที่ผู้รับจะได้ยิน



รูปที่ 2.7 รูปตัวอย่างการเกิด Jitter delay

ที่มา: เกษมศักดิ์, 2547.

2.4.3 การสูญหายของแพ็กเก็ต (Packet Loss) เครือข่ายไอพีไม่สามารถรับประกันได้ว่าแพ็กเก็ตที่ส่งไปจะครบและถูกต้องตามลำดับแพ็กเก็ตส่วนใหญ่จะสูญหายไปในช่วงที่มีการใช้งานมาก (peak load) ซึ่งเกิดจากความจุไม่เพียงพอและการถ่ายทอดเสียงต้องการความต่อเนื่องของเวลา วิธีการส่งข้อมูลซ้ำใหม่บนพื้นฐานของ TCP เดิมจึงไม่เหมาะสมกับสัญญาณเสียงต้องใช้วิธีแทรกคำพูดโดยย้อนเล่นแพ็กเก็ตก่อนหน้านี้และส่งข่าวเดิมซ้ำกันหลายๆ ครั้ง เพื่อชดเชยแพ็กเก็ตที่สูญหาย โดยทั่วไประบบสามารถทดแทนแพ็กเก็ตที่สูญหายได้ไม่เกิน 10% เพื่อให้เครื่องปลายทางสามารถถอดสัญญาณได้อย่างถูกต้องหากมีความล่าช้าหรือแพ็กเก็ตสูญหายมากจะทำให้การสนทนาไม่ต่อเนื่องอันจะทำให้เกิดเสียงขาดๆ หายๆ ไป ทำให้ผู้ใช้รู้สึกได้ จึงต้องมีการกำหนดคุณภาพการให้บริการของการส่งสัญญาณเสียงดังรูปที่ 2.8 (อรศรี ศรีระษา, 2545) แสดงให้เห็นถึงคุณภาพของสัญญาณเสียงจัดอยู่ในระดับดีมาก ถ้ามีปริมาณทราฟฟิกสูญหายไม่เกิน 5% และความล้าช้าของสัญญาณไม่เกิน 100 มิลลิวินาที และถ้าปริมาณทราฟฟิกสูญหายไม่เกิน 10% ความล้าช้าของสัญญาณไม่เกิน 150 มิลลิวินาทีก็สามารถรองรับการสนทนาได้ดี เป็นต้น



รูปที่ 2.8 ระดับคุณภาพของสัญญาณเสียงเปรียบเทียบในเชิงปริมาณ ทราฟฟิกที่สูญหายกับความล้าช้าของสัญญาณในการส่งผ่านโครงข่ายไอพี

การรักษาระดับของคุณภาพเสียงให้คงที่กระทำได้โดยใช้เทคนิคการบีบอัดสัญญาณการห้ามระงับเสียง Voice Activity Detection (VAD) หรือ Silence Suppression ซึ่งเป็นการตรวจหาช่องว่างในเสียงพูดและระงับการส่งสัญญาณในจังหวะเงียบนี้ และสามารถใช้ความสะดวกในการใช้บริการบนชั้นทรานสปอร์ตเลเยอร์ (QoS-enabled transport network)

2.4.4 การเลือก CODEC จะมีผลต่อคุณภาพของเสียงเช่นกันเพราะว่า CODEC จะใช้แปลงสัญญาณเสียงที่เป็นอนาล็อคไปเป็นแบบดิจิตอล โดย CODEC G.711 จะให้คุณภาพเสียงที่ดีที่สุดเพราะว่าไม่มีการบีบอัด แต่มีดีเลย์เล็กน้อยและมีความไวกับข้อมูลที่จะสูญหายน้อยกว่า CODEC อื่น ส่วน CODEC G.729 จะกินแบนด์วิดท์น้อยกว่าเพราะมีการบีบอัดข้อมูลซึ่งนั้นก็ถือเป็นสิ่งที่ดีเพราะว่าจะสามารถใช้งานพร้อมๆ กันได้หลายๆ concurrent แต่การบีบอัดทำให้ความชัดเจนของเสียงลดลง ดีเลย์เพิ่มขึ้นและทำให้เสียงอาจขาดหาย

2.5 วิธีการวัดคุณภาพเสียงจากเครือข่ายไอพี (สมาคมเวชสารสนเทศไทย, 2551, 18 สิงหาคม)

คุณภาพเสียงในที่นี้ก็คือคุณภาพของข้อมูลเสียงบนเครือข่ายไอพี ดังนั้นคุณภาพเสียงที่ดีก็คือเสียงที่ออกมาจะต้องใกล้เคียง หรือเหมือนกับต้นฉบับให้มากที่สุด ซึ่งการวัดคุณภาพเสียงผ่านเครือข่ายมีอยู่ 2 แบบด้วยกันคือ

2.5.1 แบบ Active Testing เป็นวิธีการแบบที่ใช้โดยการใช้เปรียบเทียบกับต้นฉบับ โดยการนำเอาออดิโอไฟล์ต้นฉบับมาแบ่งเป็นบล็อคเล็กๆ ที่เหลื่อมกันอยู่จากนั้นก็ทำการคำนวณค่า Fourier Transform Coefficient ของแต่ละบล็อคเก็บไว้ และเมื่อเสียงนั้นผ่านเครือข่ายแล้วก็ทำวิธีเดียวกันเพื่อให้ได้ชุดของค่า Fourier Transform Coefficient มาเพื่อเปรียบเทียบและทำการให้คะแนน ถึงแม้ว่าคะแนนที่ได้จะไม่ตรงกับคะแนน MOS เสียทีเดียวแต่ก็มีความน่าเชื่อถือโดยจะมีค่าของ Correlation สูงถึง 0.95 ทีเดียว (ค่าสูงสุดเท่ากับ 1) จึงนับว่าเป็นวิธีการที่น่าเชื่อถือมากทีเดียว อย่างไรก็ตามวิธีนี้ยังมีข้อเสียคือ เนื่องจากการเปรียบเทียบกับไฟล์ออดิโออ้างอิง จึงจำเป็นที่จะต้องมีการสร้างไฟล์เสียงอ้างอิงนั้นแล้วส่งเข้าไปในเครือข่าย ซึ่งจะเป็นการเพิ่มโหลดหรือทราฟฟิกให้กับเครือข่ายจะต้องมีกาวัดที่ต้นทางและปลายทาง ซึ่งส่วนใหญ่จะอยู่คนละที จึงทำให้ลำบากต่อการติดตั้งอุปกรณ์วัดและทำการวัดจริงๆ และยากที่จะทำการวัดนอกเครือข่ายของตนเองได้ จึงทำให้ขอบเขตของการวัดค่อนข้างจำกัด จึงทำให้ไม่เป็นที่นิยมมากนัก ยกเว้นกรณีที่ทดสอบในห้องทดลอง

2.5.2 แบบ Passive Monitoring วิธีการนี้จะตรงข้ามกับแบบแรกคือจะไม่มีการเปรียบเทียบแต่อย่างใด โดยจะเริ่มจากการนำเอาเสียงที่ผ่านเครือข่ายมาแล้ว ผ่านกระบวนการที่เรียกว่า Pre-Processing ซึ่งได้แก่การทำ Filtering ,ปรับระดับเสียงและแยกเสียง Voice กับ Non-Voice ออกจากกัน (Voice Activity Detection) จากนั้นก็นำมาประมวลผลเพื่อแยกเอาค่าพารามิเตอร์ของเสียงและ

