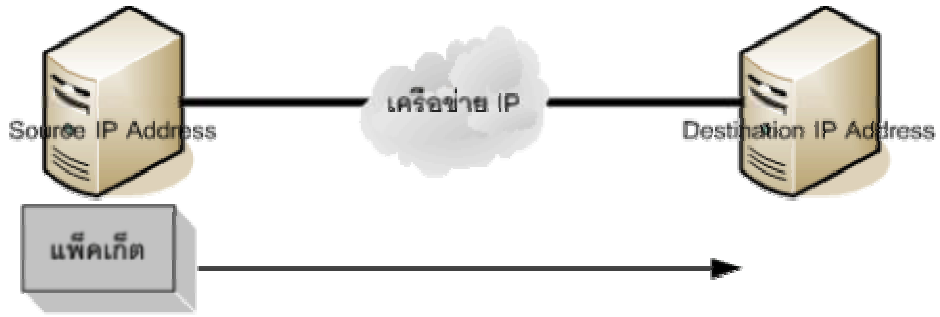
บทที่ 2

Voice over the Internet Protocol : VOIP

2.1 หลักการพื้นฐานของเครือข่ายไอพี

เครือข่ายไอพี (Internet Protocol) มีพัฒนามาจากรากฐานระบบการสื่อสารแบบแพ็กเก็ต โดยระบบมีการกำหนดแอดเดรส ที่เรียกว่า ไอพีแอดเดรส จากไอพีแอดเดรสหนึ่งไปยัง อีกไอพีแอดเดรสหนึ่ง ใช้หลักการบรรจุข้อมูลใส่ใน แพ็กเก็ต แล้วส่งไปในเครือข่าย ระบบการจัดส่งแพ็กเก็ตกระทำด้วยอุปกรณ์สื่อสารจำพวกเราเตอร์ มีหลักพื้นฐานการส่งแบบ ไปรษณีย์สมัยเก่า บางที่เราจึงเรียกการส่งแบบนี้ว่า ดาต้าแกรม

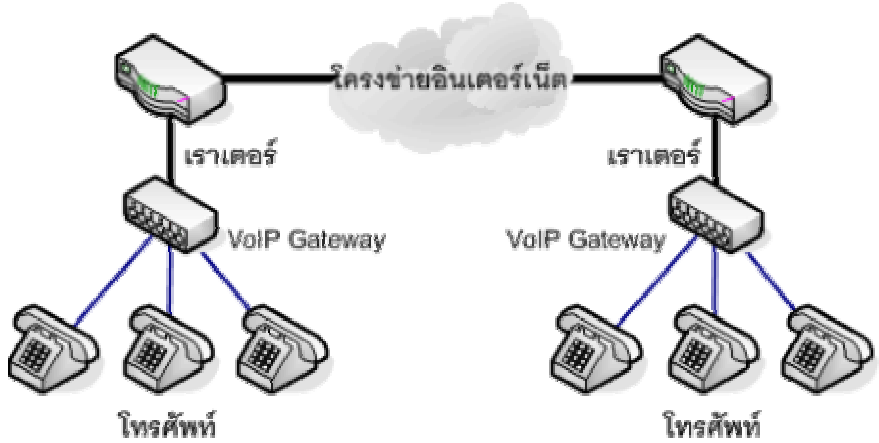
การสื่อสารแบบไอพีแพ็กเก็ต จะเป็นการส่งแพ็กเก็ตเข้าไปในเครือข่าย โดยไม่มีการประกันว่า แพ็กเก็ตนั้นจะถึงปลายทาง เมื่อไร ดังนั้นรูปแบบของเครือข่ายไอพีจึงไม่เหมาะสมกับการสื่อสารแบบต่อเนื่อง เช่น ส่งเสียง หรือวิดีโอ



รูปที่ 2.1.1 ภาพการส่ง แพ็กเก็ตระหว่างเครือข่าย

ครั้งเมื่อมีเครือข่ายไอพีกว้างขวางและเชื่อมโยงกันมากขึ้น ความต้องการส่งสัญญาณข้อมูลเสียงที่ได้คุณภาพก็เกิดขึ้น สิ่งที่สำคัญ คือระบบประกันคุณภาพการสื่อสาร โดยจัดลำดับความสำคัญ หรือจองช่องสัญญาณไว้ให้ก่อน ระบบการสื่อสารในรูปแบบใหม่นี้ จะต้องกระทำโดยเราท์เตอร์

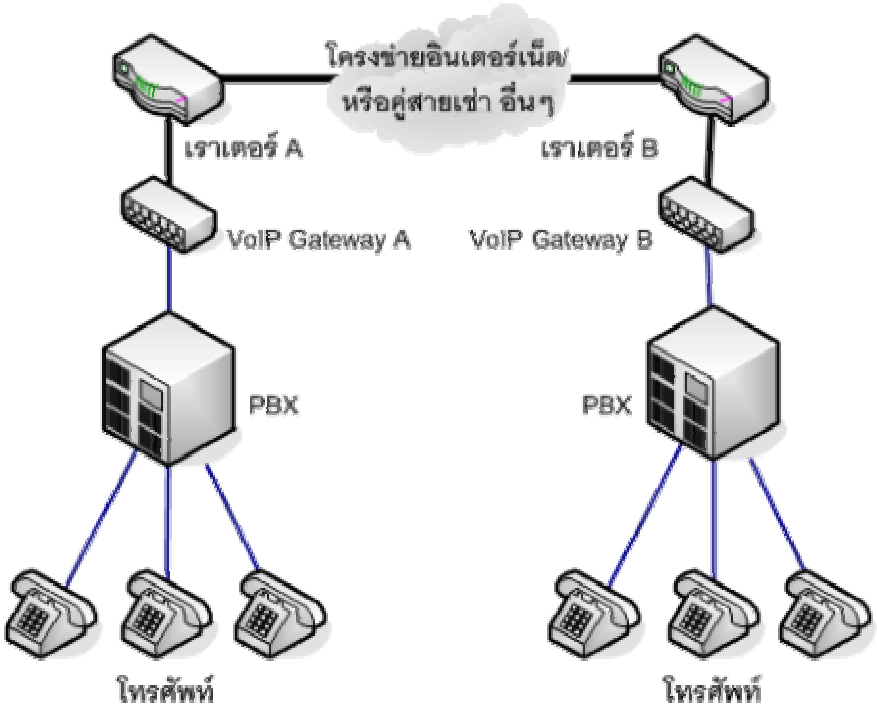
การส่งเสียงบนเครือข่ายไอพี หรือเรียกว่า VoIP-Voice Over IP เป็นระบบที่นำสัญญาณข้อมูลเสียงมาบรรจุลงเป็นแพ็กเก็ต ไอพี แล้วส่งไปโดยที่เราท์เตอร์มีวิธีการปรับตัวเพื่อรับสัญญาณแพ็กเก็ต และยังแก้ปัญหาบางอย่างให้ เช่น การบีบอัดสัญญาณเสียง ให้มีขนาดเล็กลง การแก้ปัญหาเมื่อมีบางแพ็กเก็ตสูญหาย หรือได้มาล่าช้า



