การพัฒนา SIP server ให้รองรับการใช้งาน VoIP บนโทรศัพท์เคลื่อนที่

DEVELOPMENT OF SIP SERVER FOR VOIP WITH MOBILE SERVICE

โดย

นายกฤตภาส วารี 47010909

นางสาวหทัยชนก หลงสมบุญ 47010915

อาจารย์ที่ปรึกษา

ผศ.ดร. พิเชฐ ม่วงนวล

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2550

ปริญญานิพนธ์ปีการศึกษา 2550

ภาควิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง การพัฒนา SIP server ให้รองรับการใช้งาน VoIP บนโทรศัพท์เคลื่อนที่

DEVELOPMENT OF SIP SERVER FOR VOIP WITH MOBILE SERVICE

ผู้จัดทำ

1. นายกฤตภาส วารี

2. นางสาวหทัยชนก หลงสมบุญ

..... อาจารย์ที่ปรึกษา

(ผศ.ดร. พิเชฐ ม่วงนวล)

การพัฒนา SIP server ให้รองรับการใช้งาน VoIP บนโทรศัพท์เคลื่อนที่

DEVELOPMENT OF SIP SERVER FOR VOIP WITH MOBILE SERVICE

โดย นายกฤตภาส วารี 47010909

นางสาวหทัยชนก หลงสมบุญ47010915

อาจารย์ที่ปรึกษา ผศ.ดร. พิเชฐ ม่วงนวล

บทคัดย่อ

โครงงานนี้เป็นการศึกษาและพัฒนา SIP Server ให้รองรับการใช้งานโทรศัพท์ผ่านอินเตอร์เน็ต หรือ VoIP หลักการทำงานของ server เมื่อผู้ใช้ต้องการโทรออก จะส่งหมายเลขโทรศัพท์ของตนไปยัง Server ผ่าน GPRS เมื่อ Server ได้รับจะทำการโทรกลับมายังหมายเลขผู้ใช้งาน และให้สัญญาณกดหมายเลขโทรออก ซึ่งการใช้งาน VoIP บนมือถือในรูปแบบนี้มีข้อดีคือ ไม่จำเป็นต้องเชื่อมต่อ GPRS ตลอดเวลาที่มีการสนทนา จึงลดการล่าช้าของเสียง สัญญาณที่ได้มีคุณภาพดี และประหยัดค่าใช้จ่ายในการใช้งาน

ABSTRACT

This thesis is studied and developed the SIP server in order to support mobile phone using VoIP service. Designs concept of the SIP server, GPRS mobile phone connects to SIP server to report originate number. Server will call back to originate number and give dial tone, user can push the destination number. The advantaged of this system is short time of connect GPRS phone, reduce delay, good voice quality and save service charge.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้ ด้วยความกรุณาของผู้ช่วยศาสตราจารย์ ดร. พิเชฐ ม่วงนวล อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งได้ให้คำแนะนำ ข้อชี้แนะ และความช่วยเหลือในหลายสิ่งหลายอย่างจนกระทั่งลุล่วงไปได้ด้วยดี ผู้จัดทำวิทยานิพนธ์ขอกราบขอบพระคุณเป็นอย่างสูงมา ณ ที่นี้ และขอบคุณอาจารย์ประจำห้องสอบโปรเจ็ค โดยเฉพาะอาจารย์ต้น ที่ช่วยแนะนำ และตกเตือนข้อผิดพลาด จนทำให้วิทยานิพนธ์เล่มนี้สำเร็จขึ้นมา

ขอบคุณพี่ๆที่บริษัท SIPphone ที่ให้แรงบัลดาลใจในการทำวิทยานิพนธ์ชิ้นนี้ ขอขอบคุณ พี่พงษ์ พี่เอ้ และพี่จิว ที่ช่วยอธิบาย และช่วยให้โครงงานนี้สำเร็จขึ้นมา ขอขอบคุณพี่อาร์ต ที่ให้สถานที่ในการทำงาน และขอบใจ พี่ เพื่อน น้องภาควิชาโทรคมนาคมทุกคน ที่คอยถามไถ่ด้วยความด้วยความห่วงใย ว่าจะสำเร็จการศึกษาหรือไม่ และสุดท้าย ขอขอบคุณ คุณพ่อ คุณแม่ ที่ให้กำเนิด ทำให้ผู้ทำวิทยานิพนธ์ได้ประสบความสำเร็จมาจนถึงทุกวันนี้ รวมถึงผู้มีพระคุณทุกท่านที่มิได้เอ่ยนามไว้ ณ ที่นี้

กฤตภาส วารี

หทัยชนก หลงสมบุญ

สารบัญ

สารบัญ (ต่อ)

สารบัญรูปภาพ

สารบัญรูปภาพ (ต่อ)

สารบัญตาราง

บทที่1

บทนำ

1.1 ที่มาและความสำคัญ

เนื่องด้วยในปัจจุบันโทรศัพท์เคลื่อนที่ได้เข้ามามีบทบาทในชีวิตประจำวันของเรามากขึ้น ดังจะเห็นได้จากวิวัฒนาการของโทรศัพท์เคลื่อนที่ ที่ได้มีการพัฒนาไปมาก จากอดีตที่มีการทำงานด้วยระบบอนาล็อก (Analog) มาสู่ยุคปัจจุบันที่ทำงานด้วยระบบดิจิตอล (digital) หรือยุคของ 3จี (3G) จึงทำให้โทรศัพท์เคลื่อนที่ไม่ได้เป็นเพียงแค่อุปกรณ์สำหรับการสื่อสารด้วยเสียงเพียงอย่างเดียวเท่านั้น แต่ยังสามารถใช้การสื่อสารด้วยภาพเพิ่มเติมเข้าไปด้วย ช่วยให้เราสามารถสื่อสาร และทำความเข้าใจ กับคู่สนทนาของเรา ได้ดียิ่งขึ้น ในส่วนของเทคโนโลยีการสื่อสารบนโทรศัพท์เคลื่อนที่นั้น ได้มีการพัฒนาอยู่ตลอดเวลา ไม่ว่าจะเป็นอินฟาเรด (Infrared) บลูทูธ (Bluetooth) จีพีอาร์เอส (GPRS: General Package Radio Service) และเอดจ์ (EDGE: Enhanced Data Rates for Global Evolution) ทำให้ช่องทางการในการติดต่อสื่อสารมีมากขึ้น

ระบบจีพีอาร์เอสเป็นช่องทางการติดต่อสื่อสารที่กำลังได้รับความนิยมเพิ่มขึ้นในปัจจุบัน โดยมีความสามารถในการรับส่งข้อมูลได้ทั้งภาพและเสียงในระยะไกลผ่านเครือข่ายโทรศัพท์เคลื่อนที่ มีความเร็วในการส่งข้อมูลอยู่ที่ 14 กิโลบิตต่อวินาที และความเร็วในการรับข้อมูลอยู่ที่ 28 – 64 กิโลบิตต่อวินาที ทำให้มีการตอบสนองที่เป็นไปอย่างรวดเร็วทันต่อความต้องการของผู้ใช้งาน ทั้งในเรื่องค่าใช้จ่ายที่มีการคิดค่าใช้จ่ายตามปริมาณข้อมูลที่รับส่งจริงเป็นกิโลไบต์ (Kilobyte) หรือตามเวลาของการเชื่อมต่อเป็นวินาที ซึ่งเมื่อเปรียบเทียบกับค่าใช้จ่ายในการโทรศัพท์ปัจจุบันจะเห็นว่ามีค่าใช้จ่ายที่ถูกกว่าและยังไม่มีการเอาเปรียบผู้ใช้งานอีกด้วย

ดังนั้น จึงมีการนำระบบจีพีอาร์เอสมาใช้ในการติดต่อสื่อสารแบบ Voice over IP (VoIP) ซึ่งมีพื้นฐานอยู่บนการใช้ช่องทางการติดต่อสื่อสารแบบ Packet Switched Data และยังมีการผลิตโทรศัพท์มือถือ ที่ใช้ VoIP ในการติดต่อสื่อสารโดยเฉพาะ โดยโทรศัพท์ต้องอยู่ในพื้นที่ที่มีสัญญาณ WiFi อยู่ตลอดเวลา แต่อย่างไรก็ตาม ความต้องการระดับพื้นฐานของ VoIP คือคุณภาพของการให้บริการ (QOS) ต้องเทียบเท่าคุณภาพในระบบโทรศัพท์หรือดีกว่าซึ่งเป็นปัญหาสำหรับการใช้งานในทางปฏิบัติ ที่ยังมีความล่าช้าของสัญญาณเสียง (Delay) อยู่มาก เนื่องจาก VoIP เป็นการสื่อสารแบบพหุสื่อ ต้องการคุณสมบัติแบบเวลาจริง (Real Time)

จากเหตุผลข้างต้นและแนวทางในการทำ VoIP ทางคณะผู้จัดทำ จึงมีความคิดที่จะพัฒนาการติดต่อสื่อสารด้วยเสียงของโทรศัพท์เคลื่อนที่ ผ่านตัวกลางที่เรียกว่า Sip Server ซึ่งการติดต่อสื่อสารทางฝั่ง Server นั้นจะใช้ตู้สาขาโทรศัพท์แบบ IP-PBX ที่เป็น Software คอยจัดการให้ ซึ่งวิธีนี้จะช่วยในการประหยัดค่าโทรศัพท์ของผู้ใช้งานอย่างมาก โดยเฉพาะเมื่อมีการโทรออกไปยังต่างประเทศ

1.2 วัตถุประสงค์

1. เพื่อศึกษาการติดต่อสื่อสารแบบ VoIP
2. เพื่อศึกษาการใช้โปรแกรมควบคุมตู้สาขาโทรศัพท์แบบ IP-PBX
3. เพื่อเป็นการประหยัดค่าโทรศัพท์ของผู้ใช้งานในการโทรออก