ค่าความเพี้ยนต่างๆ ออกมาเช่น Unnatural Speech เป็นเสียงประหลาดที่ไม่ใช่เสียงที่พบเห็นโดยทั่วไปเช่น เสียงปี๊บ, Noise เป็นเสียงรบกวนต่างๆรวมทั้ง Background Noise, Interruptions หรือ Mute ซึ่งเป็นเสียงที่หายไปหรือเสียงเงียบไป เป็นต้น ซึ่งเมื่อได้ค่าพารามิเตอร์ของเสียงและค่าความเพี้ยนต่างๆ แล้ว ก็จะนำมาสร้างเป็นค่า MOS ที่มีค่าตั้งแต่ 1 ถึง 5 ซึ่งจะมีค่า Correlation เท่ากับ 0.89 – 0.9 ซึ่งวิธีนี้อาจจะไม่ดีเท่ากับวิธีก่อนหน้านี้ แต่ก็นับว่าใช้ได้ทีเดียวเพราะเหมาะสมกับการวัดจากเครือข่ายที่ใช้งานอยู่จริงมากกว่า ซึ่ง MOS เป็นวิธีที่ยอมรับกันอย่างแพร่หลายซึ่งมีต้นกำเนิดจากเครือข่ายโทรศัพท์ ตามวิธีการอย่างเป็นระบบที่กำหนดโดย ITU ซึ่งจะเป็นการประเมินโดยการพิจารณาเชิงคุณภาพ (Subjective) ด้วยการให้คะแนนจากผู้ทดสอบซึ่งแน่นอนว่าต้องเอาคนที่มีทักษะในการฟังพอสมควร และความน่าเชื่อถือจะมากหรือน้อยขึ้นอยู่กับจำนวนคนที่นำมาทดสอบ และได้มีการนำเอาวิธีการในการวางแผนเครือข่าย หรือ E-Model มาปรับแต่งในการวัดคุณภาพเสียงและมีต้นทุนที่ต่ำกว่าโดยจะเกี่ยวข้องกับ Transmission Rating Factor (R- Factor) คือระดับคุณภาพการส่งสัญญาณเสียงโดยรวมซึ่งพิจารณาจากแวดล้อมต่างๆ จากผู้พูดต้นทางไปยังผู้ฟังปลายทาง (Mouth to Ear) ซึ่งกำหนดโดยองค์กรสหภาพโทรคมนาคมระหว่างประเทศ (ITU) โดยค่า R-Factor จะอยู่ระหว่าง 0 ถึง 100 ซึ่ง 100 เป็นค่าดีเยี่ยมและ 0 เป็นค่าที่แย่สุด สูตรในการคำนวณ R-Factor (Chris Bajorek, 2003) มีดังนี้

$$R\ \text{Factor} = R_o - I_s - I_d - I_e + A \qquad (1)$$

โดย R_o : อัตราส่วนของสัญญาณต่อเสียงรบกวน (Signal to noise ratio)

I_s : การสูญเสียโดยรวมทั้งหมด (A combination of all impairments simultaneously)

I_d : การสูญเสียที่เกิดจากดีเลย์ (Impairment caused by delay)

I_e : การสูญเสียที่เกิดจากอุปกรณ์ (The packet-loss dependent Effective Equipment Impairment factor)

A : ปัจจัยอื่น (Advantage factor) ซึ่งกำหนดไว้ดังนี้

ใช้งานแบบสาย Conventional (wirebound) A = 0

ใช้งานเซลลูล่าภายในอาคาร(Mobility by cellular networks in a building) A = 5

ใช้งานเซลลูล่าภายในรถยนต์ (Mobility in a geographic area or moving in a vehicle) A = 10

ใช้งานในตำแหน่งที่ยากต่อการเข้าถึง(Access to hard-to-reach locations)

A = 20

ค่า MOS Score และ R- Factor สามารถสรุปได้ดังนี้

$$MOS = 1 + 0.035R + 7*10^{-6} R(R - 60)(100 - R) \quad (2)$$

แต่ในความเป็นจริงแล้วในสมการที่ (1) จะไม่สามารถวัดค่าเหล่านั้นจากเครือข่ายจริง นั้นคือค่าอัตราส่วนของสัญญาณต่อเสียงรบกวน (R_o) การสูญเสียโดยรวมทั้งหมด (I_s) การสูญเสียที่เกิดจากดีเลย์ (I_d) การสูญเสียที่เกิดจากอุปกรณ์ (I_e) และการสูญเสียจากปัจจัยอื่นๆ (A) ผู้วิจัยจึงได้ศึกษาหาวิธีการคำนวณใหม่ เพราะจากการทำการวัดจากเครือข่ายจริง จะสามารถวัดได้เฉพาะค่า Delay, Loss และ Jitter จากเครือข่ายเท่านั้น โดยการศึกษาค้นคว้าซึ่งใช้ในเครื่องมือวัดที่มีชื่อว่า PingPlotter Pro ซึ่งผู้ใช้สามารถเปลี่ยนแปลค่าคงที่ตามสมการที่ (4), (5) ได้ตามความเหมาะสม ซึ่งวิธีการคำนวณจะใช้สมการดังนี้

$$\text{Effective Latency} = (\text{Average Latency} + \text{Jitter} * 2 + 10) \quad (3)$$

จากสมการที่ (3) ถ้าได้ค่าของ Effective Latency มีค่าน้อยกว่า 160 จะได้

$$R_I = 93.2 - (\text{Effective Latency} / 40) \quad (4)$$

แต่ถ้าค่าที่ได้จากสมการที่ (3) มากกว่า 160 ก็จะได้ค่า R_I ว่า

$$R_I = 93.2 - (\text{Effective Latency} - 120) / 10 \quad (5)$$

แล้วนำค่า R_I ซึ่งเกิดจากผลกระทบของดีเลย์กับจิสเตอร์ นำมาหาค่า R_o ซึ่งเป็นผลกระทบทั้งหมดที่เกิดขึ้นรวมทั้งแพ็กเก็ตที่สูญหายด้วย

$$R_o = R_I - (\text{Packet Loss} * 2.5) \quad (6)$$

จากสมการที่ (6) นั้นก็นำมาหาค่า MOS ได้โดยใช้สมการ ดังนี้

$$MOS = 1 + (0.035) * R_o + (.000007) * R_o * (R_o - 60) * (100 - R_o) \quad (7)$$

โดยค่า MOS Score จะอยู่ระหว่าง 1 ถึง 5 โดย 1 เป็นค่าที่มีคุณภาพเสียงแย่สุดแต่ 5 เป็นค่าที่มีคุณภาพเสียงดีสุด แต่ในความเป็นจริงค่าของ R- Factor สูงสุดจะไม่เกิน 93.2 และค่าของ MOS Score สูงสุดจะไม่เกิน 4.41 โดยรูปที่ 2.9 (กิติ ภักดีวัฒนะกุล และ จำลอง ครูอุตสาหะ, 2542) จะแสดงให้เห็นความสัมพันธ์ระหว่าง R- Factor กับ MOS Score

รูปที่ 2.9 แสดงให้เห็นความสัมพันธ์ระหว่าง R- Factor กับ MOS Score

2.6 ประเภทการใช้ VoIP ตาม OSI Layer

ในเครือข่าย VoIP ใช้ User Datagram Protocol (UDP) ร่วมกับ Real Time Protocol (RTP) ในการขนส่งข้อมูลจากต้นทางถึงปลายทางโดยชั้นที่ดูแลตาม OSI Layer ในชั้นที่ 4 คือ ชั้นทรานสปอร์ตเลเยอร์ โดยจะแสดงในตารางที่ 2.3 (อรศรี ศรีระษา, 2545)

ตารางที่ 2.3 ชั้นของ OSI Layer กับโปรโตคอลที่เกี่ยวข้องกับ VoIP

OSI Layer	โปรโตคอล IP	VoIP Stack
Layer 7 Application	Application	Call Center
Layer 6 Presentation		G.723.1, G.711, G.729
Layer 5 Session		H.323, SIP, MGCP
Layer 4 Transport	Transport	RTP/RTCP, UDP

ตารางที่ 2.3 ชั้นของ OSI Layer กับโปรโตคอลที่เกี่ยวข้องกับ VoIP (ต่อ)

OSI Layer	โปรโตคอล IP	VoIP Stack
Layer 3 Network	Network	IP
Layer 2 Data Link	Data Link	Ethernet, FR, ATM, PPP
Layer 1 Physical	Physical	Copper, Fiber

โดย UDP มีขนาดของแพ็คเก็ตเล็กและไม่มีกลไกลที่ช่วยควบคุมการส่งข้อมูลทำให้สามารถส่งข้อมูลได้เร็วเหมาะสำหรับทราฟฟิกประเภทสัญญาณเสียงที่ยอมให้เกิดความล่าช้าของข้อมูลการส่งได้น้อย แต่ยอมให้เกิดการสูญหายของข้อมูลได้ระดับหนึ่ง โดย UDP จะมีเฮดเดอร์ขนาด 8 ไบท์

RTP ถูกออกแบบมาเพื่อใช้ในการส่งข้อมูลทราฟฟิกประเภทเรียวไทม์ที่ต้องการส่งข้อมูลในช่วงเวลาที่สั้นมากๆ โดยจะทำหน้าที่รวมข้อมูลที่เข้ามาจากหลายๆ แหล่งให้ออกเป็นข้อมูลที่ไหลรวมกันเป็นข้อมูลเดียวกันเหมาะสำหรับใช้กับการส่งข้อมูลประเภทเสียง เนื่องจากช่วยให้คุณภาพของสัญญาณเสียงดียิ่งขึ้น โดย RTP มีเฮดเดอร์ขนาด 12 ไบท์