รูปที่ 2.1.2 ภาพการเชื่อมต่อเครือข่ายโทรศัพท์ผ่านอินเตอร์เน็ตโดยนำ VoIP มาใช้

ระบบ VoIP เป็นระบบที่นำสัญญาณเสียงที่ผ่านการดิจิไตซ์ โดยหนึ่งช่องเสียงเมื่อแปลงเป็นข้อมูลจะมีขนาด 64 กิโลบิตต่อ วินาที การนำข้อมูลเสียงขนาด 64 Kbps นี้ ต้องนำมาบีบอัด โดยทั่วไปจะเหลือประมาณ 10 Kbps ต่อช่องสัญญาณเสียงแล้วจึง บรรจุลงในไอพีแพ็กเก็ต เพื่อส่งผ่านทางเครือข่ายไอพี การสื่อสารผ่านทางเครือข่ายไอพีต้องมีเราเตอร์ที่ทำหน้าที่พิเศษเพื่อประกันคุณภาพช่องสัญญาณไอพีนี้ เพื่อให้ข้อมูลไปถึง ปลายทางหรือกลับมาได้อย่างถูกต้อง และอาจมีการให้สิทธิพิเศษก่อนแพ็กเก็ตไอพีอื่น เพื่อการให้บริการที่ทำให้เสียงมีคุณภาพ

ช่องสัญญาณไอพีนี้ เพื่อให้ข้อมูลไปถึง ปลายทางหรือกลับมาได้อย่างถูกต้อง และอาจมีการให้สิทธิพิเศษก่อนแพ็กเก็ตไอพีอื่น (Quality of Service : QoS) เพื่อการให้บริการที่ทำให้เสียงมีคุณภาพ จากระบบดังกล่าวนี้เอง จึงสามารถนำมาประยุกต์ใช้กับระบบเชื่อมโยงเครือข่ายโทรศัพท์ระหว่างสำนักงาน โดยแต่ละสำนักงานสามารถ ใช้ระบบสื่อสารโทรศัพท์ผ่านทางเครือข่ายไอพี (VoIP) รวมถึงยังสามารถรับส่งข้อมูล (data) ไปพร้อมๆ กันได้



รูปที่ 2.1.3 ภาพการเชื่อมต่อระบบโทรศัพท์โดยใช้ VoIP กับ PBX มาใช้

ด้วยวิธีการสื่อสารแบบ VoIP จึงทำให้ระบบโทรศัพท์ที่เป็นตู้ชุมสายภายในขององค์กร สามารถเชื่อมถึงกันผ่านทางเครือข่าย ไอพี การสื่อสารแบบนี้ทำให้สามารถใช้โทรศัพท์ข้ามถึงกันได้ในลักษณะ PABX กับ PABX และทำให้ประหยัดค่าใช้จ่ายได้มาก

2.2 ขั้นตอนการทำงานของ VoIP

2.2.1 ขั้นตอนการทำงานเบื้องต้น

1. เมื่อผู้พูด โทรศัพท์จากเครื่องโทรศัพท์ธรรมดา หรือพูดผ่านไมโครโฟนที่ถูกต่อเข้ากับการ์ด เสียงของเครื่องคอมพิวเตอร์คลื่นสัญญาณเสียง แบบ อนาล็อกก็จะได้รับการแปลงเป็นสัญญาณดิจิตอล จากนั้นจะถูกบีบอัดด้วยตัวถอดรหัสผ่านอุปกรณ์ PBX (Private Box Exchang) หรือ VoIP Gateway

2. เมื่อผ่าน VoIP Gateway แล้วก็จะถูกส่งต่อไปยัง Gatekeeper เพื่อค้นหาเครื่องปลายทางที่จะรับการติดต่อ เช่น หมายเลขไอพี หมายเลข โทรศัพท์ เป็นต้น แล้วแปลงเป็นแพ็กเกจข้อมูลส่งออกไปบนระบบ เครือข่ายอินเทอร์เน็ตนั่นเอง

3. จะผ่านมาที่ VoIP Gateway ปลายทาง แล้วจะจึงทำการย้อนกระบวนการทั้งหมดเพื่อส่งให้กับผู้รับปลายทางต่อไป

2.2.2. กระบวนการทำงานของเทคโนโลยี VoIP มีรายละเอียดการทำงานดังนี้

Conversion to PCM (Pulse Code Modulation) จะเป็นการแปลงสัญญาณ Analog ให้ไปอยู่ในรูปแบบสัญญาณ Digital หรือที่เรียกว่า PCM

PCM (Pulse Code Modulation)

รูปที่ 2.2.1 ภาพขั้นตอนแรกจะเป็นการแปลงสัญญาณ

Removal of Echo จะเป็นการมีการแยกสัญญาณออกเป็นส่วนๆ เพื่อทำการตัดสัญญาณ Echo ออก ซึ่งกระบวนการนี้จะถูกจัดการโดย DSP (Digital Signal Processors)

Removal of Echo

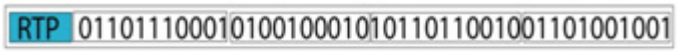
รูปที่ 2.2.2 ภาพขั้นตอนการแยกสัญญาณออกเป็นส่วนๆ เพื่อทำการตัดสัญญาณ Echo ออก

Framing ในส่วนของสัญญาณที่เหลือนั้น ก็จะถูกแบ่งและจัดรูปแบบขึ้นมาใหม่ในรูปของ Frame ซึ่งกระบวนการนี้จะถูกจัดการโดยรูปแบบการบีบอัดที่เรียกว่า CODEC หลังจากกระบวนการนี้แล้ว Frame ของสัญญาณเสียงจะถูกสร้างขึ้น

Framing Process

รูปที่ 2.2.3 ภาพการจัดแบ่งและจัดรูปแบบขึ้นมาใหม่ในรูปของ Frame

Packetisation ในกระบวนการนี้จะเป็นการแปลง Frame ของสัญญาณให้มาอยู่ในรูปของ Packet ซึ่งจะมีการเพิ่ม Header เข้าไปใน Packet โดยในส่วนของ Header นั้น ก็จะประกอบไปด้วยข้อมูลที่เรียกว่า Sequence Number และ Time Stamp หลังจากนั้น Packet นี้จะถูกส่งต่อไปที่ Host Processor



Packetisation Process

รูปที่ 2.2.4 ภาพการแปลง Frame ของสัญญาณให้มาอยู่ในรูปของ Packet

Address and Delivery หลังจากที่ได้แปลงสัญญาณให้อยู่ในรูปของ Packet แล้ว ข้อมูลนั้นจะถูกนำมาวิเคราะห์และใส่ค่า IP Address ปลายทาง