1.3 ผลที่คาดว่าจะได้รับ

1. ได้รับความรู้ ความเข้าใจเกี่ยวกับการใช้โปรแกรมควบคุมตู้สาขาโทรศัพท์แบบ IP-PBX
2. ได้รับความรู้ ความเข้าใจเกี่ยวกับระบบการทำงานของ VoIP

บทที่ 2

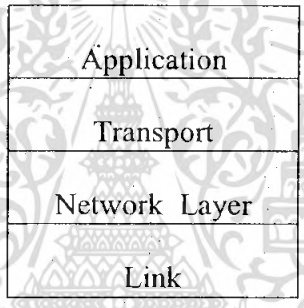
ทฤษฎีและหลักการ

2.1 TCP/IP

TCP/IP (Transmitsion Control Protocol/InternetProtocol) เป็นชุดของโปรโตคอลที่ถูกใช้ในการสื่อสารผ่านเครือข่ายอินเทอร์เน็ต ได้รับการพัฒนามาตั้งแต่ปี 1960 ซึ่งถูกใช้เป็นครั้งแรกในเครือข่าย ARPANET ซึ่งต่อมาได้ขยายการเชื่อมต่อไปทั่วโลกเป็นเครือข่ายอินเตอร์เน็ต ทำให้ TCP/IP เป็นที่ยอมรับอย่างกว้างขวางจนถึงปัจจุบัน

2.1.1การแบ่งชั้นของ TCP/IP

TCP/IP แบ่งออกเป็น 4 เลเยอร์ ดังรูปที่ 2.1



รูปที่ 2.1 การแบ่งชั้นของ TCP/IP

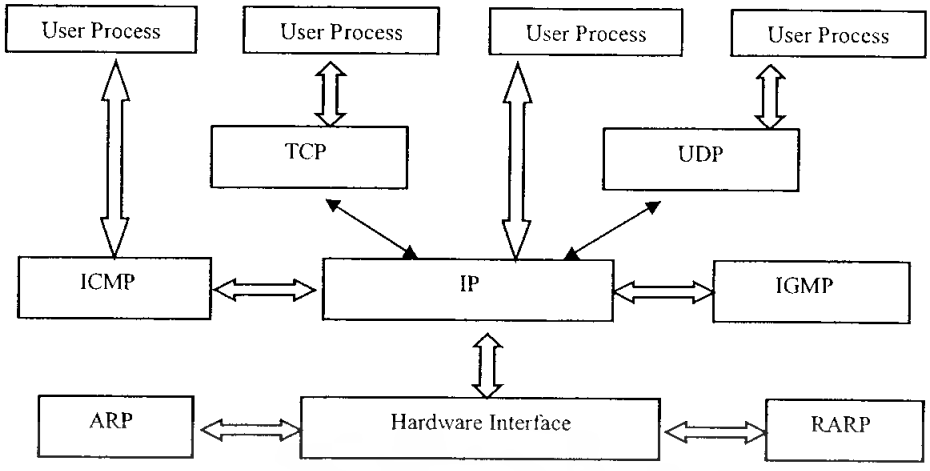
ในแต่ละเลเยอร์จะมีหน้าที่ดังนี้

1. **Link Layer** - เลเยอร์นี้มีหน้าที่ควบคุมการรับส่งข้อมูลในระดับฮาร์ดแวร์ของเครือข่าย รับผิดชอบการรับส่งข้อมูลในระดับกายภาพ จนถึงการแปลความจากสัญญาณไฟฟ้าเป็นข้อมูลทางคอมพิวเตอร์
2. **Network Layer** - ทำหน้าที่รับข้อมูลจากชั้น Transport Layer และค้นหาและเลือกเส้นทาง ระหว่างผู้รับและผู้ส่ง เทียบได้กับ Network Layer ของ OSI Model โปรโตคอลในเลเยอร์นี้ได้แก่ IP,ICMP,IGMP
3. **Transport Layer** - รับผิดชอบการรับส่งข้อมูลระหว่างปลายด้านส่งและด้านรับข้อมูล และส่งข้อมูลขึ้นไปให้ Application Layer นำไปใช้งาน ต่อ เทียบได้กับ Session Layer และ Transport Layer ของ OSI Model
4. **Application Layer** - เป็นเลเยอร์ที่แอพพลิเคชั่นเรียกโปรโตคอลระดับล่างๆลงไป เพื่อให้บริการต่างๆ เช่น FTP , SMTP , Telnet , HTTP , POP

2.1.2 โครงสร้างของโปรโตคอล TCP/IP

เนื่องจาก TCP/IP เป็นชุดของโปรโตคอลประกอบด้วยโปรโตคอลหลายตัวทำงานร่วมกันในเลเยอร์ต่างๆ และมีหน้าที่แตกต่างกันออกไป ได้แก่

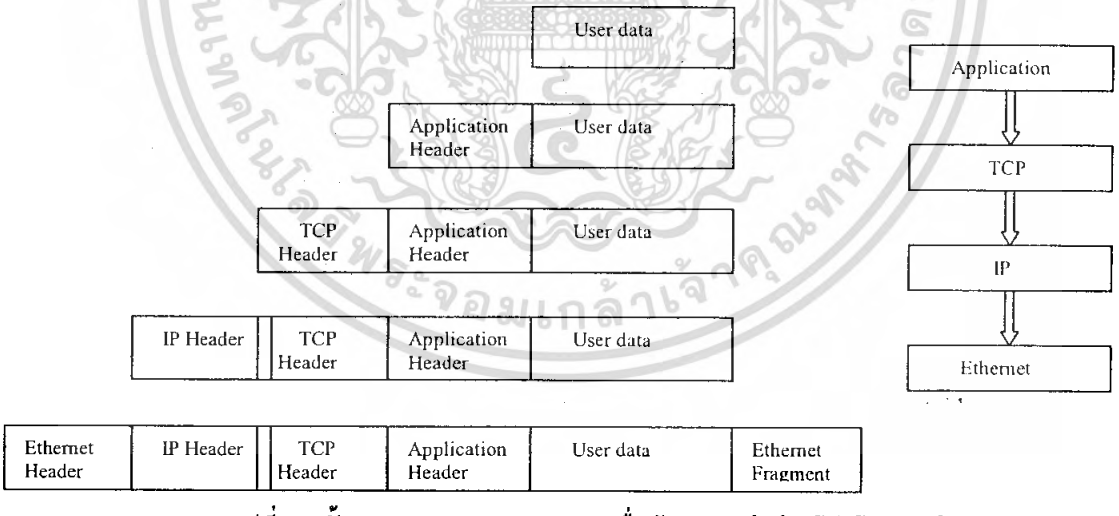
- **TCP : (Tranmission Control Protocol)** - อยู่ใน Transport Layer ทำหน้าที่จัดการและควบคุมการรับส่งข้อมูล และมีกลไกความคุมการ รับส่งข้อมูลให้มีความถูกต้อง (reliable) และมีการสื่อสารอย่างเป็นกระบวนการ (connection-orient)
- **UDP : (User Datagram Protocol)** - อยู่ใน Transport Layer ทำหน้าที่จัดการและควบคุมการรับส่งข้อมูลแต่ไม่มีกลไกความคุมการรับส่งข้อมูลให้มีเสถียรภาพและเชื่อถือได้(unreliable,connectionless) โดยปล่อยให้เป็นหน้าที่ของแอพพลิเคชั่นเลเยอร์ แต่ UDP มีข้อได้เปรียบในการส่งข้อมูลได้ทั้งแบบ unicast, multicast และ broadcast อีกทั้งยังทำการติดต่อสื่อสารได้เร็วกว่า TCP เนื่องจาก TCP ต้องเสีย overhead ให้กับขั้นตอนการสื่อสารที่ทำให้ TCP มีความน่าเชื่อถือในการรับส่งข้อมูลนั่นเอง
- **IP : (Internet Protocol)** - อยู่ใน Internetwork Layer เป็นโปรตคอลหลักในการสื่อสารข้อมูล มีหน้าที่ค้นหาเส้นทางระว่างผู้รับและผู้ส่ง โดยใช้ IP Address ซึ่งมีลักษณะเป็นเลขสี่ชุด แต่ละชุดมีค่าตั้งแต่ 0-255 เช่น 172.17.3.12 ในการอ้างอิงโฮสต์ต่างๆ และกลไกการ Route เพื่อส่งต่อข้อมูลไปจนถึงจุดหมายปลายทาง
- **ICMP : (Internet Control Message Protocol)** - อยู่ใน Internetwork Layer มีหน้าที่ส่งข่าวสารและแจ้งข้อผิดพลาดให้แก่ IP
- **IGMP : (Internet Group Management Protocol)** อยู่ในเน็ตเวิร์กเลเยอร์ ทำหน้าที่ในการส่ง UDP ดาต้าแกรมไปยัง กลุ่มของโฮสต์ หรือ โฮสต์หลายๆตัวพร้อมกัน
- **ARP : (Address Resolution Protocol)** - อยู่ใน Link Layer ทำหน้าที่เปลี่ยนระหว่าง IP แอดเดรส ให้เป็นแอดเดรสของ Network Interface เรียกว่า MAC Address ในการติดต่อระหว่างกัน MAC Address คือหมายเลขประจำของ Hardware Interface ซึ่งในโลกนี้จะไม่มี MAC Address ที่ซ้ำกัน มีลักษณะเป็นเลขฐาน 16 ยาว 6 ไบต์ เช่น 23:43:45:AF:3D:78 โดย 3 ไบต์แรกจะเป็นรหัสของผู้ผลิต และ 3 ไบต์หลังจะเป็นรหัสของผลิตภัณฑ์
- **RARP : (Reverse ARP)** - อยู่ในลิงค์เลเยอร์เช่นกัน แต่ทำหน้าที่กลับกันกับ ARP คือเปลี่ยนระหว่างแอดเดรสของ Network Interface ให้ เป็นแอดเดรสที่ใช้โดย IP Address