IP เป็นโปรโตคอลในชั้นที่ 3 สำหรับทำหน้าที่ในการหาเส้นทางที่ใช้ในการส่งข้อมูลมีขนาดเฮดเดอร์ 20 ไบท์ โดยรูปแบบของแพ็คเก็ตจะแสดงในรูปที่ 2.10

IP Hdr (20 Bytes)	UDP Hdr (8 Bytes)	RTP Hdr (12 Bytes)	Voice sample

รูปที่ 2.10 รูปแบบของแพ็กเก็ต VoIP

โดยสัญญาณเสียงเมื่อแปลงให้อยู่ในรูปของสัญญาณข้อมูลซึ่งอยู่ในรูปของแพ็คเก็ตไอพี ขนาดของแพ็คเก็ตที่แตกต่างกันจะทำให้เกิดความล่าช้าในการส่งข้อมูลที่แตกต่าง ฉะนั้นการเลือกมาตราฐานในการเข้ารหัสก็เป็นสิ่งสำคัญเพื่อจะได้กำหนดขนาดของแบนด์วิดท์ที่ใช้ได้

การเชื่อมต่อแบบ Ethernet เป็นเทคโนโลยีสำหรับเครือข่ายแบบแลน (LAN) ที่ได้รับความนิยมสูงสุดในปัจจุบัน คิดค้นโดยบริษัท Xerox ตามมาตรฐาน IEEE 802.3 การเชื่อมเครือข่ายแบบ Ethernet สามารถใช้สายเชื่อมได้ทั้งแบบ Co-Axial และ UTP (Unshielded Twisted Pair) โดยสายสัญญาณที่ได้รับความนิยม คือ UTP 10Base-T ซึ่งสามารถส่งข้อมูลได้เร็วถึง 10 Mbps โดยถ้า

ใช้ CODEC G.711 แบนด์วิดท์ 64 Kbps ก็จะมีรูปแบบของแพ็กเก็ตดังรูป 2.11 ถ้าจะคำนวณแบนด์วิทด์ทั้งหมดที่ใช้ใน 1 แพ็กเก็ตก็จะได้ว่า

220 bytes(headers+payload) / 160 bytes(payload only) * 64,000 bit per second = 88,000 bps

Ethernet Hdr (14 Bytes)	IP Hdr (20 Bytes)	UDP Hdr (8 Bytes)	RTP Hdr (12 Bytes)	Voice Data (160 Bytes)	FEC/Filler (6 Bytes)

รูปที่ 2.11 รูปแบบของแพ็กเก็ต VoIP ที่ใช้ CODEC G.711

แต่ถ้าเลือกการเข้ารหัสแบบ G.729 ซึ่งมีแบนด์วิดท์ 8 Kbps ก็จะมีรูปแบบของแพ็กเก็ตดังรูป 2.12 ถ้าจะคำนวณแบนด์วิทด์ทั้งหมดที่ใช้ใน 1 แพ็กเก็ตก็จะได้ว่า

80 bytes(headers+payload) / 20 bytes(payload only) * 8,000 bit per second = 32,000 bps

Ethernet Hdr (14 Bytes)	IP Hdr (20 Bytes)	UDP Hdr (8 Bytes)	RTP Hdr (12 Bytes)	Voice Data (20 Bytes)	FEC/Filler (6 Bytes)

รูปที่ 2.12 รูปแบบของแพ็กเก็ต VoIP ที่ใช้ CODEC G.729

และถ้าเลือกการเข้ารหัสแบบ GSM ซึ่งมีแบนด์วิดท์ 13.2 Kbps ก็จะมีรูปแบบของแพ็กเก็ตดังรูป 2.13 ถ้าจะคำนวณแบนด์วิทด์ทั้งหมดที่ใช้ใน 1 แพ็กเก็ตก็จะได้ว่า

93 bytes(headers+payload) / 33 bytes(payload only) * 13,200 bit per second = 37,200 bps

Ethernet Hdr (14 Bytes)	IP Hdr (20 Bytes)	UDP Hdr (8 Bytes)	RTP Hdr (12 Bytes)	Voice Data (33 Bytes)	FEC/Filler (6 Bytes)

รูปที่ 2.13 รูปแบบของแพ็กเก็ต VoIP ที่ใช้ CODEC GSM

จากข้อมูลทั้งหมดพอจะสรุปรวมเป็นตารางที่ 2.4 เพื่อให้เปรียบเทียบข้อมูลของแต่ละวิธีในการเข้ารหัส ซึ่งจากข้อมูลแบนด์วิดธ์ที่ต้องการในการสื่อสารด้วยเสียงนั้นจะเห็นได้ว่าแบนด์วิดธ์ที่ต้องการบนเน็ตเวิร์กอย่างเครือข่ายแลน นับว่าค่อนข้างน้อยถ้าเทียบกับแอพพลิเคชันที่มีอยู่ การที่โทรศัพท์หนึ่งสายจะใช้แบนด์วิดธ์ 64 กิโลบิตต่อวินาที หรือคิดเป็น 0.0625 เปอร์เซ็นต์ ของแบนด์วิดธ์ที่เครือข่ายแลนแบบ Full Duplex 100 เมกะบิตต่อวินาทีมีเท่านั้น เมื่อคำนวณอย่างละเอียดแล้ว บนเครือข่ายอีเทอร์เน็ตความเร็ว 100 เมกกะบิตต่อวินาทีนั้น โทรศัพท์หนึ่งสายจะใช้แบนด์วิดธ์ประมาณ 88 กิโลบิตต่อวินาที (64 กิโลบิตต่อวินาที+ไอพีเฮดเดอร์+อีเทอร์เน็ตเฮดเดอร์) ถ้าเป็นการสื่อสารทางเดียวจะรองรับโทรศัพท์ได้ทั้งหมด 1,160 สายพร้อมๆ กันบนเครือข่ายแบบ Full Duplex แต่ถ้าใช้แบ็กโบนในระดับเป็นกิกะบิตอีเทอร์เน็ตด้วยแล้ว ก็จะรองรับโทรศัพท์ได้ถึง 11,600 สายเลยทีเดียว

ตารางที่ 2.4 แสดงแบนด์วิดท์สำหรับตัวเข้า/ถอดรหัสแต่ละชนิดบน Ethernet

ชนิดของการเข้ารหัส	แบนด์วิดท์ของเสียง (กิโลบิตต่อวินาที)	MOS	ขนาดแพ็กเก็ต (ไบต์)	เฮดเดอร์ L3-4 IP/UDP/RTP (ไบต์)	เฮดเดอร์ L2 (ไบต์)	แบนด์วิดท์ทั้งหมด (กิโลบิตต่อวินาที)
G.711	64	4.10	160	40	14	88
G.729	8	3.91	20	40	14	32
GSM	13.2	3.57	33	40	14	37.2

อย่างไรก็ตามถ้าแบนด์วิดธ์เป็นปัจจัยเพียงอย่างเดียว เทคโนโลยีของระบบโทรศัพท์ผ่านไอพี คงจะได้รับความนิยมมาเป็นเวลานานแล้ว แต่ปัญหาที่แท้จริงนั้นอยู่เวลาในการตอบสนอง (Respons Time) เพราะในระบบเครือข่ายจะต้องให้บริการแอพพลิเคชันทางธุรกิจ ที่ต้องใช้แบนด์วิดธ์จำนวนมาก ซึ่งก่อให้เกิดปัญหาความล่าช้า (Delay) ในการส่งข้อมูล โดยเฉพาะการสื่อสารด้วยเสียงที่ข้อมูลต้องได้รับการถ่ายโอนโดยใช้เวลาให้น้อยที่สุดได้อย่างเพียงพอ ดังนั้นเทคโนโลยีที่ถูกนำมาใช้เพื่อแก้ปัญหานี้ก็คือ QoS ที่มี Bandwidth Manager หรือ Complex Queuieng Scheme คอยทำหน้าที่จัดลำดับความสำคัญให้กับข้อมูลบนเครือข่ายแลนและแวน

2.7 วิธีการปรับปรุงคุณภาพเสียงบนเครือข่ายไอพี (สมิทธิชัยและรังสิมา, 2550), (เอกพลชัยและนาโอฬาร, 2548)