Address and Delivery

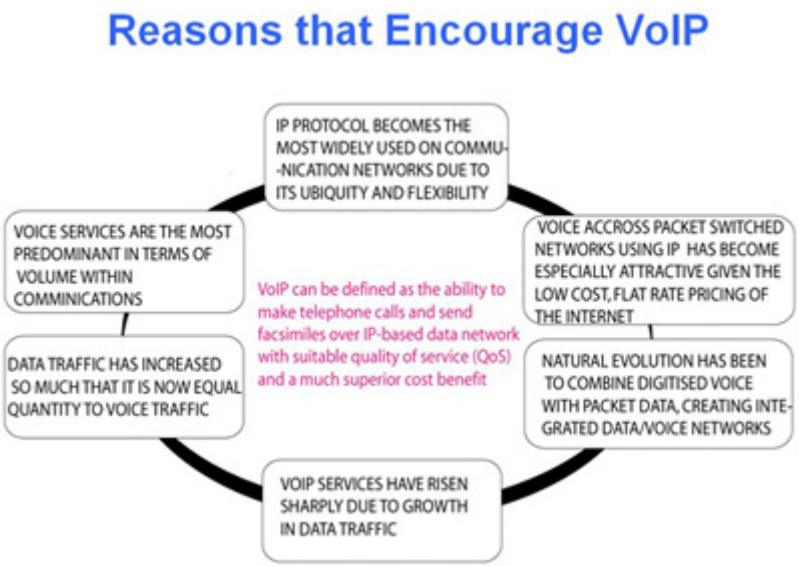
รูปที่ 2.2.5 ภาพการใส่ค่า IP Address ปลายทาง

Conversion to Analog หลังจากที่ได้ทำการใส่ค่าของ IP Address ปลายทางไปใน Header ของ Packet แล้วนั้น เมื่อ Packet เหล่านั้นไปถึงด้านปลายทาง ข้อมูล Header เหล่านี้จะถูกแยกออกเพื่อให้เหลือแค่ Voice Frame หลังจากนั้นก็จะทำการแปลงสัญญาณ Digital PCM ให้กลับมาเป็นสัญญาณรูปแบบ Analog ที่เป็นสัญญาณเสียงที่เราได้ยินกันอีกครั้งหนึ่ง

Conversion to Analog

รูปที่ 2.2.6 ภาพการแปลงสัญญาณ Digital PCM ให้กลับมาเป็นสัญญาณรูปแบบ ที่เราได้ยินกันอีกครั้งหนึ่ง

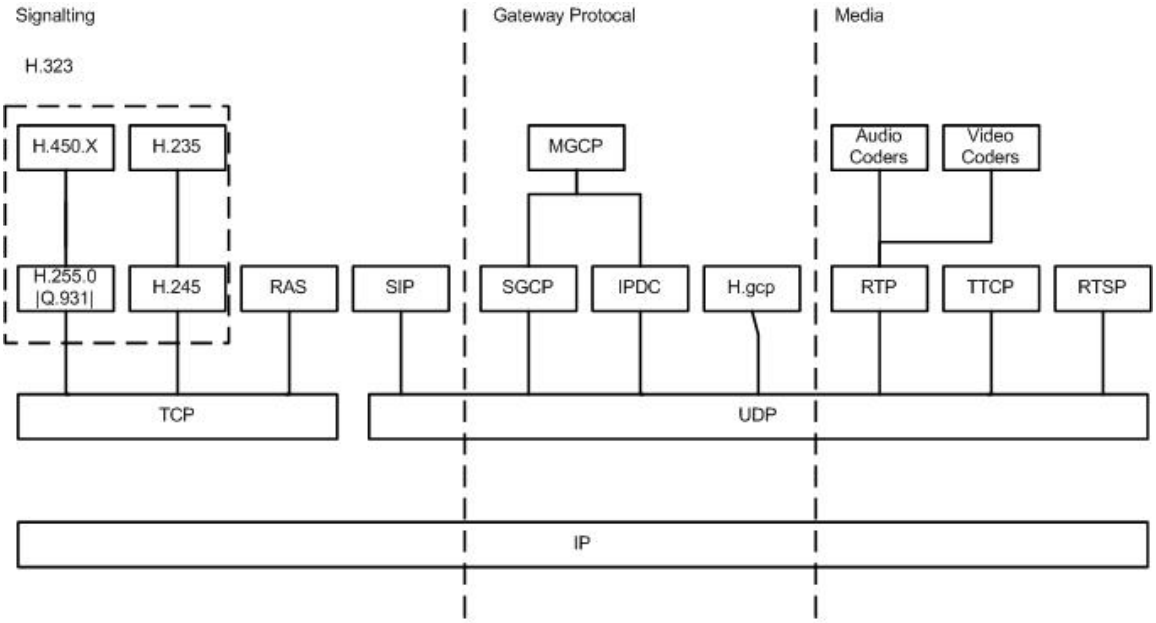
Error Correction กระบวนการนี้จะเป็นกระบวนการที่ใช้ในการตรวจสอบและแก้ไขข้อผิดพลาดซึ่งอาจจะเกิดขึ้นระหว่างการส่งสัญญาณและนำมาซึ่งความผิดเพี้ยนหรือความเสียหายของสัญญาณจนทำให้เราไม่สามารถทำการสื่อสารอย่างถูกต้องได้



รูปที่ 2.2.7 ภาพขั้นตอนการตรวจสอบความผิดพลาด

2.3. Standard of VoIP Technology

โปรโตคอลสำหรับ VoIP มีอยู่ 2 มาตรฐานคือ H.323[2] และ SIP(Session Initial Protocol)[1] โปรโตคอล H.323 เป็นโปรโตคอลที่พัฒนาโดย ITU-T (International Telecommunications Union- Telecommunications section) ส่วน SIP ถูกพัฒนาโดย IETF (Internet Engineering Task Force) มาตรฐานเหล่านี้ เราสามารถเรียกได้อีกอย่างหนึ่งว่า “Call Control Technologies”โปรโตคอลทั้งสองมีหน้าที่หลักในการสร้าง สิ้นสุด และการเปลี่ยนแปลงรายละเอียดของการเรียก ระหว่างผู้ใช้ VoIP รวมทั้งยังสามารถให้ฟังก์ชันเพิ่มเติมอื่นๆ โปรโตคอลทั้งสองเป็นโปรโตคอลสำหรับ VoIP ซึ่งใช้บริการชุดโปรโตคอล TCP/IP ในชั้นต่ำกว่า และสามารถใช้งานร่วมกับโปรโตคอลอื่น เพื่อให้เกิดการบริการที่มีคุณภาพมากขึ้น



รูปที่ 2.3.1 VOIP Protocol Stack

โปรโตคอล H.323 และ SIP เป็นโปรโตคอลในชั้นแอปปลิเคชัน (application layer) และใช้บริการของโปรโตคอลในชั้นที่ต่ำกว่า SIP สามารถใช้ได้ทั้ง UDP และ TCP ส่วน H.323 ใช้ TCP เท่านั้น แต่เนื่องจากว่าฟังก์ชันของ H.323 และ SIP มีขอบเขตจำกัด ดังนั้นจึงได้นำโปรโตคอลอื่นมาช่วยในการทำงาน ซึ่งได้แก่ RTSP (Real-time Streaming Protocol) [3] RSVP (Resource Reservation Protocol) [7] และ RTP/RTCP [4] ซึ่งทำให้ VoIP สามารถให้บริการได้อย่างมีประสิทธิภาพมากขึ้น โปรโตคอลดังกล่าวเป็นโปรโตคอลในชั้นแอพปลิเคชันซึ่งทำงานอยู่บนชุดโปรโตคอล TCP/IP โปรโตคอลเหล่านี้ไม่ได้เป็นโปรโตคอลเฉพาะสำหรับ VoIP ดังนั้นจะกล่าวถึงอย่างคร่าวๆ ในส่วนนี้ แต่สำหรับโปรโตคอล SIP ซึ่งเป็นโปรโตคอลหลักสำหรับ VoIP จะกล่าวถึงรายละเอียดในหัวข้อถัดไป