รูปที่ 2.2 แสดงให้เห็นถึงความสัมพันธ์ระหว่างโปรโตคอลต่างๆใน TCP/IP

2.1.3 Encapsulation/Demultiplexing

เวลาส่งข้อมูล เมื่อข้อมูลถูกส่งผ่านในแต่ละเลเยอร์ แต่ละเลเยอร์จะทำการประกอบข้อมูลที่ได้รับมา กับส่วนควบคุมซึ่งอยู่ส่วนหัวของข้อมูลเรียกว่า Header ภายใน Header จะบรรจุข้อมูลที่สำคัญของโปรโตคอลที่ทำการ Encapsulate เมื่อผู้รับ ได้รับข้อมูล ก็จะเกิดกระบวนการทำงานย้อนกลับคือโปรโตคอลเดียวกัน ทางฝั่งผู้รับก็จะได้รับข้อมูลส่วนที่เป็น Header ก่อนและนำไปประมวลและทราบว่าข้อมูลที่ตามมามีลักษณะอย่างไร ซึ่งกระบวนการย้อนกลับนี้เรียกว่า Demultiplexing



รูปที่ 2.3 ขั้นตอนการ encapsulation เมื่อข้อมูลถูกส่งผ่านโปรโตคอลต่างๆ

ข้อมูลที่ผ่านการ Encapsulate ในแต่ละระดับมีชื่อเรียกแตกต่างกันข้อมูลที่มาจาก User หรือก็คือข้อมูลที่ User เป็นผู้ป้อนให้กับ Application เรียกว่า **User Data** เมื่อ Application ได้รับข้อมูลจาก user ก็จะนำมาประกอบกับส่วนหัวของ Appliction เรียกว่า Application Data และส่งต่อไปยังโปรโตคอล TCP เมื่อโปรโตคอล TCP ได้รับ Application Data ก็จะนำมารวมกับ Header ของ โปรโตคอล TCP เรียกว่า **TCP Segment**และส่งต่อไปยังโปรโตคอล IP เมื่อโปรโตคอล IP ได้รับ TCP Segment ก็จะนำมารวมกับ Header

ของ โปรโตคอล IP เรียกว่า **IP Datagram**และส่งต่อไปยังเลเยอร์ Datalink Layer ในระดับ Datalink จะนำ IP Datagram มาเพิ่มส่วน Error Correction และ flag เรียกว่า Ethernet Frame ก่อนจะแปลงข้อมูลเป็นสัญญาณไฟฟ้า ส่งผ่านสายสัญญาณที่เชื่อมโยงอยู่ต่อไป

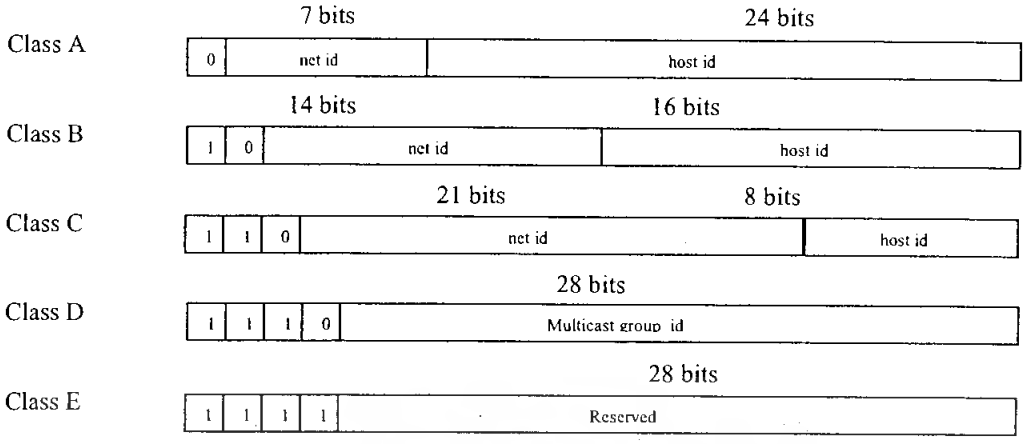
2.1.4 Internet Protocol

IP เป็นโปรโตคอลที่ทำหน้าที่รับภาระในการนำข้อมูลไปส่งยังผู้รับ ที่เชื่อมต่ออยู่ในระบบ network ซึ่งทั้งสองฝั่งอาจอยู่คนละเน็ตเวิร์คกันก็ได้ โปรโตคอลอื่นๆ ในระดับ network Layer ขึ้นไปทั้ง TCP, UDP ,ICMP ต่างก็ต้องอาศัยโปรโตคอล IP ในการรับส่งข้อมูลทั้งสิ้น

โปรโตคอล IP มีความสามารถในการค้นหาเส้นทางจากผู้รับไปยังผู้ส่ง มีกลไกที่ชาญฉลาดในการค้นหาเส้นทาง สามารถค้นหาเส้นทางได้ไปถึงผู้รับได้เอง หากมีเส้นทางที่สามารถไปได้ แต่ไม่ได้ติดต่อระหว่างผู้รับกับผู้ส่งโดยตรง และไม่มีการยืนยันว่า ข้อมูลถึงผู้รับจริงหรือไม่ ทั้งนี้อาจเกิดจากหลายสาเหตุ เช่น ที่อยู่ของผู้รับไม่มีการเชื่อมต่ออยู่ในระบบ Internet กล่าวได้ว่า โปรโตคอล IP มีหน้าที่ในการค้นหาเส้นทางเท่านั้น ไม่มีการยืนยันผลสำเร็จในการส่งข้อมูล หากเกิดข้อผิดพลาดในการส่งข้อมูล แม้ว่าจะมีการส่ง icmp massage กลับมารายงานข้อผิดพลาด แต่ก็รับประกันไม่ได้อยู่ดีว่า icmp message จะกลับมาถึงเรียบร้อยหรือไม่ ด้วยเหตุนี้ จึงถือว่า IP เป็นโปรโตคอลที่ไม่มีความน่าเชื่อถือ (reliable)

ทุกอินเตอร์เฟซที่ต่ออยู่บนอินเตอร์เน็ตจะต้องมีหมายเลขประจำตัวเพื่อใช้ในการสื่อสารข้อมูล เรียกว่า Internet Address หรือเรียกย่อๆว่า IP Address โดยค่า IP Address นี้จะเป็นหมายเลขจำนวน 32 บิต แต่แทนที่จะกำหนดให้เลขทั้ง 32 บิตนั้นถูกนับต่อเนื่องกันไป ก็จะใช้วิธีการแบ่งหมายเลขดังกล่าวออกเป็นกลุ่มของเลขขนาด 8 บิตจำนวน 4 ชุด และคั่นแต่ละชุดด้วยจุด ตัวอย่างเช่น 172.17.3.12 นอกจากนี้ใน IP Address นั้นยังถูกแบ่งออกเป็น 2 ส่วนคือ ส่วนที่ เป็นแอดเดรสของเน็ตเวิร์ก (Network ID) และส่วนที่เป็นแอดเดรสของโฮสต์ (Host ID) ซึ่งข้อมูลในส่วนนี้จะถูกใช้สำหรับ ค้นหาเส้นทางของ IP ในการที่จะขนส่งข้อมูลจากต้นทางให้ถึงปลายทางอย่างถูกต้อง เพื่อเป็นการกำหนดขนาดของเน็ตเวิร์กสำหรับ IP Address ต่างๆดังนั้นจึงมีการจัด IP Address ในแต่ละช่วงออกเป็นคลาส (class) ต่างๆกันจาก A ถึง E เพื่อจะได้ทำการจัดสรร IP Address ได้อย่างเหมาะสมกับขนาดของเน็ตเวิร์ก

จากข้อกำหนดในการแบ่งคลาสของ IP Address หากลองนำบิตที่อยู่ในดอนต้นของ IP address ในแต่ละคลาสมาแปลงเป็น IP address ในเลขฐานสิบ จะเห็นว่าแต่ละคลาสครอบคลุม IP address ช่วงต่างๆ ดังตารางที่ 2.1

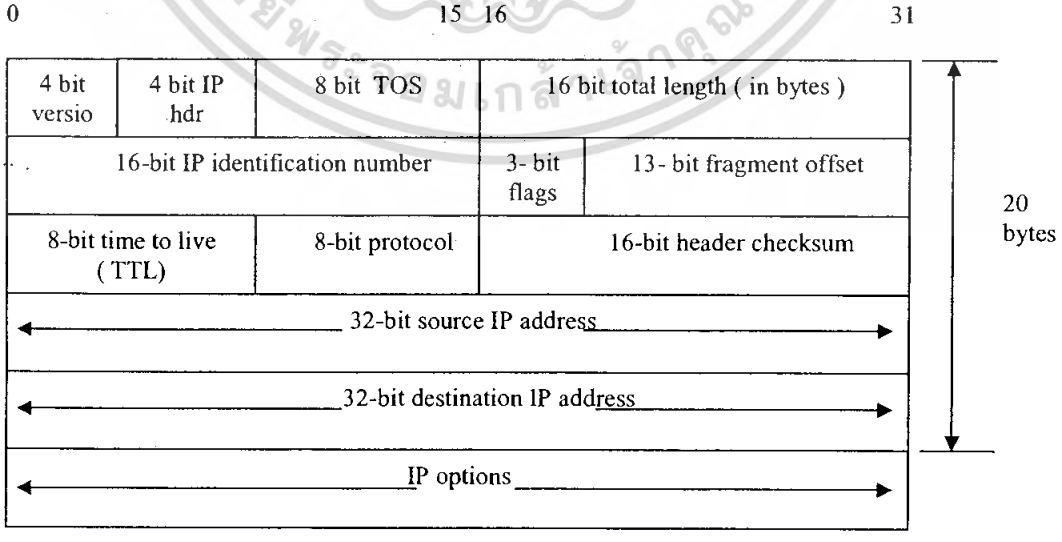


รูปที่ 2.4 การกำหนด IP Address ในคลาสต่างๆ

ตารางที่ 2.1 แสดงช่วงของ IP Adress ในแต่ละคลาส

Class	IP Range
A	0.0.0.0 - 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255
D	224.0.0.0 - 239.255.255.255
E	240.0.0.0 - 255.255.255.255