ระบบโทรศัพท์ผ่านไอพี (IP Telephone) เป็นแอพพลิเคชั่นที่ใช้กันอย่างแพร่หลายในแผนกไอทีขององค์การต่างๆ โดยผู้ใช้ยังมีความคาดหวังในระบบโทรศัพท์ผ่านไอพีไว้สูง ด้วย หนึ่งในสิ่งที่คนส่วนใหญ่ต้องการก็คืออย่างน้อยก็คือระบบโทรศัพท์ผ่านไอพี จะมีความเสถียรเทียบเท่ากับระบบ PBX เดิมที่เคยใช้มาก่อน แต่ระบบโทรศัพท์ผ่านไอพีนั้น ต้องพึ่งพาโครงสร้าง พื้นฐานทางการสื่อสารบนด้านข้อมูล ดังนั้น ความเสถียรของระบบการสื่อสารข้อมูลจึงมักเป็นจุดอ่อนที่สุดในระบบโทรศัพท์ผ่านไอพีซึ่งต่างจาก PBX ตรงที่โทรศัพท์ผ่านไอพี มีจุดเชื่อมต่อจำนวนมาก อย่างเช่น เซิร์ฟเวอร์ โทรศัพท์ เกตเวย์ เราเตอร์ สวิตซ์ และอื่นๆ อีกมากมาย หากเกิดปัญหาที่จุดใด จุดหนึ่ง ก็สามารถก่อให้เกิดปัญหาติดต่อกันขึ้นทั้งระบบเลยทีเดียว ความเสถียรนั้นจำเป็นต้องเริ่มต้นกันตั้งแต่การออกแบบ ซึ่งหมายความถึงมีแนวทางและระเบียบปฏิบัติที่เหมาะสม ไม่ใช่แค่เพียงมีฮาร์ดแวร์ จำนวนมากเท่านั้น ฮาร์ดแวร์ที่มีระบบสำรองทุกตัวในโลกนี้จะไม่สามารถแก้ไขปัญหาที่เกิดจากการออกแบบ โดยการส่งข้อมูลเสียงไปบนเครือข่ายไอพีนั้นจำเป็นจะต้องส่งข้อมูลแบบเวลาจริง แต่สำหรับ TCP/IP นั้น ไม่ได้ถูกออกแบบมาให้ทำเช่นนั้นได้ เราทำได้เพียงกำหนดนโยบายเพื่อให้ แพ็กเก็ต ของเสียง ผ่านเราเตอร์แต่ละตัวไปให้เร็วที่สุด โดยจะขึ้นอยู่กับโครงสร้างของเครือข่ายซึ่งสามารถทำได้ดังนี้

2.7.1 การแบ่งชั้นตามความสำคัญของข้อมูล (Traffic classification)

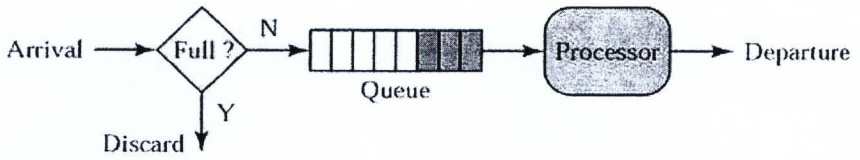
1) การทำ Virtual LAN (VLAN) ซึ่งจะเป็นการแยกซับเน็ตของเสียงและข้อมูลออกจากกันเพราะเมื่อเราแยกอุปกรณ์เสียง (โทรศัพท์,เกตเวย์) ออกจากอุปกรณ์ข้อมูล (เวิร์กสเตชัน, เซิร์ฟเวอร์) เราสามารถแยกการติดต่อสื่อสารของเสียงและข้อมูลออก จากกันได้ ซึ่งจะช่วยเพิ่มความเสถียรและความปลอดภัยได้อีกมาก โดยการจัดวางอุปกรณ์เสียงและอุปกรณ์ข้อมูลไว้บน VLAN คนละวง แล้วกำหนดไอพีแอดเดรสโดยแยกแอดเดรสเป็นคนละวงกัน นอกจากนั้นการแยก VLAN ยังทำให้สามารถกำหนดระดับการให้บริการ (Qos) และนโยบายความปลอดภัยให้แก่เสียงกับข้อมูลแตกต่างกันได้ เพราะ ไม่มีความจำเป็นที่โทรศัพท์ต้องติดต่อสื่อสารไปยังพีซี หรือในทางตรงกันข้าม เมื่อได้จัดการแยกการสื่อสารซับเน็ตของเสียงและข้อมูลจากกันแล้ว จะส่งผลให้ช่องโหว่ของระบบความปลอดภัย การกำหนดค่าผิดพลาด และข้อผิดพลาดในการปฏิบัติงานหมดไป แต่มีข้อยกเว้นคือ สะเตชันของฝ่ายบริหารยังคงสามารถเข้ามาดูระบบได้ โดยใช้หลักการเดียวกันคือจัดวางเวิร์กสเตชันเหล่านั้นไว้ใน VLAN แยกวงกัน แล้วให้ VLAN วงนั้นเข้าถึงได้เฉพาะซับเน็ตของเสียงเท่านั้น โดยการกำหนดรายการควบคุมการเข้าถึง ACL(Access Control List) เพื่อแยกเสียงออกจากข้อมูล ซึ่งถ้าหากใช้ไอพีแอดเดรสจริง (Public IP) สำหรับข้อมูล ก็ควรให้ระบบ

โทรศัพท์ผ่านไอพี ใช้ไอพีแอดเดรสส่วนตัว (Private IP) เนื่องจากไม่มีความจำเป็นต้องให้โทรศัพท์ใช้ไอพีแอดเดรสที่สามารถสื่อสารเป็นไอพีไปโลกภายนอก เซิร์ฟเวอร์สำหรับระบบโทรศัพท์ควรจะใช้ VLAN แยกจากวงอื่นด้วย ซึ่งจะช่วยให้สามารถกลั่นกรองข้อมูลที่ส่งไปยัง (และกลับจาก) เซิร์ฟเวอร์ เนื่องจากเซิร์ฟเวอร์สำหรับระบบโทรศัพท์เป็นหัวใจของระบบโทรศัพท์ผ่านไอพี เราต้องปกป้องไว้ไม่ให้เกิดเหตุอันไม่พึงประสงค์ โดยการกำหนด ACL ให้อนุญาตเฉพาะทราฟฟิกที่จำเป็นจริงๆ เท่านั้น (ปกติก็คือทราฟฟิกที่เกี่ยวกับการตั้งค่าและบริหารจัดการโทรศัพท์) ที่สามารถเข้าถึงเซิร์ฟเวอร์ได้ ถ้าจะให้ดียิ่งขึ้นไปอีก (หากมีงบประมาณพอ) ควรติดตั้งไฟร์วอลล์กั้นไว้ระหว่างเซิร์ฟเวอร์สำหรับระบบโทรศัพท์กับส่วนอื่นๆ ในเครือข่ายเพื่อสกัดกั้นทราฟฟิกที่ไม่พึงประสงค์

2) การกำหนดคุณภาพการให้บริการ (Quality of Service : QoS) ซึ่งอยู่ใน header ของ IP Protocol จะถูกกำหนดให้เป็น high เพื่อระบุให้ แพ็กเก็ต นั้นเป็น แพ็กเก็ต ที่มีความสำคัญสูง ยิ่งให้ความสำคัญสูง แพ็กเก็ต ยิ่งใกล้ถูกส่งออกไปใกล้เวลาจริงยิ่งขึ้น เพราะ QoS เป็นสิ่งที่จำเป็นอย่างยิ่งสำหรับโทรศัพท์ผ่านไอพีเพราะต้องการคุณภาพของการให้บริการที่คงที่นั้นคือความสามารถในการควบคุมความเร็วและแบนวิดท์ของเครือข่ายการรับส่งข้อมูลระหว่างต้นทางและปลายทางได้ เนื่องจากเสียงการสนทนาถ้าไม่ต่อเนื่องจะฟังไม่รู้เรื่อง ดังนั้นข้อมูลเสียงจะต้องถึงปลายทางตามกำหนดเวลา และให้รูปแบบที่ต่อเนื่องตลอดเวลา เพราะว่าเครือข่ายนั้นเปลี่ยนแปลงอยู่ตลอดเวลา ลิงค์ที่มีการใช้งานน้อยอาจจะกลายเป็นลิงค์ที่มีการใช้งานมากไปก็ได้ หากไม่มีการทำ QoS ซึ่งมักจะก่อให้เกิดปัญหาคุณภาพเสียง (ขาดๆ หายๆ) เนื่องจาก การใช้งานเครือข่ายไม่เท่ากันในแต่ละช่วงของวัน หากมีการติดตั้ง QoS ให้คอยพิจารณาแอพพลิเคชันอื่นๆ ที่ไวต่อความล่าช้าของ สัญญาณด้วย อย่างเช่น วิดีโอคอนเฟอร์เรนซ์ หรือสตรีมมิ่งมีเดีย ที่สำคัญควรวางแผนไว้เผื่อการเติบโตในอนาคต