2.3.1 SIP: Session Initial Protocol)

มาตรฐาน SIP นั้นถือเป็นมาตรฐานใหม่ในการใช้งานเทคโนโลยี VoIP โดยที่มาตรฐาน SIP นั้น ได้ถูกออกแบบมาให้ใช้งานกับระบบ IP โดยเฉพาะ ซึ่งโดยปกติแล้วเราจะแนะนำให้ลูกค้าใหม่ที่จะมีการใช้งาน VoIP ให้มีการใช้งานอยู่บนมาตรฐาน SIP โดยมีเนื้อหาสำคัญดังนี้

1.มาตรฐาน SIP นั้นเป็นมาตรฐานภายใต้ IETF Standard ซึ่งถูกออกแบบมาสำหรับการเชื่อมต่อ VoIP

2.มาตรฐาน SIP นั้นจะเป็นมาตรฐาน Application Layer Control Protocol สำหรับการเริ่มต้น (Creating), การปรับเปลี่ยน)Modifying) และการสิ้นสุด)Terminating) ของ Session หรือการติดต่อสื่อสารหนึ่งครั้ง

3.มาตรฐาน SIP จะมีสถาปัตยกรรมการทำงานคล้ายคลึงการทำงานแบบ Client-Server Protocol

4.เป็นมาตรฐานที่มี Reliability ที่ค่อนข้างสูง

SIP เป็นโปรโตคอลใช้งานสำหรับ IP Telephony ที่กำหนดโดย IETF (Internet Engineering Task Force) SIP เป็นโปรโตคอลในชั้นแอปปลิเคชันซึ่งทำหน้าที่ในการสร้าง สิ้นสุด และเปลี่ยนแปลงแก้ไข เซสชันของพหุสื่อ (multimedia session) หรือ การเรียก ซึ่งรวมถึง Internet telephony การประชุมแบบพหุสื่อ (multimedia conference) และแอปปลิเคชันอื่นที่คล้ายคลึงกัน SIP เป็นโปรโตคอลไคล์เอนท์-เซิร์ฟเวอร์ (client-server) โดยใช้การส่งข้อมูลในรูปของตัวอักษร (text based) เช่นเดียวกับโปรโตคอล HTTP (Hypertext Transfer Protocol) รวมทั้งยังมีกลไกที่คล้ายคลึงกัน ทำให้สามารถใช้เฮดเดอร์และกลไกที่มีอยู่บางอย่างของ HTTP ได้ สำหรับฟังก์ชันที่ SIP สนับสนุนมีดังนี้

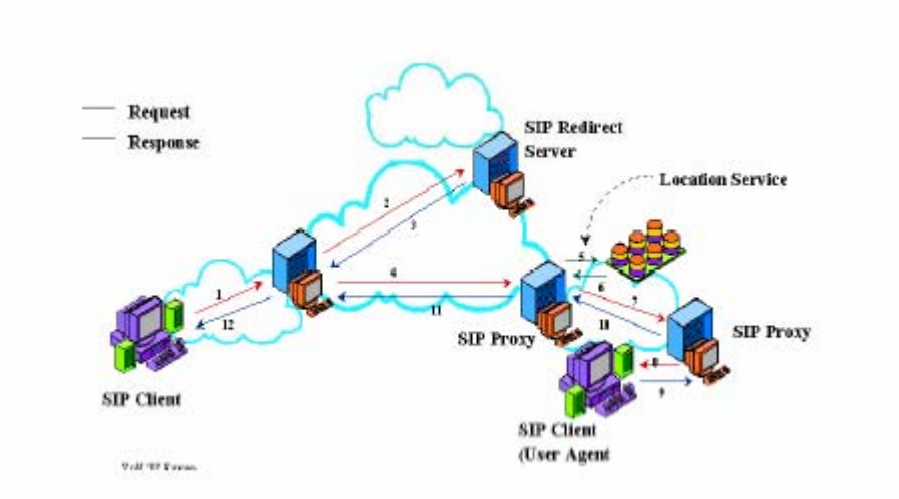
• User location การกำหนด endpoint ที่ใช้ในเซสชันการสื่อสาร

• User capabilities การกำหนดมีเดียและพารามิเตอร์ของมีเดียที่ใช้ในการสื่อสาร

• User availability การกำหนดความต้องการของผู้ถูกเรียกว่าต้องการเข้าร่วมในเซสชันหรือไม่

• Call setup การสร้าง การเรียก และกำหนดพารามิเตอร์ของการเรียก

• Call handling การจัดการกับ การเรียก รวมทั้งการโอนย้าย การเรียก และการสิ้นสุดการเรียก



รูปที่ 2.3.2 ภาพแสดงสถาปัตยกรรมของ SIP

SIP ถูกพัฒนาโดย IETF โดยเป็นส่วนหนึ่งของสถาปัตยกรรมควบคุมและข้อมูลพหุสื่อ (multimedia data and control architecture) ซึ่งรวมถึงโปรโตคอล เช่น RSVP RTP RTSP และ SDP (Session Data Protocol) เป็นต้ โดย SIP สามารถใช้งานหรือทำงานร่วมกับโปรโตคอลเหล่านี้เพื่อประสิทธิภาพที่ดีขึ้น แต้งก์ชันและการทำงานของ SIP ไม่ขึ้นอยู่กับโปรโตคอลเหล่านี้ สำหรับใน SIP ได้ถูกพัฒนาอยู่ในเวอร์ชัน 2

2.3.1.1. สถาปัตยกรรมและองค์ประกอบของ SIP (SIP architecture & Components)

SIP เป็นโปรโตคอลไคลเอนท์-เซิร์ฟเวอร์ ไคลเอนท์จะทำหน้าที่ส่งคำร้องขอให้กับเซิร์ฟเวอร์เพื่อทำการประมวลผลแล้วจึงตอบสนองกับมายัง ไคลเอนท์ ในการส่งแมสเสจร้องขอแมสเสจอาจจะถูกส่งผ่านเซิร์ฟเวอร์หลายตัวจนกระทั่งถึงเซิร์ฟเวอร์ที่สามารถตอบสนองคำร้องขอของไคลเอนท์ได้ ในระบบ SIP จะมีองค์ประกอบที่ทำหน้าที่ของไคลเอนท์และเซิร์ฟเวอร์ องค์ประกอบเหล่านี้จะทำการติดต่อสื่อสารกันโดยใช้แมสเสจ SIP ซึ่งมีสถาปัตยกรรมดังรูปที่ 2.3.4

ใน SIP จะแบ่งองค์ประกอบเป็น 2 ชนิดหลักคือ user agent และ network server ดังรายละเอียดต่อไปนี้