เมื่อข้อมูลถูกส่งลงมาจากชั้น Transport Layer สู่ชั้นNetwork Layer กระบวนการ Encapsulate ของ IP Protocol จะทำการเพิ่มส่วน Header ลงไป Header ของ IP datagram มีขนาด 20-32 ไบต์ มีส่วนประกอบต่างๆ ดังแสดงในรูปที่ 2.5



รูปที่ 2.5 IP Header

ตารางที่ 2.2 IP Header

<table>
<tr><th>ตำแหน่ง</th><th>ชื่อ</th><th>อธิบาย</th></tr>
<tr><td>0-3</td><td>Version</td><td>มีขนาด 4 บิตเป็นเวอร์ชั่นของ IP ปัจจุบันค่านี้ถูกกำหนดให้เป็น 4</td></tr>
<tr><td>4-7</td><td>Length</td><td>มีขนาด 4 บิตเป็นค่าความยาวของ Header นี้ โดยปกติจะเป็น 5 หมายความว่า 5*32 บิต = 20 ไบต์</td></tr>
<tr><td>8-15</td><td>Type of Service</td><td>เป็นข้อมูลขนาด 8 บิต ปัจจุบันไม่ได้ใช้งานแล้ว</td></tr>
<tr><td>16-31</td><td>Total length</td><td>เป็นฟิลด์ที่บอกจำนวนไบต์ทั้งหมดของ IP Datagram ด้วยขนาด 16 บิตทำให้ Datagram มีขนาดสูงสุดไม่เกิน 65535 ไบต์ และมีขนาดเล็กสุดไม่ต่ำกว่า 512 ไบต์</td></tr>
<tr><td>32-47</td><td>Identification</td><td>ใช้ในกรณีที่มีการแบ่งดาต้าแกรมออกเป็นแฟรกเมนต์ เมื่อนำกลับมารวมกันใหม่จะได้รู้ว่ามาจากดาต้าแกรมเดียวกัน</td></tr>
<tr><td>48-50</td><td>Flag</td><td>ใช้ในกรณีที่มีการแบ่งข้อมูลออกเป็นแฟรกเมนต์ มีความหมายดังนี้
บิต 0 : reserved เป็น 0 เสมอ
บิต 1 (DF) 0 = May Fragment, 1 = Don't Fragment
บิต 2 (MF) 0 = Last Fragment, 1 = More Fragments.</td></tr>
<tr><td>51-63</td><td>fragment offset</td><td>เป็นส่วนระบุข้อมูลที่ใช้แยกรวมข้อมูล เพื่อให้ข้อมูลที่ถูกแยกออกเป็นแฟรกเมนต์กลับมารวมกันได้อย่างถูกต้องตามลำดับ</td></tr>
<tr><td>64-71</td><td>Time to Live (TTL)</td><td>เป็นจำนวนครั้งสูงสุดที่ดาต้าแกรมนี้จะถูกส่งผ่านเครือข่ายไปยังปลายทางได้ เพื่อ ป้องกันไม่ให้ดาต้าแกรมถูกเราต์ไปเรื่อยๆอย่างไม่สิ้นสุด ปกติค่านี้จะเริ่มต้นที่ 32 และจะถูกลดค่าลงทีละ 1 เมื่อมีการเราต์ จนค่านี้มีค่าเป็น 0 ก็จะไม่ถูกเราต์อีกต่อไป</td></tr>
<tr><td>72-79</td><td>Protocol</td><td>เป็นข้อมูลที่ระบุโปรโตคอลที่ส่งดาต้าแกรมนี้มา ตัวอย่างโปรโตคอลที่ใช้บ่อยๆ ได้แก่
<table>
<tr><th>โปรโตคอล</th><th>ค่าในฟิลด์</th><th>อธิบาย</th></tr>
<tr><td>ICMP</td><td>1</td><td>Internet Comtrol Message Protocol</td></tr>
<tr><td>TCP</td><td>6</td><td>Transmission Control Protocol</td></tr>
<tr><td>UDP</td><td>17</td><td>User Datagram Protocol</td></tr>
</table>
</td></tr>
<tr><td>80-95</td><td>Header Checksum</td><td>เป็นส่วนตรวจสอบความถูกต้องของข้อมลใน Header โดยไม่เกี่ยวกับส่วนข้อมูลที่อยู่ภายใน payload ค่านี้จะถูกคำนวนใหม่ทุกครั้งที่มีการเปลี่ยนแปลงข้อมูลใน Header</td></tr>
<tr><td>86-127</td><td>Source IP address</td><td>คือ IP Address ของผู้ส่งดาต้าแกรม</td></tr>
</table>

ตารางที่ 2.2 (ต่อ) IP Header

ตำแหน่ง	ชื่อ	อธิบาย
128-163	Destination IP Address	คือ IP Address ของผู้รับดาต้าแกรม
ไม่แน่นอน	Option	มีขนาดข้อมูลไม่แน่นอน ใช้สำหรับกำหนดค่าพารามิเตอร์ปลีกย่อย ซึ่งส่วนใหญ่ไม่มีการนำไปใช้งาน
ขึ้นอยู่กับ Option	Padding	มีข้อมูลว่างเปล่า ใช้เป็นส่วนเติมเต็มของฟิลด์ Option ให้ครบ 32 ไบต์

2.1.5 IP Routing

IP Routing เป็นกระบวนการค้นหาเส้นทางในการส่งผ่านข้อมูลจากต้นทางไปยังปลายทางโดยผ่านการส่งต่อข้อมูลไปจนกว่าจะถึงปลายทาง นับเป็นกลไกสำคัญที่ทำให้ IP เป็นโปรโตคอลที่สามารถส่งข้อมูลจากโฮสต์หนึ่งไปอีกโฮสต์หนึ่งได้แม้ว่าจะอยู่ไกล ส่วนประกอบต่างๆ ของเน็ตเวิร์ค ในแง่ของ IP Routing มีดังนี้

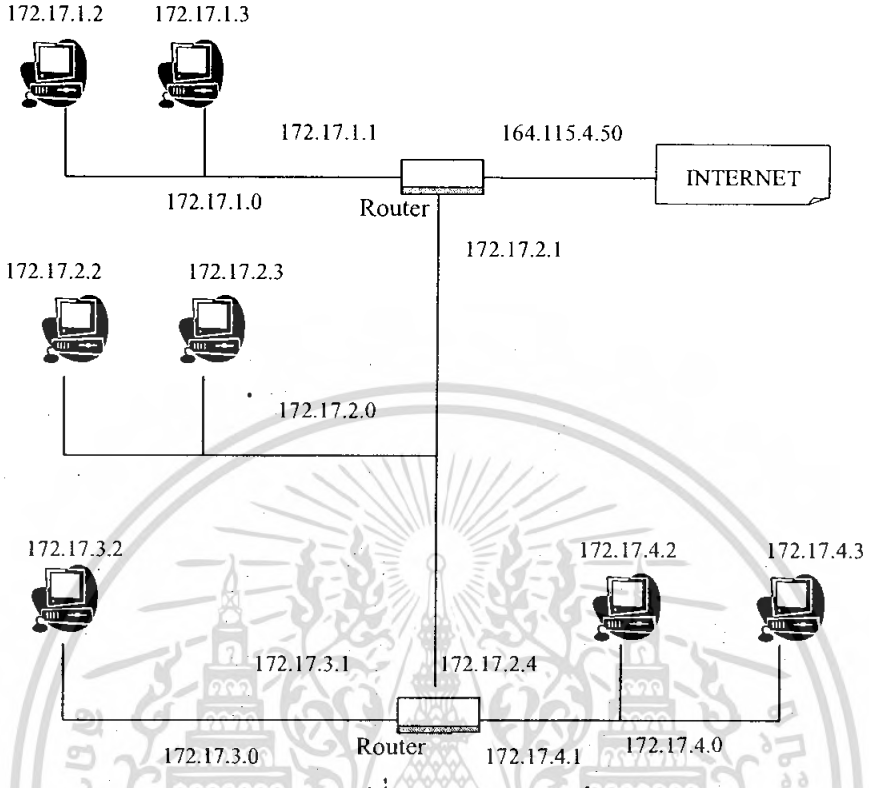
โฮสต์ (Host) เป็นอุปกรณ์ที่ทำหน้าที่ให้กำเนิดข้อมูลในกรณีเป็นผู้ส่ง หรือทำหน้าที่รับข้อมูลไปใช้งานในกรณีเป็นผู้รับ การสื่อสาร ข้อมูลใดๆจะต้องเป็นการสื่อสารจากโฮสต์ไปยังโฮสต์เสมอ สำหรับ IP Packet แล้วข้อมูลในเฮดเดอร์ที่ปรากฏอยู่ในฟิลด์ Source Address และ Destination Address ซึ่งเรียกว่า IP Address จะเป็นหมายเลขระบุตำแหน่งของโฮสต์ต้นทางและโฮสต์ ปลายทางเท่านั้น

เน็ตเวิร์ค (Network) เป็นเครือข่ายที่มีการเชื่อมต่อกันของโฮส 2 ตัวขึ้นไป โฮสต์แต่ละตัวในเน็ตเวิร์คเดียวกันสามารถเชื่อมต่อถึงกันได้โดยตรง

เราเตอร์ (Router) ทำหน้าที่ในการส่งผ่านข้อมูลจากเน็ตเวิร์กหนึ่งไปยังอีกเน็ตเวิร์กหนึ่งตำแหน่งของเราเตอร์จะอยู่ในจุดที่เชื่อมต่อระหว่างสองเน็ตเวิร์กเข้าด้วยกัน ด้วยข้อกำหนดของ IP ข้อมูลจะส่งไปถึงกันโดยตรงข้ามเน็ตเวิร์กไม่ได้ จะต้องอาศัยเราเตอร์เป็นผู้ทำหน้าที่ส่งผ่านข้อมูลไปให้ ใน Router จะมี Routing Table สำหรับเก็บข้อมูล เพื่อใช้ในการพิจารณาเลือกเส้นทางในการส่งดาต้าแกรม