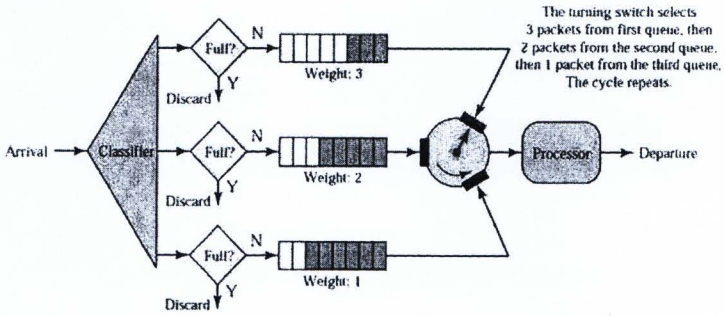
2.7.2 วิธีการจัดแถวคอยของ แพ็กเก็ต มีอยู่ด้วยกันหลายวิธีคือ

1) FIFO (First in First Out) ถือเป็นพื้นฐานที่สุดของเครือข่ายทุกชนิด โดยเป็นการเลือกแพ็คเกตที่มาถึงเราท์เตอร์เป็นตัวแรกให้ทำการส่งออกไปก่อน ซึ่ง FIFO นี้จะมีคิวเพียงคิวเดียวโดยไม่สนใจความสำคัญ (priority) และเนื่องจากพื้นที่ว่างของเราท์เตอร์แต่ละตัวมีขีด จำกัด เมื่อแพ็คเกตมาถึง แต่ไม่มีพื้นที่ว่างเพียงพอ เราท์เตอร์จะทำการละทิ้งแพ็คเกตนั้น โดยการละทิ้งนี้ จะไม่สนใจว่าแพ็คเกตมีความสำคัญมากน้อยเพียงใด จะมีลักษณะการทำงานตามรูปที่ 2.14 (กิติ ภักดีวัฒนะกุล และจำลอง ครูอุตสาหะ, 2542)



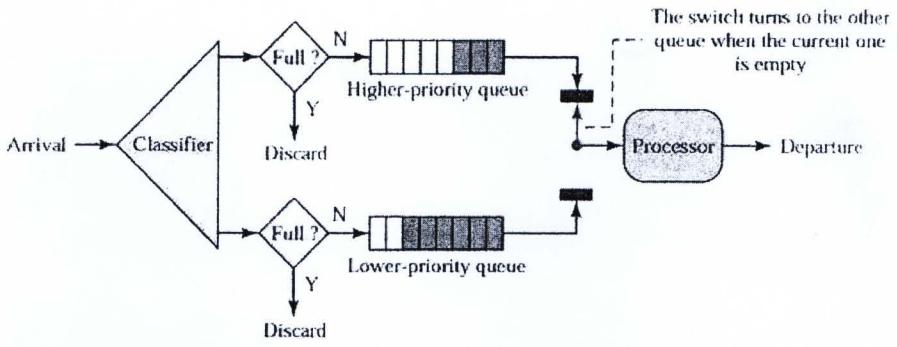
รูปที่ 2.14 การจัดแถวคอยแบบ First in First Out

2) WFQ (Weighted Fair Queuing) วิธีนี้จะกำหนดให้มีความเสมอภาคกันของแต่ละ คิว เพื่อไม่ให้มีเซอร์วิสตัวใดตัวหนึ่งใช้ช่องสัญญาณมากเกินไป แต่ในส่วนของการให้น้ำหนักในคิวแต่ละคิวจะแตกต่างกัน สำหรับคิวที่มีความสำคัญมาก จะได้รับจำนวนบิตที่ส่งไปมากกว่าคิวที่มีความสำคัญน้อยลงมา แต่ยังคงมีการวนรอบให้เซอร์วิสกับทุกๆ คิวเช่นเดิม โดยจะมีลักษณะการทำงานตามรูปที่ 2.15 (กิติ ภักดีวัฒนะกุล และจำลอง ครูอุตสาหะ, 2542)



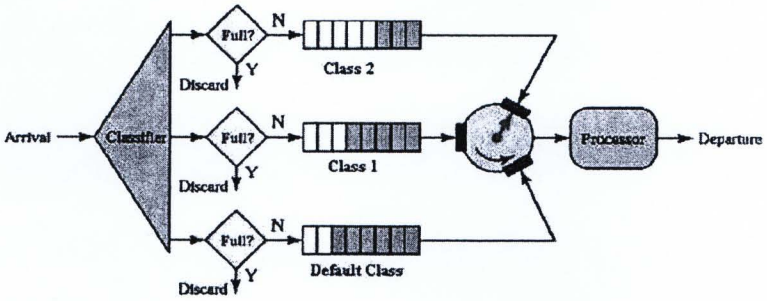
รูปที่ 2.15 การจัดแถวคอยแบบ Weighted Fair Queuing

3) PQ (Priority Queuing) เป็นรูปแบบหนึ่งที่ปรับเปลี่ยนมาจาก FIFO คือ เราเตอร์จะสามารถเลือกแพ็คเก็ตได้จากคิวหลายคิว และ จะมีการกำหนดความสำคัญให้กับแต่ละคิว ซึ่งจะแตกต่างกันไป เราเตอร์จะส่งแพ็คเก็ตโดยเลือกจากคิวที่มีความสำคัญมากที่สุดเป็นอันดับแรก จากนั้นจะเลือกคิวที่มีความสำคัญรองลงไปตามลำดับ และในแต่ละคิวจะมีการจัดการกับแพ็คเก็ตในคิวนั้นแบบ FIFO จะมีลักษณะการทำงานตามรูปที่ 2.16 (กิติ ภักดีวัฒนะกุล และจำลอง ครูอุตสาหะ, 2542)



รูปที่ 2.16 การจัดแถวคอยแบบ Priority Queuing

4) CQ (Custom Queuing) หรืออีกอย่างเรียกว่า Class-Based Queue(CBQ) เป็นวิธีการจัดคิวที่มีการกำหนดความสำคัญเหมือนกับแบบ PQ แต่จะเลือกให้บริการแพ็กเก็ตในคิวต่างๆ แบบหมุนวน (Round Robin) ตามข้อกำหนดที่ตั้งไว้เพื่อแก้ปัญหาการรอโดยไม่มีกำหนดของแพ็กเก็ตที่มีความสำคัญละดับต่ำ ซึ่งผู้ดูแลระบบสามารถกำหนดค่าสำหรับการให้บริการแพ็กเก็ตในแต่ละคิวเพื่อประกันขนาดของช่องทางต่ำสุดที่แต่ละคิวจะได้รับ ดังนั้นในแต่ละรอบของคิวต่างๆ จะได้รับบริการอย่างน้องสุดตามค่าที่ระบุไว้ โดยจะมีลักษณะการทำงานตามรูปที่ 2.17 (กิติ ภักดีวัฒนะกุล และจำลอง ครูอุตสาหะ, 2542)



รูปที่ 2.17 การจัดแถวคอยแบบ Custom Queuing

5) CB-WFQ (Class Based Weighted Fair Queuing) วิธีการนี้จะมีความคล้ายคลึงกับ WQF แต่ต่างกันที่ ได้มีการเพิ่มคุณสมบัติของ class เข้าไป โดยให้ค่าของแบนด์วิดท์เป็นคุณสมบัติของแต่ละ class

2.8 Visual Basic (ixiacom, 1998-2011)

ปัจจุบันระบบปฏิบัติการ (Operating System) ในลักษณะของ Windows ได้เข้ามาแทนที่ในระบบปฏิบัติการในลักษณะเดิม ซึ่งส่วนใหญ่ที่นิยมใช้กันอยู่คือ MS-DOS เพราะรูปแบบของจอภาพที่ใช้ติดต่อระหว่างคอมพิวเตอร์กับผู้ใช้อยู่ในรูปของคำสั่งซึ่งอยู่ในรูปแบบของตัวอักษรเป็นแบบป้อนทีละบรรทัดหรือเรียกว่า Command Line ซึ่งผู้ใช้จะต้องเรียนรู้และจดจำรูปแบบของคำสั่งให้ถูกต้องและแม่นยำจึงจะใช้งานโปรแกรมนั้นได้เป็นอย่างดี ซึ่งต่างจาก Visual Basic ที่รูปแบบของคำสั่งจะอยู่ในรูปแบบของ Graphic User Interface (GUI) ที่ใช้รูปภาพแทนคำสั่งต่างๆ แทน ซึ่งแต่เดิมการพัฒนาโปรแกรมจะอยู่บน MS-DOS จึงต้องเปลี่ยนแปลงรูปแบบและแนวความคิด และหันมาพัฒนาโปรแกรมบนวินโดว์แทน