1. User agent เป็น endpoint ที่ทำหน้าที่แทนผู้ใช้ในการติดต่อสื่อสารเนื่องจากว่าผู้ใช้ต้องสามารถเริ่ม การเรียก หรือตอบสนองต่อการเรียก ที่เข้ามา ดังนั้น user agent ควรจะสามารถทำหน้าที่เป็นได้ทั้งไคลเอนท์และเซิร์ฟเวอร์ในกรณีที่มีการเริ่ม การเรียก ผู้ใช้จะทำหน้าที่เป็น ไคลเอนท์เพื่อทำการร้องขอไปยังผู้ถูกเรียกซึ่งจะทำหน้าเป็นเซิร์ฟเวอร์ในการตอบสนองการร้องขอ โดยทั่วไป user agent จึงประกอบด้วยส่วนที่ทำหน้าที่เป็นไคลเอนท์และเซิร์ฟเวอร์ดังนี้

User agent client (UAC) จะทำหน้าที่ในการเริ่ม การเรียก โดยการส่งส่งแมสเสจร้องขอไปยังผู้ถูกเรียกโดยผ่านทาง network server

2. User agent server (UAS) จะทำหน้าที่ในการรับคำร้องขอ และตอบสนองต่อคำร้องขอโดยจะรอการตอบสนองจากผู้ใช้ ซึ่งการตอบสนองอาจจะเป็นการยอมรับหรือปฏิเสธการเรียก ในกรณีที่ผู้ใช้มีการใช้งานเทอร์มินัลหลายตัว ผู้ใช้ยังอาจจะกำหนดให้ UAS ทำการ redirect ไปยังที่ UAS อื่นที่ผู้ใช้ใช้งานอยู่จริง

2.3.1.2 Network server

เป็นเซิร์ฟเวอร์ภายในเครือข่ายซึ่งจะทำหน้าที่ในการจัดการกับแมสเสจที่ได้รับ โดยอาจจะได้รับจาก user agent หรือ network server อื่นๆ การจัดการกับแมสเสจจะขึ้นกับชนิดของเซิร์ฟเวอร์ ซึ่งมี 2ชนิดคือ

1.Proxy server เซิร์ฟเวอร์จะทำการกำหนดเอนทิตี้ที่จะรับ ข้อมูลต่อไป โดยอาจจะเป็น UAS หรือ network server ก็ได้ จากนั้นเซิร์ฟเวอร์จะเป็นผู้ทำการร้องขอไปยังเอนทิตี้นั้นพร้อมกับข้อมูลตอบสนองให้กับ UAC (หรืออาจจะเป็น network server อื่นที่ส่งข้อมูลร้องขอมา) เพื่อระบุว่ากำลังรอการตอบสนองจากผู้ถูกเรียก เมื่อเซิร์ฟเวอร์ได้รับการตอบสนองจากผู้ถูกเรียกหรือ UAS เซิร์ฟเวอร์จึงจะส่งแมสเสจตอบสนองต่อกลับไปให้กับ UAC ดังรูปที่ 22. เซิร์ฟเวอร์ชนิดนี้จะทำหน้าที่เป็นทั้งไคลเอนท์และเซิร์ฟเวอร์ ในกรณีที่ส่งแมสเสจร้องขอจะเป็นไคลเอนท์ส่วนในกรณีที่ส่งข้อมูลตอบสนองจะเป็นเซิร์ฟเวอร์

2. Redirect server เมื่อเซิร์ฟเวอร์ได้รับแมสเสจร้องขอแล้วจะกำหนดเอนทิตี้ที่จะรับข้อมูลต่อไป จากนั้นเซิร์ฟเวอร์จะส่งแอดเดรสของเอนทิตี้นั้นไปให้กับ UAC หรือ network server ที่ส่งข้อมูลร้องขอมา เมื่อ UAC (หรือ network server) ได้รับแอดเดรส แล้วจึงจะทำการส่งคำร้องไปยังเซิร์ฟเวอร์นั้นด้วยตนเอง

เนื่องจากว่าผู้ใช้อาจจะมีการเปลี่ยนเทอร์มินัลที่ใช้งานได้ network server จึงจะต้องสามารถกำหนดเอนทิตี้ที่รับข้อมูลเพื่อให้สามารถส่งแมสเสจให้กับผู้ถูกเรียกได้ โดย network server จะทำการติดต่อกับ location server เพื่อกำหนดเอนทิตี้ต่อไปที่จะรับแมสเสจ location server จะทำหน้าที่ในการหาตำแหน่งปัจจุบันของผู้ถูกเรียกโดยการกำหนดเอนทิตี้ที่จะรับแมสเสจต่อไปแล้วส่งแอดเดรสของเอนทิตี้นี้ให้กับ network server ข้อมูลของ location server จะได้รับจาก registrar ซึ่งทำหน้าที่ในการรับข้อมูลเกี่ยวกับตำแหน่งของผู้ใช้แล้วส่งข้อมูลนี้จะให้กับ location server ในการให้อมูลของผู้ใช้กับ registrar จะทำได้โดยใช้แมสเสจ REGISTER เพื่อบอกตำแหน่งที่อยู่ของผู้ใช้ โดยทั่วไปแล้ registrar จะถูกรวมเข้ากับ network server

2.3.1.3. SIP Respond

โปรโตคอล ซิพ มีข้อความตอบกลับมีความหมายดังนี้

1XX Provisional 100 Trying

ตั้งแต่ 100 ถึง 199 เป็น Provisional message หมายถึง กำลังทำการ จะมีการส่งการตอบกลับประเภทนี้เมื่ออยู่ในขณะการรอ Successful message เพื่อบอกว่ากำลังทำการอยู่(เช่น กำลัง Register อยู่)2XX Successful 200 OK

ตั้งแต่ 200 ถึง 299 เป็น Successful หมายถึง ได้ทำการเรียบร้อยแล้ว

3XX Redirection 302 Moved Temporarily

ตั้งแต่ 300 ถึง 399 เป็น Redirection message หมายถึง ทำการปรับทิศทางใหม่

4XX Client Error 404 Not Found

ตั้งแต่ 300 ถึง 399 เป็น Message error ที่เกิดจากไคลเอนท์ เช่น ไม่พบไคลเอนท์ที่ถามถึง

5XX Server Error 504 Server Time-Out

ตั้งแต่ 500 ถึง 599 เป็น Message error ที่เกิดจากเซิร์ฟเวอร์ เช่น เกิดการหมดเวลา (Time out)

6XX Global Failure 603 Decline

ตั้งแต่ 600 ถึง 699 เป็น Message error ที่เกิดจาก Global เช่น เกิดการ ปฏิเสธการร้องขอ

2.3.1.4 Header Field

Accept-Contact	a	Refer – to	r
Allow-Event	u	Referred-by	b
Call-ID	I	Reject-Contact	j
Contact	m	To	t
Content-Encoding	e	Via	v
Content-length	l		
Content-Type	c		
Event	o		
From	f		
Subject	s		