การ Routing จะเป็นไปตามขั้นตอนดังนี้

1. ถ้าโฮสต์ต้นทางและปลายทางต่อเชื่อมร่วมอยู่ในเน็ตเวิร์กเดียวกัน มีการเชื่อมต่อถึงกันโดยตรง เช่น อีเธอร์เน็ตหรือโทเค็นริง ดังแสดงในภาพที่ 2.6 เป็นการติดต่อระหว่าง 172.17.2.2 และ 172.17.2.3 (เครื่องสีแดง) IP ดาต้าแกรมก็จะถูกส่งไปยังโฮสต์ปลายทางโดยตรง



รูปที่ 2.6 network ตัวอย่าง

2. หากโฮสต์ต้นทางและปลายทางไม่ได้อยู่ในเน็ตเวิร์กเดียวกัน IP ดาต้าแกรมจะถูกส่งไปยังดีฟอลต์เราเตอร์ 3. เมื่อเราเตอร์ได้รับ IP ดาต้าแกรมจากข้อ 2 แล้วตรวจสอบดู หากพบว่าโฮสต์ปลายทางต่อร่วมอยู่บนเน็ตเวิร์กเดียวกันกับเราเตอร์ ให้ทำการส่งดาต้าแกรมไปที่โฮสต์นั้น เช่น หาก 172.17.3.2 ต้องการส่งดาต้าแกรมไปยัง 172.17.4.2 (เครื่องสีเหลือง) จะต้องส่งดาต้าแกรมไปที่ Router B Router B จะส่งดาต้าแกรมต่อไปยังโฮสปลายทาง หากไม่ได้ต่อร่วมกันก็ส่งดาต้าแกรมไปที่เราเตอร์ตัวต่อไป โดย Router จะเป็นผู้เลือกเส้นทาง ซึ่งมีอยู่ 2 กรณีคือ

1. ถ้ามีข้อมูลของโฮสปลายทางอยู่ใน Routing Table Router จะส่งดาต้าแกรมไปยังเราเตอร์ตัวที่ระบุไว้ใน routing table
2. ถ้าไม่มีข้อมูลของโฮสปลายทางอยู่ใน Routing Table Router จะส่งดาต้าแกรมไปยัง default router

สมมติว่าเครื่อง 172.17.1.3 ต้องการติดต่อกับ 172.17.4.3 จะต้องส่ง ip datagram ไปยัง Router A หาก Router A มีข้อมูลเกี่ยวกับ 172.17.4.3 อยู่ ก็จะรู้ว่าต้องส่งดาต้าแกรมไปยัง Router B คือ 172.17.2.4 และ Router B ก็จะส่ง ip datagram ไปยังโฮสปลายทางได้สำเร็จ

2.1.6 Subnet Adressing / Subnet Mask

ในการใช้งาน โปรโตคอล TCP/IP ใน internet นั้นการแบ่ง IP Address ออกเป็นแอดเดรสของเน็ตเวิร์ก (net id) และแอดเดรสของ โฮสต์ ตามที่ระบุของแต่ละคลาสค่อนข้างจะขาดประสิทธิภาพ คือในเน็ตเวิร์กคลาส A และ B แต่ละเน็ตเวิร์กนั้น สามารถมีจำนวนโฮสต์ได้มาก ซึ่งการที่จะนำ IP Address มาใช้อย่างทั่วถึงนั้นมีโอกาสเป็นไปได้ยากมากทั้งคลาส A และคลาส B เพราะมีโอกาสน้อยมากที่จะมีเน็ตเวิร์ก ใดในโลกมีจำนวนโฮสต์มากมายขนาดนั้นอยู่ภายในเน็ตเวิร์กเดียว ดังนั้น IP Address ที่จัดสรรให้ไปในแต่ละเน็ตเวิร์กของ คลาสเหล่านี้จึงถูกใช้ไม่หมดและไม่สามารถนำไปใช้ประโยชน์ที่อื่นได้เลย ดังนั้นเพื่อให้การจัดสรร IP เป็นไปอย่างมีประสิทธิภาพ จึงมีการนำส่วนของ host id มาแบ่งย่อยเป็นสองส่วนคือ subnet id และ host id ทำให้ได้เน็ตเวิร์คย่อยหลายๆเน็ตเวิร์ค โดยในแต่ละเน็ตเวิร์ค มีจำนวนโฮสไม่มากเกินไปและเพียงพอต่อการใช้งาน

การแบ่ง Subnet ใช้เทคนิคที่เรียกว่า Subnet Mask ซึ่งเป็นตัวเลขมีความยาว 32 บิต แบ่งออกเป็นสี่ชุดเช่นเดียวกับ IP แต่ค่าของ subnet mask จะขึ้นอยู่กับความต้องการในการแบ่ง subnet ว่าต้องการจำนวน subnet เท่าใดและมีจำนวนโฮสเท่าใด หากนำ subnet mask มาเขียนเป็นเลขฐานสอง จะมีลักษณะพิเศษคือ ขึ้นต้นด้วยเลข 1 มีจำนวนกี่ตัวก็ได้ ตามแต่ความต้องการในการแบ่ง subnet และตำแหน่งที่เหลือจะมีค่าเป็น 0

2.1.7 Ethernet Address Resolution Protocol

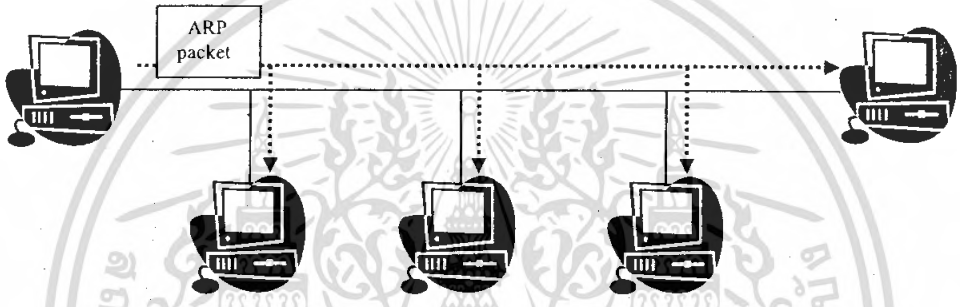
ในการสื่อสารใดๆ ก็ตาม จำเป็นต้องมีการสื่อสารผ่านตัวกลางในระดับ Physical เสมอ ซึ่งเป็นระดับล่างสุดในการสื่อสาร สำหรับในโปรโตคอล TCP/IP ถือว่าเป็นชั้น Link Layer นั่นเอง การสื่อสารในระดับนี้เป็นการสื่อสารระหว่าง Hardware Interface ในเน็ตเวิร์คเดียวกัน ซึ่งมองข้อมูลเป็น Ethernet Frame เท่านั้น จะไม่สนใจว่าข้อมูลภายในเป็นอย่างไร มีต้นทางอยู่ที่ไหนหรือปลายทางไปหาใคร แต่สิ่งที่โปรโตคอลในชั้นนี้สนใจก็คือ ข้อมูลที่ Network Layer ส่งมาให้นั้น จะต้องส่งไปยัง Hardware Interface ไหน ซึ่งการระบุ Hardware Interface จะใช้เป็น MAC Address มีลักษณะเป็นเลขฐาน 16 ยาว 6 ไบต์ เช่น 23:43:AA:5B:32:2C ซึ่งจะไม่มีอุปกรณ์ที่มีหมายเลขนี้ซ้ำกันเด็ดขาด

2.1.8 ARP คืออะไร

ในกรณีที่มีการส่งข้อมูลจาก interface หนึ่ง ทุกๆ interface ที่อยู่ในเน็ตเวิร์คเดียวกันจะได้รับข้อมูล แต่มีเพียงอินเทอร์เฟสที่มี MAC Address ตรงกับ MAC Address ของผู้รับที่ระบุในเฟรมข้อมูลเท่านั้น ที่จะนำข้อมูลนั้นไปประมวลผล ดังนั้นในการส่งข้อมูลจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง ฝั่งผู้ส่งจะต้องระบุ MAC Address ของผู้รับให้ถูกต้อง จึงจะสามารถส่งข้อมูลไปได้ สมมติว่า เครื่องคอมพิวเตอร์ IP 172.17.3.12 ต้องการติดต่อกับ 161.246.10.21 การทำงานในระดับ IP จะสั่งให้ ส่งข้อมูลไปยัง

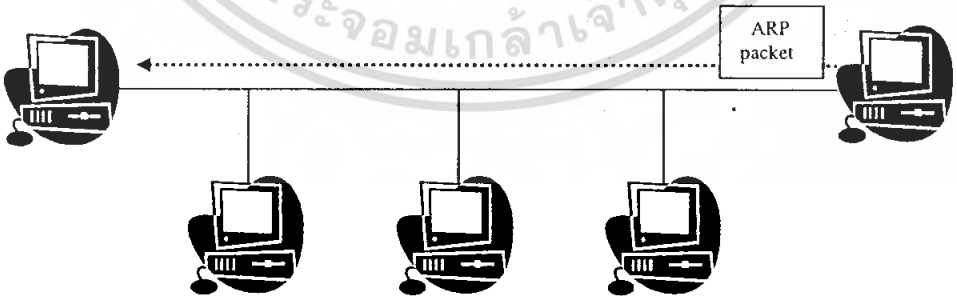
172.17.3.1 ซึ่งเป็น default Router แต่ 172.17.2.12 จะรู้ได้อย่างไรว่า 172.17.2.12 มี MAC Address คืออะไร ? จุดนี้เองที่จะต้องมีการใช้ ARP ในการสอบถาม MAC Address จากเครื่องที่เราต้องการส่งข้อมูล เมื่อได้รับ MAC Address ของผู้รับมาแล้วจึงสามารถเชื่อมต่อกับ เครื่องอีกฝั่ง เพื่อการสื่อสารในระดับสูงขึ้นไปได้ การทำงานของ ARP เป็นเรื่องไม่ซับซ้อน มีเพียง 2 ขั้นตอนเท่านั้นคือ