ภาษา BASIC ถูกสร้างขึ้นมาในปี 1963 โดย Hohn Keneny และ Thomas Kurtz ที่วิทยาลัย Dartmount ในเบื้องต้นพวกเขามีจุดมุ่งหมายในการพัฒนาภาษา BASIC ขึ้นเพื่อใช้ในการสอนแนวเขียนโปรแกรม (Programming Concept) โดยเน้นให้รูปแบบของภาษานั้นง่ายต่อการเข้าใจและใช้งาน รวมทั้งทำงานในลักษณะ Interpreter ซึ่งแตกต่างจากภาษาคอมพิวเตอร์อื่นๆ ในยุคนั้นที่จะอาศัย Job Control Language (JCL) และขั้นตอนในการ Compile และ Link ผลก็คือภาษา BASIC ได้กลายมาเป็นที่นิยมกันอย่างกว้างขวาง โดยเฉพาะในหมู่ผู้ใช้คอมพิวเตอร์ส่วนบุคคล จึงอาจกล่าวได้ว่าภาษา BASIC ได้รับการพัฒนาควบคู่ไปกับการพัฒนาคอมพิวเตอร์ส่วนบุคคล ในปี 1970 Microsoft ได้เริ่มผลิตตัวแปรภาษา BASIC ใน ROM ซึ่งเรียกว่า ROM-Based BASIC ขึ้น เช่น ชิป Radio Sheek TRS-80 เป็นต้น ต่อมาได้พัฒนาเป็น GW-BASIC ซึ่งเป็น Interpreter ภาษาที่ใช้กับ MS-DOS และในปี 1982 Microsoft QuickBasic ไดรับการพัฒนาขึ้น โดยการเพิ่มความสามารถในการ Compile ให้เป็น Executed Program รวมทั้งทำให้ BASIC มีความเป็น "Structured Programming" มากขึ้นโดยการตัด Line Number ทิ้งไป เพื่อลบข้อกล่าวหาว่าเป็นภาษาคอมพิวเตอร์ที่มีโครงสร้างในลักษณะ Spaghetti Code (Logical Flow ของภาษาขาดโครงสร้าง) มาใช้รูปแบบของ Subprogram และ User Defined รวมทั้งการใช้ Structured Data Type และการพัฒนาการใช้งานด้านกราฟฟิกให้มีการใช้งานในระดับที่สูงขึ้น รวมทั้งมีการใช้เสียงประกอบได้เหมือนกับภาษาคอมพิวเตอร์อื่นๆ เช่น C หรือ Pascal

Visual Basic เป็นภาษาคอมพิวเตอร์ที่ได้รับความนิยมนำมาใช้พัฒนาโปรแกรมบน Windows เนื่องจากเป็นภาษาคอมพิวเตอร์ที่ใช้เทคโนโลยีในลักษณะ Visualize ซึ่งเพียงแต่เลือก Control ที่เหมาะสมแล้ววาดลงบน Form ก็สามารถสร้างจอภาพที่ใช้สำหรับติดต่อกับผู้ใช้รวมถึงการใช้เทคนิคการเขียนโปรแกรมแบบ Even-driven ซึ่งเป็นการเขียนโปรแกรมเพื่อกำหนดขั้นตอนการทำงานให้กับ Control ต่างๆ ที่สร้างตามเหตุการณ์ (Even) ต่างๆ ที่เกิดขึ้น เช่น การเลื่อนเมาท์

หรือการรับข้อมูลจากคีย์บอร์ด ฯลฯ เป็นต้น ประกอบกับภาษาที่ใช้เขียนโปรแกรมเป็นภาษา BASIC ซึ่งเป็นภาษาคอมพิวเตอร์ที่ผู้ใช้บนคอมพิวเตอร์ส่วนบุคคลส่วนใหญ่คุ้นเคยจึงส่งผลทำให้การพัฒนาโปรแกรมบน Windows ด้วย Visual Basic มีขั้นตอนน้อยกระทำได้ง่ายและสะดวกต่อการใช้งานจึงทำให้ผู้ใช้สามารถเรียนรู้ได้ภายในเวลา 2-3 ชั่วโมง ก็สามารถพัฒนาโปรแกรม Windows ขึ้นเป็นโปรแกรมแรก

Visual Basic นี้เป็นเครื่องมือที่ใช้ในการพัฒนาโปรแกรมขึ้นใช้งาน ที่ใช้ได้ตั้งแต่ผู้ใช้ระดับต้นเพื่อใช้สร้างโปรแกรมง่ายๆ บน Windows หรือโปรแกรมเมอร์ระดับกลาง ที่เรียกใช้ฟังก์ชั่นการทำงานต่างๆ ของ Visual Basic ได้อย่างมีประสิทธิภาพตลอดจนโปรแกรมเมอร์ในระดับอาชีพที่จะพัฒนาในโปรแกรมระดับสูงโดยการใช้ Object Linking and Embedding (OLE) และ Application Programming Programming Interface (API) ของ Windows มาประกอบในการเขียนโปรแกรม

2.9 โปรแกรม iperf (Mitchkutzko Jdugan, 2008)

โปรแกรม iperf เป็นโปรแกรมฟรี (freeware) ใช้สำหรับตรวจสอบระบบ network เป็นสิ่งที่สำคัญอย่างยิ่งในการใช้งานระบบ VoIP เนื่องจากระบบ VoIP เป็นการทำงานแบบ Realtime ซึ่งเป็นการทำงานที่มีความอ่อนไหวเป็นอย่างมากกับระบบ Network ซึ่งหากมีปัญหากับระบบ Network จะมีผลกระทบโดยตรงต่อคุณภาพเสียง ซึ่งในการใช้งานจริงผู้ใช้งานบางท่านอาจคิดว่าในปัจจุบันก็สามารถใช้งาน internet, mail ได้ดีอยู่แล้วทำไมต้องทำการตรวจสอบอีก จึงขออธิบายว่าในการใช้งานระบบเครือข่ายนั้น บาง Protocol เช่น Web (http) หรือ Mail (POP3) จะเป็นการทำงานโดยใช้ Protocol TCP เป็นหลัก โดยหากมีปัญหากับระบบ network เช่น delay หรือ package loss จะไม่ส่งผลกระทบกับ Applicationนั้นมาก เนื่องจาก Application นั้นๆ สามารถจะรอ หรือร้องขอ data ชุดนั้นๆใหม่ได้ ส่วน ระบบ VoIP ส่วนใหญ่ทำงานในลักษณะ Realtime และใช้ UDP เป็น Protocol หลักในการส่งเสียง ซึ่งจะไม่สามารถรอ data ได้นาน และ ถ้า data lost ก็จะไม่สามารถส่ง data นั้นได้ใหม่

Iperf เป็นโปรแกรมที่ใช้ในการสร้างแพ็กเก็ตและทดสอบเครือข่ายเบื้องต้น โดยจะทำการวัดขนาดของการส่งข้อมูล (Bandwidth) บนเครือข่ายระหว่างจุดที่สนใจ ประกอบด้วยส่วนที่เป็นเซิร์ฟเวอร์และไคล์แอนต์ ในตัวเดียวกัน โดยสามารถเลือกได้ว่าจะใช้แบบใด หลักการทำงานคือ ทำการรันที่เครื่องเซิร์ฟเวอร์ก่อนแล้วจากนั้นจึงทำการรันตัวไคล์แอนต์เพื่อทำการส่งแพ็กเก็ตไปที่เครื่องเซิร์ฟเวอร์ แล้วจะคำนวณค่าต่างๆส่งกลับไปยังตัวไคล์แอนต์ โดยโปรแกรมสามารถกำหนดโปรโตคอลของการส่งข้อมูลได้หลายชนิด ได้แก่ TCP Protocol, UDP Protocol เป็นต้น

คุณสมบัติของ Iperf

1) ใช้วัดความจุดของเครือข่าย (แบนด์วิดท์)

2) ไคล์แอ้นต์สามารถสร้างสตรีมแบบ UDP ส่งเข้าไปยังเครือข่ายเพื่อทำการตรวจวัด

3) สามารถวัดความขาดหายของแพ็กเก็ต

4) สามารถวัดค่าดีเลย์จิสเตอร์

2.10 คำสั่ง Ping (Microsoft, 2552, 1 กรกฎาคม), (วัชรพงษ์. 2547)