2.3.1.5. SIP Application

ซิพโปรโตคอล (SIP Protocal) สนับสนุนการติดต่อสื่อสารแบบบุคคลต่อบุคล โดยรวมสื่อที่หลากหลายไว้ด้วยกัน เช่น ตัวหนังสือ,รูปภาพ,เสียง และวีดีโอ เป็นต้น นอกจากนี้ยังใช้ในการบอกตำแหน่งของจดหมายปลายทาง และแสดงสถานะต่างๆ (Presence information) ของผู้ใช้ ดังนั้นจึงเกิดพแอพพลิเคชั่นต่างๆ เช่น เรียลไทม์วิดีโอแชร์ริ่ง (Real-Time Video Sharing),พุชทูทอล์กโอเวอร์เซลลูลาร์ (PoC : Push-to-talk Oer Cellular), โปรแกรมรับส่งสารด่วน (Insant Messaging) และ เกมออนไลน์แบบจุดต่อจุด (Peer to Peer Game Online) เป็นต้น โดยในที่นี้จะยกตัวอย่าง 2 แอพพลิเคชั่น คือ เกมออนไลน์แบบจุดต่อจุดบนโทรศัพท์มือถือ และ โปรแกรมรับส่งสารด่วนผ่านวินโดว์เมสเซนเจอร์ (Windows Messenger) บนเครื่องคอมพิวเตอร์

2.3.1.6. ชื่อและแอดเดรส (Addressing & Naming)

ในระบบ SIP การส่งแมสเสจระหว่างเอนทิตี้จะต้องระบุ SIP URL เพื่อใช้อ้างอิงถึงผู้ใช้ SIP URL จะประกอบด้วย SIP แอดเดรส รูปแบบของแอดเดรสจะอยู่ในรูปของ name@domain โดยอาจจะเป็ user@domain user@address phone-number@gateway และ user@host แอดเดรสนี้จะถูกใช้อ้างอิงถึงผู้ใช้ทั้งผู้เรียกและผู้ถูกเรียกในการส่งแมสเสจ ตัวอย่างของ SIP URL เช่นSIP://j.doe@example.com โดยที่ URL นี้จะอยู่ในส่วนเฮดเดอร์ของแมสเสจ ในการส่งแมสเสจไปยัง SIP URL ที่ระบุไว้จะต้องมีการแปลง SIP แอดเดรสให้อยู่ในของ User@host โดยอาจจะผ่านการแปลงมากกว่าหนึ่งครั้งจนกระทั่งได้ตำแหน่งที่อยู่ของผู้ใช้ ในการแปลงแอดเดรสอาจจะใช้ DNS (Domain Name Service) หรือ LDAP (Lightweight Directory Access Protocol)

2.3.1.7 Locating Server

ในการส่งแมสเสจจะใช้ SIP URL อ้างอิงถึงในการส่ง โดยจะต้องมีการแปลงส่วน domain ของ SIP แอดเดรสไปเป็นหมายเลข IP ซึ่งเป็น แอดเดรสของ SIP server ที่สามารถค้นหาตำแหน่งของผู้ใช้ออกไปได้ การแปลง SIP แอดเดรสอาจจะทำโดย UAC หรือ UAC จะส่งแมสเสจให้กับเซิร์ฟเวอร์ที่กำหนดซึ่งเซิร์ฟเวอร์จะเป็นผู้ที่ทำหน้าที่ในการแปลง SIP แอดเดรสแทน ในการแปลง SIP แอดเดรสนี้สามารถใช้ DNS เข้ามาช่วยได้

2.3.1.8 Locate User

จากข้างต้นเมื่อได้ตำแหน่งของเซิร์ฟเวอร์ที่สามารถส่งข้อมูลให้กับผู้ถูกเรียกแล้วต่อไปจะเป็นการหาตำแหน่งของผู้ถูกเรียก เมื่อ SIP server ได้รับแมสเสจร้องขอแล้ว เซิร์ฟเวอร์จะต้องทำการค้นหาผู้ใช้ที่อ้างอิงถึงใน SIP แอดเดรส โดยการร้องขอข้อมูลไปยัง location server ซึ่งจะตอบกลับด้วยรายการตำแหน่งที่เป็นไปได้ของผู้ถูกเรียก เมื่อ SIP server ได้อมูลเกี่ยวกับตำแหน่งข

องผู้ ถ้าเป็น proxy server จะทำส่งแมสเสจร้องขอต่อไปยังตำแหน่งต่างๆ ตามรายการที่ได้รับจาก location serverไว้ โดยอาจจะส่งแบบ sequential หรือ parallel ส่วนถ้าเป็ redirect server จะส่งรายการตำแหน่งของผู้ถูกเรียกไปให้ผู้เรียกผ่านโดยใช้เฮดเดอร์ contact เพื่อให้ผู้เรียกส่งแมสเสจร้องขอไปเอง สำหรับตำแหน่งของผู้ใช้จะต้องทำการลงทะเบียนกับ registrar โดยใช้เฮดเดอร์ REGISTER รวมทั้งยังอาจจะอัพโหลด script ของผู้ใช้เองเพื่อเก็บไว้ที่เซิร์ฟเวอร์สำหรับจัดการกับการเรียก ตามความต้องการของผู้ใช้

2.3.1.9 ความเชื่อถือได้ (Reliability)

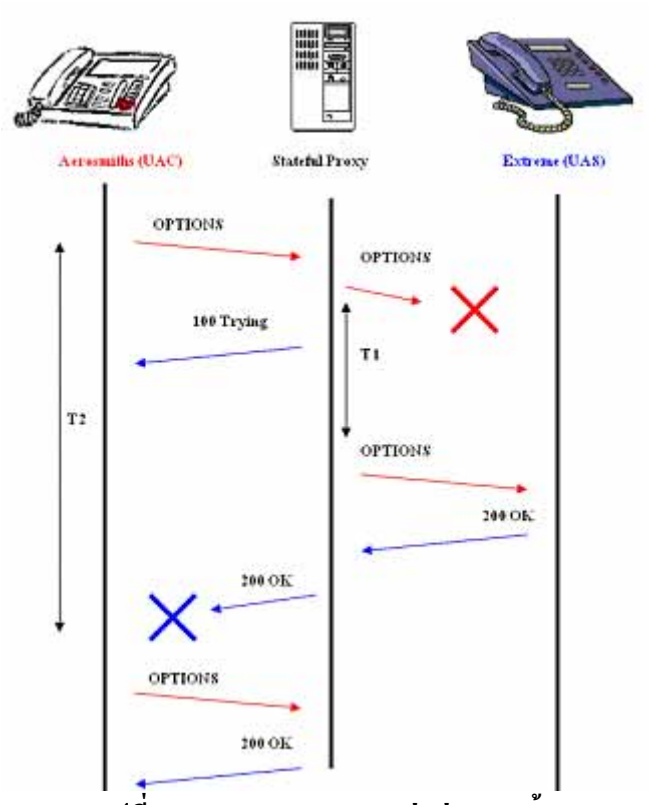
SIP มีกลไกหนึ่งที่ทำให้การรับส่งข้อมูลน่าเชื่อถือในขณะที่ใช้โปรโตคอล UDP (User Datagram Protocol) ซึ่งมีการเชื่อมต่อแบบ Connectionless ส่วนการรับส่งข้อมูลโดยใช้โปรโตคอล TCP (Transmission Control Protocol) นั้นมีความเชื่อถือที่ดีอยู่แล้ว จึงไม่จำเป็นต้องใช้กลไกดังกล่าว แต่แก้ไขโดยการส่งข้อมูลซ้ำเมื่อระบบแจ้งว่ามีการสูญหายของข้อมูลกลไกในการรับส่งข้อมูลให้มีความน่าเชื่อถือมีองค์ประกอบดังนี้