1. เครื่องที่ต้องการสอบถาม MAC Address ส่ง ARP packet เรียกว่า **ARP Request** ซึ่งบรรจุ IP, MAC Address ของตนเอง และ IP Address ของเครื่องที่ต้องการทราบ MAC Address ส่วน MAC Address ปลายทางนั้น จะถูกกำหนดเป็น FF:FF:FF:FF:FF:FF ซึ่งเป็น Broadcast Address เพื่อให้ ARP packet ถูกส่งไปยังเครื่องทุกเครื่องที่อยู่ในเน็ตเวิร์คเดียวกัน



รูปที่ 2.7 ARP Request จะถูกส่งไปยังเครื่องทุกเครื่องในเน็ตเวิร์ค

2. เฉพาะเครื่องที่มี IP Address ตรงกับที่ระบุใน ARP Packet จะตอบกลับมาด้วย ARP Packet เช่นกัน โดยใส่ MAC Address และ IP Address ของตนเองเป็นผู้ส่ง และใส่ MAC Address และ IP Address ของเครื่องที่ส่งมาเป็นผู้รับ packet ที่ตอบกลับนี้เรียกว่า **ARP Reply**



รูปที่ 2.8 ARP Reply จะถูกตอบกลับมาจากเครื่องที่มี IP Address เพื่อบอก MAC Address ของตนเอง

จากที่กล่าวมา จะเห็นว่ากระบวนการ ARP จะเกิดขึ้นทุกครั้งที่มีการส่ง IP datagram และกระบวการ ARP ก็กินเวลารับส่งข้อมูลและทรัพยากรในเน็ตเวิร์คพอสมควร โดยเฉพาะในจุดที่ต้องมีการ Broadcast ARP Request ซึ่งหากเป็นเช่นนั้น แบนวิธ์อันมีค่าของเน็ตเวิร์คลงหมดไปกับ ARP Packet ที่วิ่งพล่านในสายเคเบิ้ล จึงมีการออกแบบบัฟเฟอร์เป็นตารางจับคู่ ระหว่าง ARP กับ IP Address เพื่อไม่ต้องส่ง ARP Request / Reply ทุกครั้งที่จะทำการส่ง IP datagram แต่ IP Address นั้นเป็นสิ่งที่ผู้ใช้กำหนดขึ้น เป็น Logical ซึ่งสามารถเปลี่ยนแปลงได้ ดังนั้น ข้อมูลในตารางนี้จึงต้องมีอายุการใช้งาน โดยทั่วไป กำหนดให้เป็นเวลา 20 นาที เมื่อหมดเวลาแล้ว หากจะส่ง IP Datagram ครั้งต่อไป จะต้องทำการส่ง ARP Request ใหม่ สามารถเรียกดู ARP cache ในระบบปฏิบัติการ Linux ได้ด้วยคำสั่ง #ARP [Enter]

```
[root@Sandy root]# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.17.0.1               ether   00:09:E9:95:D9:40   C                     eth0
172.17.3.28              ether   00:01:03:41:52:D5   C                     eth0
[root@Sandy root]#
```

รูปที่ 2.9 ผลของคำสั่ง arp แสดงตาราง arp cache สำหรับระบบปฏิบัติการ Linux

Ethernet destination Address	Ethernet source Address	Frame Type	Hard Type	Prot Type	Hard size	Prot size	Sender Ethernet address	Sender IP address	Target Ethernet address	Target IP address

รูปที่ 2.10 ARP Packet Format

ตารางที่ 2.3 ARP Packet Format

ตำแหน่ง	ชื่อ	อธิบาย
ไบต์ 0-5	Ethernet Destination Address	ส่วนนี้อยู่ใน Header ของ Ethernet Frame ทั่วไป มีความหมายเป็น Address ปลายทาง ในกรณีของ ARP Request ข้อมูลในฟิลด์นี้จะเป็น FF:FF:FF:FF:FF:FF
ไบต์ 6-11	Ethernet Source Address	ส่วนนี้อยู่ใน Header ของ Ethernet Frame ทั่วไป มีความหมายเป็น Address ต้นทาง
ไบต์ 12-13	Ethernet Frame Type	ระบุถึงโปรโตคอลที่ Encapsulate อยู่ใน Ethernet Frame นี้ สำหรับ ARP จะต้องเป็น 0x0806
ไบต์ 14-15	Hard Type	ระบุถึงประเภทของ Hardware ที่โปรโตคอล ARP ถามอยู่ สำหรับกรณีนี้คือ Ethernet Address จะต้องเป็น 1
ไบต์ 16-17	Prot Type	ระบุชนิดของโปรโตคอลที่ถาม ว่าเป็น Hardware Address ของโปรโตคอลอะไร ในที่นี้คือ IP
ไบต์ 18	Hard Size	

ตารางที่ 2.3 (ต่อ) ARP Packet Format

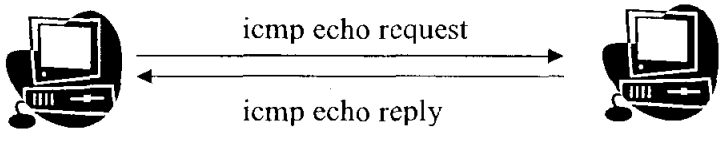
ตำแหน่ง	ชื่อ	อธิบาย
ไบต์ 19		ระบุขนาดของแอดเดรสในโปรโตคอลที่ถาม ซึ่งมีค่าเป็น 4 สำหรับ IP
ไบต์ 20-21	OP Field	เป็นการระบุว่าเป็น ARP ชนิดใด
ไบต์ 22-27	Sender Ethernet Address	Ethernet Address ของผู้ส่ง มีค่าซ้ำกับในไบต์ที่ 6-11
ไบต์ 28-31	Sender IP Address	IP Address ของผู้ส่ง
ไบต์ 32-37	Target Ethernet Address	Ethernet Address ของผู้รับ ค่านี้จะว่างไว้ในกรณีของ ARP Request
ไบต์ 38-41	Target IP Address	IP Address ของผู้รับ

2.1.9 ICMP: Internet Control Message Protocol

ICMP เป็นโปรโตคอลที่ใช้ในการตรวจสอบและรายงานสถานภาพของดาต้าแกรม โปรโตคอลนี้ทำงานในระดับ Network Layer เช่นเดียวกับ IP ในกรณีที่เกิดปัญหากับดาต้าแกรม เช่น เราเตอร์ไม่สามารถส่งดาต้าแกรมไปถึงปลายทางได้ ICMP จะถูกส่งออกไปยังโฮสต้นทางเพื่อรายงานข้อผิดพลาด ที่เกิดขึ้น อย่างไรก็ดี ไม่มีอะไรรับประกันได้ว่า ICMP Message ที่ส่งไปนั้น จะถึงผู้รับจริงหรือไม่ หากมีการส่งดาต้าแกรมออกไปแล้วไม่มี ICMP Message ฟ้อง Error กลับมา ก็แปลความหมายได้สองกรณีคือ ข้อมูลถูกส่งไปถึงปลายทางอย่างเรียบร้อย หรืออาจจะมีปัญหา ในการสื่อสารทั้งการส่งดาต้าแกรม และ ICMP Message ที่ส่งกลับมาก็มีปัญหาระว่างทางก็ได้ ICMP จึงเป็นโปรโตคอลที่ไม่มีความน่าเชื่อถือ (unreliable) ซึ่งจะเป็นหน้าที่ของ โปรโตคอลในระดับสูงกว่า Network Layer ในการจัดการให้การสื่อสารนั้นๆ มีความน่าเชื่อถือ

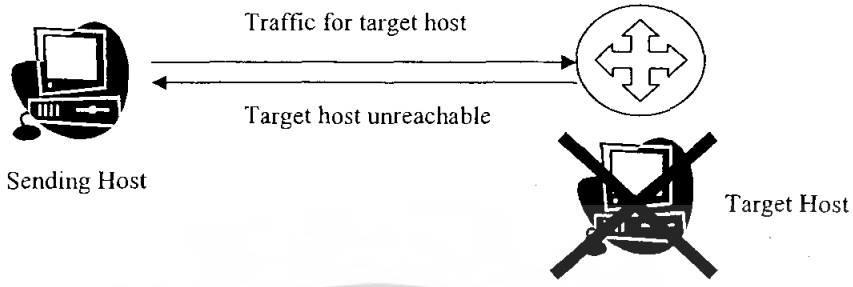
การใช้งาน ICMP โดยทั่วไป ICMP มีการใช้งานในสองลักษณะคือ

1. **Query** ใช้สอบถามสถานะระหว่างกัน ในรูปที่ 2.11เป็นการส่ง Echo request เพื่อถามสถานะของปลายทาง ซึ่งโฮสปลายทางอยู่ในสถานะปกติ สามารถทำการสื่อสารได้จะส่ง Echo Reply กลับมา



รูปที่ 2.11 การใช้งานโปรโตคอล ICMP เพื่อสอบถามสถานะระหว่างกัน

2. **Error Report** ใช้รายงานข้อผิดพลาดที่เกิดขึ้น เช่น หากไม่สามารถส่งดาต้าแกรมไปถึงปลายทางได้ เราเตอร์จะส่ง ICMP Message Host Unreachable กลับมารายงานโฮสต้นทาง (รูปที่ 2.12)