คำสั่ง Ping เป็นคำสั่งที่ใช้ในการตรวจสอบการเชื่อมต่อกับเครือข่ายระหว่างคอมพิวเตอร์แต่ละเครื่องที่อยู่ในเครือข่าย โดยคำสั่ง Ping จะส่งข้อมูลที่เป็นแพ็คเกจ 4 ชุดๆละ 32 Byte ไปยังคอมพิวเตอร์ปลายทางที่ต้องการตรวจสอบ หากมีการตอบรับกลับมาจากคอมพิวเตอร์เป้าหมายก็แสดงว่าการเชื่อมต่อเครือข่ายยังเป็นปกติ แต่หากไม่มีการตอบรับกลับมาก็แสดงว่าคอมพิวเตอร์ปลายทางหรือเครือข่ายอยู่ในช่วงหนาแน่น ดังนั้นจะเห็นว่าคำสั่ง Ping มีประโยชน์อย่างมากในการตรวจสอบสถานการเชื่อมต่อเครือข่ายเบื้องต้นได้เป็นอย่างดีโดยคำสั่ง ping จะใช้โปรโตคอล ที่มีชื่อว่า ICMP

2.10.1 รูปแบบการใช้คำสั่ง Ping

Ping [ไอพีแอดแดรส,ชื่อเครื่องคอมพิวเตอร์] เช่น ping 10.40.0.1 จะหมายถึงการตรวจสอบเครื่องที่มี IP Address 10.40.0.1 ว่ามีการทำงานติดต่อระบบเครือข่ายหรือไม่

2.10.2 การรายงานข้อผิดพลาดของคำสั่ง ping

เมื่อคำสั่ง ping ทำงานแล้วไม่ว่าระบบเครือข่ายจะสามารถเชื่อมต่อได้หรือไม่ คำสั่ง ping ก็รายงานผลออกมาโดยการแจ้งผลเมื่อไม่สามารถติดต่อกับเครือข่ายปลายทางได้ก็คือ

1) คำร้องหมดเวลา (Request time out)

2) หา Host ปลายทางไม่พบ (Host unknown)

ข้อผิดพลาด แต่ละอย่างที่โปรแกรม ping รายงานให้ทราบนั้นจะระบุรายละเอียดให้ด้วยว่าข้อผิดพลาดนั้นเกิดจากอะไร ซึ่งข้อผิดพลาดแต่ละอย่างมีความหมายดังนี้

คำร้องหมดเวลา นี้หมายความว่า เมื่อคำสั่ง Ping ส่งแพ็คแกจ ไปยังเครื่องปลายทางแล้วเครื่องปลายทางไม่ตอบกลับมาภายในเวลาที่กำหนด ปัญหาที่พบส่วนใหญ่จะมีดังนี้

1) เครื่องปลายทางไม่ได้เปิดอยู่

2) ระบบเครือข่ายมีปัญหาไม่สามารถติดต่อกับเครื่องปลายทางได้

3) ระบบเครือข่ายช้ามากไม่สามารถตอบรับการ ping ได้ภายในเวลากำหนดที่กำหนด

4) เครื่องปลายทางทำงานหนักมากไม่สามารถตอบรับข้อมูลการ ping ไม่ทัน

Host unknown ข้อผิดพลาด Host unknown นี้เกิดจากการที่เราสั่งให้ ping เป็นชื่อเครื่องคอมพิวเตอร์แล้ว เครื่องพิวเตอร์ไม่สามารถเปลี่ยนชื่อเครื่องคอมพิวเตอร์ให้เป็นไอพีแอดแดรสได้ ping ได้ เพราะว่าการ ping นั้นจะต้อง ping ไปยังไอพีแอดแดรส

2.10.3 Options ของคำสั่ง ping

-t คือ Ping ไปยัง Host ตามที่ระบุเรื่อยๆ จนกว่าจะสั่งยกเลิกโดยกดแป้น Ctrl-C และหากต้องการดูสถิติให้กดแป้น Ctrl-Break

-a คือ เปลี่ยนหมายเลข IP Address ของ Host เป็นชื่อแบบตัวอักษร

-n คือ count Ping แบบระบุจำนวน echo ที่จะส่ง

-l คือ size กำหนดขนาด buffer

-f คือ ตั้งค่าไม่ให้แยก flag ใน packet.

-i คือ TTL Ping แบบกำหนด Time To Live โดยกำหนดค่าตั้งแต่ 1-255

-v คือ TOS กำหนดประเภทของบริการ (Type of service)

-r คือ count Ping แบบให้มีการบันทึกเส้นทางและนับจำนวนครั้งในการ hops จนกว่าจะถึงปลายทาง

-s คือ count Ping แบบนับเวลาในการ hop แต่ละครั้ง

-j คือ host-list Loose source route along host-list.

-k คือ host-list Strict source route along host-list.

-w คือ timeout Ping แบบกำหนดเวลารอคอยการตอบรับ

2.11 การตรวจสอบความถูกต้อง และการวิธียอมรับของโปรแกรมที่พัฒนาขึ้น

การตรวจสอบและการยอมรับของโปรแกรมที่พัฒนาขึ้นมานี้ จะใช้หลักสถิติ วิธีการแบบ Hypothesis (สมมติฐาน) ในการตรวจสอบความถูกต้องหรือไม่ ซึ่ง Hypothesis คือ คำตอบที่คาดการณ์ความสัมพันธ์ในเชิงเหตุผลระหว่างตัวแปรต่างๆ ที่มีผลต่อปัญหาที่ศึกษา เป็นการคาดคะแนนคำตอบไว้ล่วงหน้า เพื่อทดสอบด้วยข้อเท็จจริง (empirical data) ว่ามีความถูกต้องหรือไม่ สมมติฐานมี 2 ประเภทคือ

1) สมมติฐานของการวิจัย (Research Hypothesis) เป็นการสมมติที่เขียนอยู่ในรูปของข้อความที่อธิบายความสัมพันธ์ของตัวแปรที่ศึกษา แบ่งออกเป็น 2 ประเภท คือ สมมติฐานแบบมีทิศทาง (Direction Hypothesis) และ สมมติฐานแบบไม่มีทิศทาง (Non-direction Hypothesis)

2) สมมติฐานในทางสถิติ (Statistical Hypothesis) เป็นสมมติฐานที่เขียนขึ้นในรูปโครงสร้างทางคณิตศาสตร์เพื่ออธิบายความสัมพันธ์ของตัวแปร ประกอบด้วยสมมติฐานที่เป็นกลางหรือ

สมมติฐานหลัก (Null Hypothesis : H_0) เช่น เท่ากับ มากกว่าเท่ากับ หรือน้อยกว่าเท่ากับ สมมติฐานไม่เป็นกลาง หรือสมมติฐานรองหรือสมมติฐานทางเลือก (Alternative Hypothesis : H_a หรือ H_1) เช่น มากกว่า น้อยกว่า หรือไม่เท่ากับ

ประเภทของความคลาดเคลื่อน

1. ความคลาดเคลื่อนประเภท I (Type I error) เป็นความคลาดเคลื่อนที่เกิดขึ้นจากการปฏิเสธสมมติฐานกลาง (H_0) เมื่อสมมติฐานกลางเป็นจริง และเรียกความผิดพลาดชนิดนี้ว่า "ระดับนัยสำคัญ" (Level of Significance)

2. ความคลาดเคลื่อนประเภท II (Type II error) เป็นความคลาดเคลื่อนที่เกิดขึ้นจากการยอมรับสมมติฐานกลาง (H_0) เมื่อสมมติฐานกลางไม่เป็นจริง ตามตารางที่ 2.5

ตารางที่ 2.5 ข้อเท็จจริงกับการตัดสินใจ

การตัดสินใจ	**ข้อเท็จจริงของ H_0**	
	H_0 เป็นจริง	**H_0 ไม่เป็นจริง**
ปฏิเสธ H_0	ความคลาดเคลื่อนประเภท I เขียนแทนด้วย α	การตัดสินใจถูกต้อง
ยอมรับ H_0	การตัดสินใจถูกต้อง	ความคลาดเคลื่อนประเภท II เขียนแทนด้วย β