-ตัวจับเวลาส่งข้อมูลซ้ำ

-หมายเลขลำดับคำสั่ง

-ข่าวสารการตอบรับ

ตัวจับเวลาจะเริ่มจับเวลาเมื่อมีการส่งข่าวสารออกไป หากเกินเวลาที่กำหนดไว้ (T1) จะส่งข่าวสารเดิมซ้ำ และเริ่มจับเวลาใหม่ แต่คราวนี้หากเวลาที่จับไว้เกินค่าเวลาที่กำหนด (T2) จึงค่อยส่งข่าวสารซ้ำ ทั้งนี้การส่งข่าวสารซ้ำมีได้จำนวนจำกัด เช่น มากที่สุด 10 ครั้ง เป็นต้น



รูปที่ 2.3.3 ภาพแสดงการส่งข่าวสารซ้ำ

รูปที่ 2.3.3 แสดงตัวอย่างการส่งข่าวสารซ้ำ โดยข่าวสาร OPTIONS ที่ส่งโดย Stateful Proxy Server ไปยัง UAS (User Agent Server) สูญหาย ดังนั้นเมื่อใช้เวลาเกิน T1 (เช่น 500 มิลลิวินาที) จึงมีการส่งข่าวสารซ้ำ และในขณะที่ตัวจับเวลาที่ UAC เกินค่า T2 (เช่น 4 วินาที) จึงต้องส่งข่าวสาร OPTIONS ใหม่อีกครั้ง แต่พร็อกซีทราบว่าข่าวสาร 200 OK ได้สูญหายไป จึงทำการส่งซ้ำ ทั้งนี้ช่วงเวลาระหว่างหมายเลขลำดับคำสั่งไม่ได้แสดงถึงข่าวสารที่สูญหายเสมอไป แต่ว่าอาจเกิดจากการที่ไม่ได้ผ่านขั้นตอนการตรวจสอบสิทธิ์

2.3.1.10 ความสามารถในการขยาย (Protocol xtension)

SIP สามารถรองรับคุณลักษณะใหม่ที่เพิ่มเติมขึ้นสำหรับ เมธอด เฮดเดอร์ และ status code ได้ดังนี้

• เมธอด เซิร์ฟเวอร์จะส่งแมสเสจแสดงความผิดพลาด (error message) กลับมาให้ไคลเอนท์เมธอดที่ร้องขอมาเซิร์ฟเวอร์ไม่เข้าใจ และจะบอกเมธอดที่เซิร์ฟเวอร์เข้าใจโดยใช้เฮดเดอร์ Public และ Allow ไคลเอนท์อาจจะส่งแมสเสจร้องขอเพื่อขอทราบเมธอดที่เซิร์ฟเวอร์สนับสนุนโดยใช้วเลือกที่เฮดเดอร์ (header option)

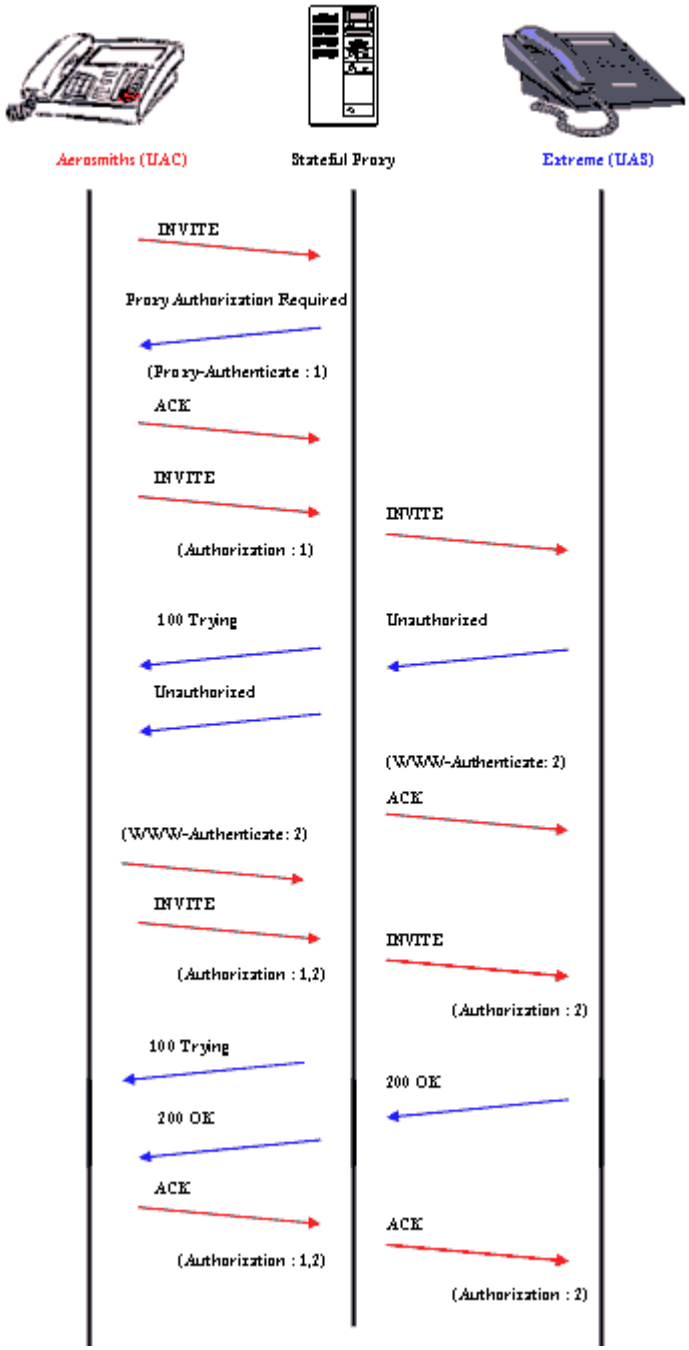
• เฮดเดอร์ เมื่อเอนทิตี้ได้รับเฮดเดอร์ที่ไม่เข้าใจ ก็จะละทิ้งเฮดเดอร์นั้น ในกรณีที่ไคลเอนท์จำเป็นต้องการใช้เฮดเดอร์บางเฮดเดอร์ ไคลเอนท์จะส่งแมสเสจเพื่อร้องขอเฮดเดอร์ที่จำเป็นต้องใช้

ไปโดยระบุในเฮดเดอร์ Require หากมีเฮดเดอร์ที่เซิร์ฟเวอร์ไม่สามารถให้การสนับสนุนได้เซิร์ฟเวอร์จะตอบปฏิเสธกลับมา