รูปที่ 2.12 การใช้งานโปรโตคอล ICMP เพื่อรายงานข้อผิดพลาดที่เกิดขึ้น

ICMP Message

8-bit Type	8-bit Type	16-bit checksum
ICMP Data		

รูปที่ 2.13 แสดงรูปร่างของ ICMP Message

ตำแหน่งต่างๆของข้อมูลภายใน Data จะขึ้นอยู่กับชนิดของ ICMP นั้นๆ

ตารางที่ 2.4 ICMP Message

ตำแหน่ง	ชื่อ	อธิบาย
บิต 0-7	Type	ประเภทของ ICMP Message
บิต 8-15	Code	รหัสของ ICMP Message
บิต 16-31	Checksum	เป็นตัวตรวจสอบความถูกต้องของ ICMP Massage ทั้งหมด
ไม่แน่นอน	Data	ข้อมูลภายใน ICMP Message ขึ้นอยู่กับ Type

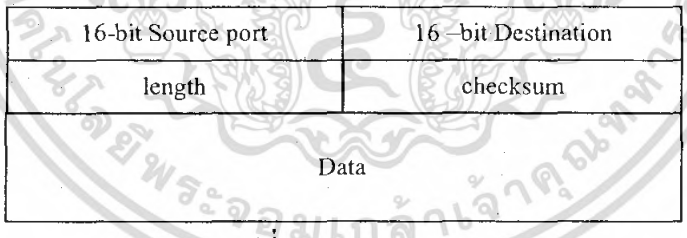
ICMP Message Type

TYPES ของ ICMP มีความหมายดังนี้

TYPE	Description	TYPE	Description
0	Echo Reply	13	Timestamp Request
3	Destination Unreachable	14	Timestamp Reply
4	Source Quench	15	Information Request
5	Redirect Message	16	Information Reply (No Longer Used)
8	Echo Request	17	Address Mask Request
11	Time Exceeded	18	Address Mask Reply
12	Parameter Problem		

2.1.10 UDP : User Datagram Protocol

UDP เป็นโปรโตคอลที่ถูกออกแบบมาให้ทำหน้าที่รับส่งข้อมูลโดยมีขั้นตอนการทำงานไม่ซับซ้อนและทำงานได้รวดเร็ว แต่มีจุดด้อยคือไม่มีความน่าเชื่อถือ (unreliable) และเป็นการสื่อสารแบบไม่ต่อเนื่อง (connectionless) โปรโตคอล UDP ทำงานในชั้น Transport Layer ซึ่งจะต้องพึ่งพาโปรโตคอล IP ในการรับส่งข้อมูล



รูปที่ 2.14 UDP Header

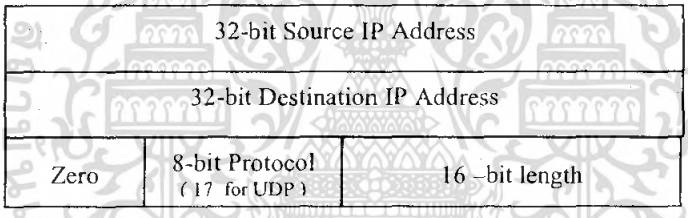
UDP Checksum

Checksum เป็น เลข 16 บิตถูกคำนวนด้วยวิธี one's complement โดยนำ Pseudo Header และข้อมูลทั้งหมดใน UDP Datagram มาคำนวน

Pseudo Header เป็นข้อมูลที่อยู่ในส่วนของ IP Header ประกอบด้วยฟิลด์ source IP address, destination IP address , zero , protocol , UDP length ดังแสดงในรูปที่ 2.15

ตารางที่ 2.5 UDP Header

ตำแหน่ง	ชื่อ	อธิบาย
บิต 0-15	Source port number	หมายเลขพอร์ตต้นทางที่ส่งดาต้าแกรมนี้ มีความยาว 16 บิต
บิต 16-31	destination port number	หมายเลขพอร์ตปลายทางที่จะเป็นผู้รับดาต้าแกรม มีความยาว 16 บิตเช่นกัน
บิต 32-47	UDP length	ความยาวของดาต้าแกรม ทั้งส่วน Header และ data นั่นหมายความว่า ค่าที่น้อยที่สุดในฟิลด์นี้คือ 8 ซึ่งเป็นขนาดของ Header
บิต 48-63	Checksum	เป็นตัวตรวจสอบความถูกต้องของ UDP datagram และจะนำข้อมูลบางส่วนใน IP Header มาคำนวนด้วย



รูปที่ 2.15 Pseudo Header

หากค่า Checksum ที่คำนวนออกมาเป็น 0 ค่า checksum จะถูกเซ็ตเป็น 1 ทั้งหมดแทน (มีค่าเท่ากันในระบบ 1's complement) ทั้งนี้เพราะในบางแอพพลิเคชั่นที่ไม่ต้องการตรวจสอบค่า checksum ในระดับ UDP จะเซ็ตค่านี้เป็น 0 (disable checksum)

2.1.11 TCP : Transmission Control Protocol

TCP เป็นโปรโตคอลที่ใช้สื่อสารระหว่างโฮสที่มีความน่าเชื่อถือ จะเห็นได้ว่าโปรโตคอลในระดับ IP หรือแม้กระทั่ง UDP จะสนใจ ข้อมูลเพียง 1 ดาต้าแกรม กลไกของโปรโตคอลจะมีหน้าที่ตรวจสอบความถูกต้องเพียงเฉพาะดาต้าแกรมนั้น ๆ เมื่อจะทำ การส่งดาต้าแกรมใหม่ก็จะถือว่าเป็นข้อมูลชุดใหม่ที่ไม่มีความสัมพันธ์ใด ๆ กับข้อมูลดาต้าแกรมอื่น (การสื่อสาร 1 ครั้ง จึงใช้เพียง 1 ดาต้าแกรม) แต่สำหรับ TCP แล้วจะเห็นว่าข้อมูลนั้นเป็น stream คือมีความสัมพันธ์ต่อเนื่องกัน มีกลไกในการตรวจสอบทั้งด้านส่ง และด้านรับเพื่อให้แน่ใจว่าสามารถสื่อสารกันได้จริงจึงจะมีการส่งรับข้อมูลเกิดขึ้น ตลอดจนการยกเลิกการติดต่อก็มีกลไกสำหรับแจ้งให้อีกฝั่งทราบ ทำให้การสื่อสารด้วย TCP จึงเสมือนว่าทั้ง 2 ฝ่าย

คือฝ่ายรับและฝ่ายส่งได้ทำการต่อสาย เน็ตเวิร์กถึงกัน (connected) ตลอดเวลาที่การรับส่งข้อมูลจนกระทั่งการสื่อสารทั้งหมดเสร็จสิ้นจึงจะทำการยกเลิกการเชื่อมต่อนั้นเสีย

จุดเด่นประการสำคัญของ TCP ที่กล่าวถึงอยู่เสมอคือ ความมีเสถียรภาพและความถูกต้องของการสื่อสารซึ่งมีความเชื่อถือได้สูง คุณสมบัติที่ทำให้ TCP มีข้อดีดังกล่าวคือ

1. ข้อมูลที่จะส่งผ่าน TCP จะถูกนำมาแตกย่อยออกเป็นส่วน ๆ ให้มีขนาดเหมาะสมสำหรับการส่งข้อมูล โดย TCP มีกลไกในการพิจารณาว่าขนาดเท่าใดจะทำให้การรับและส่งนั้นมีประสิทธิภาพและน่าเชื่อถือสูงสุด โดยข้อมูลแต่ละชุดที่แบ่งออกและ ทำการส่งโดย TCP แต่ละครั้งจะเรียกว่า TCP เซกเมนต์

2. ในการส่งข้อมูลแต่ละครั้ง TCP จะมีการจับเวลาไว้เสมอ เพื่อรอการตอบรับจากผู้รับว่าได้รับข้อมูลถูกต้อง หากหมดเวลาแล้วไม่มีการตอบรับ TCP จะถือว่าข้อมูลไปไม่ถึงและทำการแก้ปัญหาที่เกิดขึ้น เช่น ยกเลิกการติดต่อ, ส่งข้อมูลซ้ำ ทำให้ Application ทราบสถานะการส่งข้อมูลตลอดเวลา

3. TCP มี checksum ซึ่งจะครอบคลุมทั้ง TCP Header และ TCP Data เพื่อเป็นการป้องกันและตรวจสอบว่าข้อมูล ที่ส่งมานั้นถูกต้อง และไม่ได้ถูกแก้ไขระหว่างทาง หาก TCP ได้รับข้อมูลที่ทำการตรวจสอบกับ checksum แล้วปรากฏว่า มีความผิดพลาดเกิดขึ้น TCP จะทิ้งข้อมูลที่ได้รับและจะไม่ทำการตอบรับข้อมูลนั้นกลับไปยังผู้ส่ง คือถือเสมือนว่าไม่ได้รับ ข้อมูลนั้น เพื่อให้ทางฝ่ายผู้ส่งทำการส่งใหม่หรือหาข้อบกพร่องและพยายามแก้ไขตามแต่แอพพลิเคชั่นทางฝ่ายผู้ส่งเห็น สมควร

4. เนื่องจาก TCP อาศัย IP ในการส่งข้อมูล ซึ่ง IP เองอาจจะถูกแฟรกเมนต์ได้ และทำให้ข้อมูลที่ถูกแฟรกเมนต์นั้นส่งถึง ปลายทางในลำดับที่ไม่ถูกต้องได้ หน้าที่ของ TCP เมื่อรับข้อมูลที่แฟรกเมนต์มานั้นจะต้องนำข้อมูลแต่ละส่วนมาประกอบ รวมกันให้ถูกต้องสมบูรณ์ก่อนจะส่งไปยัง Application Layer ต่อไป

5. การส่ง - รับข้อมูลด้วย IP อาจจะมีกรณีที่ IP Datagram นั้นถูกส่งซ้ำขึ้นได้ TCP ที่รับข้อมูลซ้ำดังกล่าวจะต้องทราบว่า เป็น IP Datagram ที่ซ้ำและไม่นำข้อมูลไปใช้งาน