ซึ่ง α และ β เป็นความน่าจะเป็นที่จะตัดสินใจผิด 1- α และ 1- β เป็นความน่าจะเป็นที่จะตัดสินใจถูกต้อง ไม่ว่าจะตัดสินใจอย่างไรก็มีโอกาสคลาดเคลื่อนได้ทั้ง 2 ชนิด ดังนั้นการตัดสินใจในแต่ละครั้งจึงต้องการให้ความน่าจะเป็นที่จะเกิดจากความคลาดเคลื่อนทั้ง 2 ชนิดมีค่าน้อย ซึ่งพบว่า α และ β จะมีค่าลดลงถ้าขนาดของตัวอย่างเพิ่มขึ้น แต่การเพิ่มของขนาดตัวอย่างก็จะเป็นการเพิ่มค่าใช้จ่ายและเวลามากยิ่งขึ้น นอกจากนั้นแล้วยังพบว่า α และ β มีความสัมพันธ์กัน โดยถ้า α มีค่าลดลง β จะเพิ่มขึ้นหรือถ้า α มีค่าเพิ่มขึ้น β ก็จะมีค่าลดลง แต่ผลบวกของ α และ β ไม่เท่ากับ 1 และโดยเหตุที่ความน่าจะเป็นของการเกิดความคลาดเคลื่อนชนิดที่ 2 หรือ β มีผลกระทบต่อการตัดสินใจมากกว่าความน่าจะเป็นของการเกิดความคลาดเคลื่อนชนิดที่ 1 หรือ α ด้วยเหตุนี้ ในการทดสอบสมมติฐานแต่ละครั้งผู้ทดสอบต้องทำการเลือกขนาดของ α และ n ไว้ก่อน แล้วค่าของ β ก็จะถูกกำหนดโดย α และ n ข้างต้น ทั่วไปการทดสอบสมมติฐานนิยมกำหนดระดับความมีนัยสำคัญ $\alpha = 0.05$ หรือ 0.01

ประโยชน์ของสมมุติฐาน

1) ช่วยบอกขอบเขตของปัญหา
2) ช่วยชี้แนวทางในการวางแผนการวิจัย
3) ช่วยให้นักวิจัยมีความคิดแจ่มแจ้งในเรื่องที่ ทำการวิจัย
4) เป็นแนวทางในการลงสรุป

ลักษณะของสมมุติฐานที่ดี

1) สอดคล้องกับจุดมุ่งหมายของการวิจัย
2) อธิบายหรือตอบคำถามได้หมด
3) แต่ละข้อควรตอบคำถามเพียงข้อเดียว
4) สอดคล้องกับสภาพความเป็นจริง
5) สมเหตุสมผลตามทฤษฎี
6) เข้าใจง่าย ชัดเจน
7) สามารถตรวจสอบได้
8) มีขอบเขตพอเหมาะ
9) มีอำนาจในการพยากรณ์สูง

การทดสอบสมมติฐาน (Tests of Hypothesis)

จากผลการทดสอบโดยการวัดของโปรแกรมที่พัฒนาขึ้นมา เปรียบเทียบกับเครื่องมือวัด JDSU ว่าจะสามารถยอมรับได้หรือไม่ แค่ไหนนั้น ก็โดยการใช้วิธีการทดสอบสมมติฐาน ซึ่งมีวิธีการดังนี้

โดยจากการวัดทดสอบจำนวน 10 ครั้ง ที่ CODEC ต่างๆ ซึ่งจะนำค่าเฉลี่ยและค่าเบี่ยงแบนมาตรฐานมาคำนวณโดยใช้สูตร

$$\overline{X}_1 = \{\sum_{i=1}^{n1} X_{1i}\} / n_1$$

$$\overline{X}_2 = \{\sum_{i=1}^{n2} X_{2i}\} / n_2$$

$$Z = (\overline{x}_1 - \overline{x}_2) / \sqrt{(\sigma_1^2 / n_1)+(\sigma_2^2 / n_2)}$$

เมื่อ $\overline{x}$ คือ ค่าเฉลี่ยที่วัดได้

σ คือ ค่าเบี่ยงแบนมาตรฐาน

n คือ จำนวนที่ทดสอบ

2.12 งานวิจัยที่เกี่ยวข้อง

2.11.1 งานวิจัยเรื่องโปรแกรมช่วยออกแบบเครือข่าย VoIP (อรศรี ศรีระษา, 2545) ได้สรุปไว้ว่า โปรแกรมช่วยออกแบบเครือข่าย VoIP เป็นเครื่องมือที่ช่วยออกแบบโดยมุ่งเน้นการคำนวณหาขนาดของอุปกรณ์หลักต่างๆ ในโครงข่าย VoIP เช่น ขนาดของ Gateway จำนวนของ Gatekeeper ขนาดของสื่อสัญญาณที่ใช้เชื่อมโยงกันในโครงข่ายไอพี โดยคำนึงคุณภาพการให้บริการของสัญญาณเสียงคือ เรื่องข้อจำกัดของความล้าช้าของสัญญาณและประสิทธิภาพการใช้งานของวงจรเพื่อหลีกเหลี่ยงการเกิดสภาวะปริมาณทราฟฟิกคับคั่งในเครือข่าย โดยจะแสดงผลการออกแบบโครงสร้างของโครงข่าย VoIP และสามารถนำไปเป็นพื้นฐานประกอบการออกแบบเครือข่าย VoIP จริง เพื่อใช้เป็นข้อมูลในการวิเคราะห์และตัดสินใจหารูปแบบเครือข่ายที่เหมาะสมและสอดคล้องตามปริมาณความต้องการใช้งานและค่าใช้จ่ายเพื่อเป็นข้อมูลในการวิเคราะห์และตัดสินใจเพื่อหารูปแบบเครือข่ายที่เหมาะสมและสอดคล้องกับปริมาณการใช้งานภายในเครือข่าย

2.11.2 งานวิจัยเรื่อง ระบบการวิเคราะห์แบนด์วิดท์ของเครือข่ายสำหรับการส่งข้อมูลเสียงบนไอพี (วาริน เล้าสกุล, 2544) ได้สรุปไว้ว่าการพัฒนาโปรแกรมวิเคราะห์แบนด์วิดท์จะใช้เป็นเครื่องมือสนับสนุนการตัดสินใจของผู้ออกแบบเครือข่ายในการออกแบบขนาดแบนด์วิดท์แต่ละเส้นทางที่เชื่อมโยงโหนดต่างๆ เข้าหากันว่าควรจะมีค่าความเร็วของการส่งข้อมูลสายเท่าไรเพราะว่าค่าเช่าวงจรจะเพิ่มราคาตามขนาดความเร็วการส่งข้อมูลสาย ดังนั้นผู้ออกแบบเครือข่ายจึงต้องออกแบบให้เส้นทางเชื่อมต่อโหนดภายในเครือข่ายมีขนาดที่เหมาะสม มิฉะนั้นจะทำให้ต้นทุนการสร้างเครือข่ายสูงจนเกินจำเป็น โดยโปรแกรมวิเคราะห์แบนด์วิดท์ มีจุดประสงค์หลักเพื่อนำเสนอผลการคำนวณที่แสดงให้เห็นถึงขนาดความเร็วการส่งข้อมูลของสายบนเส้นทางเชื่อมโยงโหนดต่างๆ ที่มีต้นทุนเครือข่ายต่ำที่สุดในขณะที่ค่า Round Trip Time (RTT) ของทุกเส้นทางในเครือข่ายจะมีค่าไม่เกินค่าที่กำหนดไว้ที่ 200 มิลลิวินาที

จากการศึกษางานวิจัยที่เกี่ยวข้องกับวิทยานิพนธ์ที่นำเสนอสามารถเปรียบเทียบคุณสมบัติได้ดังตารางที่ 2.6

ตารางที่ 2.6 การเปรียบเทียบคุณลักษณะของงานวิจัยที่เกี่ยวข้อง

ความสามารถของโปรแกรม / งานวิจัย	*VNDAT* (1)	*BASVN* (2)	*QSMP* (3)
หาขนาดของเกตเวย์	✓	✗	✗
หาจำนวน Gatekeeper	✓	✗	✗
หาขนาดของสื่อสัญญาณ	✓	✓	✗
วัดแบนด์วิดท์ที่เหลือของสื่อสัญญาณ	✗	✗	✓
วัดการสูญหายของแพ็คเก็ต	✗	✗	✓
วัดความผันแปรเฉลี่ยของระยะเวลาดีเลย์ (Jitter)	✗	✗	✓
หา Concurrent Users ในแต่ละ CODEC	✗	✗	✓

หมายเหตุ 1. VNDAT = VoIP Network Design Assistant Tool

2. BASVN = Bandwidth Analysis System for VoIP Network

3. QSMP = Development of a Quality of Service Measurement Program for Voice over IP usage (นำเสนอในงานวิทยานิพนธ์ฉบับนี้)