• status code ได้แบ่งเป็นคลาสต่างๆ เช่นเดียวกับ response code ของโปรโตคอล HTTP ซึ่งไคลเอนท์ต้องเข้าใจในความหมายในแต่ละคลาสเพื่อที่จะได้ทราบผลของการร้องขอว่าสำเร็จหรือไม่ สำหรับ status code ในแมสเสจตอบจะมีข้อความต่อหลังซึ่งจะเป็นความหมายของ code ซึ่งสามารถอ่านเข้าใจได้ โดยถ้าไคลเอนท์ไม่เข้าใจในรายละเอียดของ code ทั้งหมด ไคลเอนท์จะตีความหมายเป็น X00 เมื่อ X เป็นตัวเลขตัวแรกของ status code และนอกจากนั้นอาจจะนำ PEP (protocol extension protocol) มาปรับปรุงใช้งานกับ SIP ได้ ในกรณีมีการส่งแมสเสจผ่านหลายเซิร์ฟเวอร์ จะใช้เฮดเดอร์ Via เพื่อระบุเซิร์ฟเวอร์ที่เป็นทางผ่านของแมสเสจทั้งหมด สำหรับใช้ในการส่งแมสเสจตอบสนองกลับไปให้ผู้เรียก ในระหว่างการส่งแมสเสจร้องขอและแมสเสจตอบสนองจะมีการตกลงเกี่ยวกับพารามิเตอร์ของเซสชันด้วย ซึ่งรายละเอียดจะอยู่ในส่วนของ message body เช่นในกรณีของการสื่อสารโดยใช้เสียง พารามิเตอร์จะเป็น IP แอดเดรส พอร์ตสำหรับ RTP และการเข้า/ถอดรหัสเสียง หลังการสร้าง การเรียก เสร็จสมบูรณ์ ช่องสัญญาณสำหรับ RTP จะถูกสร้างขึ้นทำให้ทั้งสองฝ่ายสามารถสื่อสารกันได้ รวมทั้งยังอาจจะเชิญผู้อื่นมาเข้าร่วมในเซสชันนี้ได้ ในกรณีที่ต้องการเปลี่ยนพารามิเตอร์ของเซสชัน สามารถทำได้โดยส่งแมสเสจร้องขอใหม่อีกครั้งโดยใช้เมธอด Invite ซึ่งมี call-id เดิม ไปยังผู้ร่วมเซสชันพร้อมทั้งค่าพารามิเตอร์ของเซสชันใหม่ที่ต้องการใช้ รายละเอียดในส่วนนี้จะอยู่ในส่วนของ message body ซึ่งโดยทั่วไปจะใช้โปรโตคอล SDP ในการอธิบายความหมาย

2.3.1.11 การตรวจสอบสิทธิ์ผู้ใช้

รูปแบบในการตรวจสอบสิทธิ์ของผู้ใช้ (Authentication) ในโครงข่าย SIP มี 2 แบบหลัก ๆ คือการตรวจสอบสิทธิ์ SUA โดย Proxy Server, Redirect Server หรือ Registration Server และการตรวจสอบโดย SUA ตัวอื่น ปกติแล้วพร็อกซีหรือ Redirect Server ต้องการการตรวจสอบสิทธิ์ SUA เพื่ออนุญาตให้เข้าใช้การบริการ ยกตัวอย่าง Proxy Server อาจจะต้องการการตรวจสอบสิทธิ์ของ SUA ก่อนส่งต่อข่าวสาร INVITE ไปยังเกตเวย์หรือ Registration Server อาจจะต้องการการตรวจสอบสิทธิ์เพื่อป้องกันการเรียกของผู้บุกรุก อย่างไรก็ตาม SUA สามารถตรวจสอบสิทธิ์ซึ่งกันและกันเพื่อตรวจสอบว่ากำลังสนทนากับใคร



รูปที่ 2.3.4 ภาพแสดงตัวอย่างการโต้ตอบข่าวสารการเรียกที่เกี่ยวข้องกับทั้งพร็อกซีและการตรวจสอบสิทธิ์ SUA

2.3.2. Real Time Protocal

1.ใช้ในการส่งผ่านข้อมูลผ่าน เครือข่ายสำหรับการส่งข้อมูลพวกใช้เวลาจริง เช่น วีดีโอ

2.สามารถใช้งานร่วมกับโปรแกรมประยุกต์โครงข่ายมัลติมีเดียอื่นได้

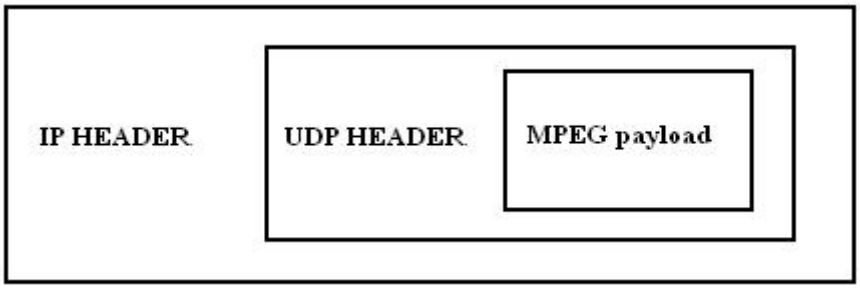
3.อาร์ทีพีไม่เป็นแบบ Connection-Oriented

4.ไม่มีความผิดพลาดในการเรียงข้อมูล ซึ่งแตกต่างจากโปรโตคอล ยูดีพี เมื่อส่งแล้วมีปัญหาในการลำดับก่อนหลัง

5.ข้อมูลที่จะส่งถูกควบคุมด้วย RTCP :Real Time Control Protocal

6.RTP ไม่มีการรับประกันคุณภาพของการส่งข้อมูลที่ หมายความว่าไม่มีกลไกใดๆยืนยันว่าการส่งสำเร็จหรือไม่

2.3.2.1 สถาปัตยกรรมของ RTP



รูปที่ 2.3.5 แสดงลักษณะการส่งข้อมูล

รูปที่ 2.3.6 แสดงตำแหน่งของ RTP ใน แพ็คเก็ต

รูปที่ 2.3.7 แสดง RTP packet header

ซึ่งภายใน RTP packet header นั้นจะประกอบด้วยส่วนต่างๆดังนี้

-Payload Type จะเป็นตัวบอกรูปแบบการเข้ารหัสทาง วีดีทัศน์ ดังตารางที่แสดงดังนี้

ตารางที่ 1 แสดง Payload Type Number กับ Video Formate

Payload Type Number	Video Formate
26	Motion JPEG
31	H.261
32	MPEG 1 Video
33	MPEG 2 Video

-Sequence Number

-Timestamp ทำให้สามารถนำมาจัดเรียงข้อมูลได้อย่างถูกต้อง

-Synchronization Soucre Identifer (SSRC)

2.3.2.2 RTP Control Protocol

แพ็คเก็ต RTP จะถูกส่งออกไปเป็นช่วงๆ เพื่อเก็บข้อมูลรายงานทางสถิติของ ทางฝ่ายส่งและฝ่ายรับเพื่อการนำไปใช้ประโยชน์ ซึ่งสถิตินี้ประกอบไปด้วย จำนวนของแพ็คเก็ตที่ส่งออกไปและจำนวนของแพ็คเก็ตที่สูญเสีย รายงานการรับนี้ประกอบไปด้วย

-SSRC (Synchronization Soucre Identifer)ของสตรีม RTP ที่รายงานเกี่ยวกับแหล่งกำเนิด

-เศษส่วนของแพ็คเก็ตที่สูญเสียในสายข้อมูล RTP นี้