6. TCP มีกลไกควบคุมการไหลของข้อมูล (Flow Control) โดยการควบคุมนี้จะต้องอาศัยลำดับของการรับส่งที่ถูกต้อง และสัมพันธ์กันทั้ง 2 ฝั่ง ในขณะเดียวกันข้อมูลที่ส่งนั้นจะต้องอาศัย IP หลายดาต้าแกรมจึงจะได้รับข้อมูลครบทั้งหมด ดังนั้นในการรับข้อมูลทางฝ่ายรับจึงต้องเตรียมบัฟเฟอร์ไว้จำนวนหนึ่งเพื่อรอรับข้อมูลและรวบรวมข้อมูลทั้งชุดให้อยู่ใน บัฟเฟอร์ก่อนที่จะทำการจัดเรียงข้อมูล ตรวจสอบความถูกต้องแล้วจึงส่งต่อไปยังแอพพลิเคชั่น ด้วยเหตุผลดังกล่าวจะเห็น ได้ว่าขนาดของข้อมูลมิได้ถูกจำกัดที่ขนาดของดาต้าแกรมใด ๆ ข้อมูลที่ส่งอาจจะมีขนาดใหญ่มากอยู่ในหลายดาต้าแกรม ก็เป็นได้ ดังนั้นเพื่อป้องกันการส่งข้อมูลขนาดใหญ่เร็วเกินไปจนทำให้ทางฝ่ายรับไม่มีหน่วยความจำเพียงพอที่จะเป็น บัฟเฟอร์ที่พักข้อมูล การส่งข้อมูลจึงถูกจำกัดโดยจะอนุญาต เท่าที่ฝ่ายรับมีบัฟเฟอร์เพียงพอเท่านั้น

<table>
<tr><td colspan="8">16-bit Source Port Number</td><td colspan="8">16-bit Source Destination Number</td></tr>
<tr><td colspan="16">32-bit Sequence Number</td></tr>
<tr><td colspan="16">32-bit Acknowledgment Number</td></tr>
<tr><td>Header Length</td><td colspan="3">16-bit Reserved</td><td>URG</td><td>ACK</td><td>PUSH</td><td>RESET</td><td>SYN</td><td>FIN</td><td colspan="6">16-bit Windows Size</td></tr>
<tr><td colspan="10">16-bit TCP Checksum</td><td colspan="6">16-bit Urgent Pointer</td></tr>
<tr><td colspan="16">TCP Option</td></tr>
<tr><td colspan="16">Data</td></tr>
</table>

รูปที่ 2.16 TCP Header

ตารางที่ 2.6 TCP Header

ชื่อ	อธิบาย
Source Port Number	หมายถึงพอร์ตที่โฮสต์ต้นทางใช้ในการสื่อสารกันของเซสชั่นนี้ และ TCP/IP จะใช้พอร์ตนั้นไป ตลอดตราบใดที่การสื่อสารในเซสชั่นนี้ยังไม่ยุติลง โดยทั่วไปพอร์ตนี้จะเรียกว่า "ไคลเอนต์พอร์ต" คือพอร์ตที่ไคลเอนต์เปิดขึ้น มาเพื่อรอการตอบรับจากเซิร์ฟเวอร์ (พิจารณาจากทิศทางของแพ็กเก็ตที่ส่งมาจากไคลเอนต์ไปยังเซิร์ฟเวอร์) ไคลเอนต์พอร์ตจะมีหมายเลขไม่แน่นอนและเปลี่ยนไปทุกครั้งที่มีการเริ่มการเชื่อมต่อใหม่ เป็นพอร์ตที่ถูกเปิดไว้ในระยะเวลาสั้น ๆ (ephenumeral port) ค่าที่เป็นไปได้ของพอร์ตนี้ขึ้นอยู่กับการจัดสรรของระบบปฏิบัติการ ในการกำหนดขอบเขตของพอร์ตเหล่านี้ส่วนใหญ่จะมีค่า อยู่ในช่วง 1024 - 5000
Destination Port Number	หมายถึงหมายเลขพอร์ตบนโฮสต์ปลายทางที่โฮสต์ต้นทางต้องการติดต่อด้วย โดยนัยแล้วจะ หมายถึงแอพพลิเคชั่นที่ให้บริการอยู่พอร์ตนั้นที่โฮสต์ปลายทางนั่นเอง พอร์ตนั้นจะเรียกอีกอย่างหนึ่งว่า "เซิร์ฟเวอร์พอร์ต" หมายเลขพอร์ตที่เปิดไว้จะขึ้นอยู่กับแอพพลิเคชั่นที่ให้บริการ โดยทั่วไปแอพพลิเคชั่นแต่ละประเภทจะมีหมายเลขพอร์ต เป็นมาตรฐานสำหรับให้ไคลเอนต์ได้เรียกใช้บริการ
Sequence Number	เป็นฟิลด์ที่ระบุถึงหมายเลขลำดับที่ใช้อ้างอิงในการสื่อสารข้อมูลแต่ละครั้ง เพื่อให้ทั้ง 2 ฝ่าย จะได้รับทราบตรงกันว่าเป็นข้อมูลของชุดใด การนำไปใช้งานจะได้ไม่ปะปนกัน และมีลำดับที่ถูกต้อง เนื่องจากการสื่อสารข้อมูลผ่าน TCP นั้นจังหวะและลำดับเป็นส่วนสำคัญของโปรโตคอลไม่ยิ่งหย่อนไปกว่าข้อมูลใน TCP Header รวมไปถึง การที่ข้อมูลในแต่ละ TCP Segment อาจจะถูกทำการแฟรกเมนต์ในเลเยอร์ของ IP ถัดลงไป ทำให้ข้อมูลถูกแบ่งออกและส่งไปในลำดับที่ไม่เรียงกัน หากไม่มีจุดอ้างอิงของข้อมูลก็จะไม่สามารถอ่านข้อมูลกลับใหม่ได้อย่างสมบูรณ์และถูกต้อง การส่งข้อมูลและการตอบรับจะใช้ฟิลด์ นี้เป็นตัวยืนยันระหว่างกันเสมอ

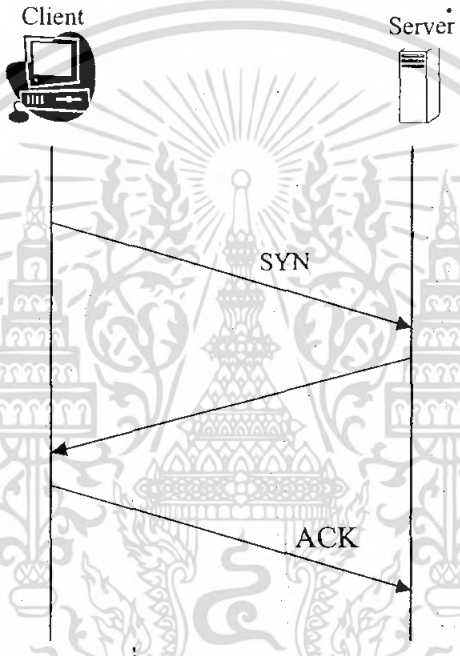
ตารางที่ 2.6 (ต่อ) TCP Header

<table>
<tr><th>ชื่อ</th><th>อธิบาย</th></tr>
<tr><td>Acknowledge Number</td><td>ทำหน้าที่เช่นเดียวกับ Sequence Number ต่างกันตรงที่เป็น Sequence Number ซึ่งในการตอบรับ กล่าวคือ เนื่องจาก Sequence Number ที่ใช้ในการอ้างอิงนั้นผู้ที่เริ่มส่งข้อมูลจะเป็นผู้กำหนดเลขขึ้น มาและส่งไปพร้อมกับการสร้างการเชื่อมต่อครั้งใหม่ แต่สำหรับฝ่ายที่ถูกติดต่อก็จำเป็นต้องกำหนดหมายเลขสำหรับใช้อ้างอิง ในการตอบรับเช่นกัน ค่าที่อยู่ใน Acknowledge Number ก็คือหมายเลขที่ใช้อ้างอิงในการตอบรับนี้</td></tr>
<tr><td>Header Length</td><td>โดยปกติความยาวของ TCP Header จะเท่ากับ 20 ไบต์ แต่ถ้าหากมีการใช้ Option อาจจะทำให้ ขนาดของเฮดเดอร์ยาวขึ้นตามข้อมูลที่ต้องเพิ่มมาจาก Option นั้น แต่ทั้งหมดแล้วจะไม่เกิน 60 ไบต์</td></tr>
<tr><td></td><td>เป็นข้อมูลในระดับบิตที่ใช้เป็นตัวบอกคุณสมบัติของ TCP Segment ที่กำลังส่งอยู่นั้น และใช้เป็นตัวควบคุมจังหวะ การรับส่งข้อมูลด้วย ซึ่ง Flag ทั้งหมดมีอยู่ 6 บิต แต่ละบิตมีชื่อและมีความหมายดังนี้
<table>
<tr><th>Flag</th><th>อธิบาย</th></tr>
<tr><td>URG</td><td>ใช้บอกความหมายว่าเป็นข้อมูลด่วน และมีข้อมูลพิเศษมาด้วย (อยู่ใน Urgent pointer)</td></tr>
<tr><td>ACK</td><td>แสดงว่าข้อมูลในฟิลด์ Acknowledge Number นำมาใช้งานได้</td></tr>
<tr><td>DSH</td><td>เพื่อแจ้งให้ผู้รับข้อมูลทราบว่า ควรจะส่งข้อมูล Segment นี้ไปยังโพรเซสที่กำลังรออยู่ทันที</td></tr>
<tr><td>RST</td><td>ใช้ในการณีที่เกิดการสับสนขึ้นด้วยเหตุผลต่างๆ
เช่น โฮสต์มีปัญหา ให้เริ่มต้นสื่อสารกันใหม่</td></tr>
<tr><td>SYN</td><td>ใช้ในการเริ่มต้นขอติดต่อกับปลายทาง</td></tr>
<tr><td>FIN</td><td>ใช้ส่งเพื่อแจ้งให้ปลายทางทราบว่ายุติการติดต่อ</td></tr>
</table></td></tr>
<tr><td>Window Size</td><td>เป็นขนาดของการรับ - ส่งข้อมูลในแต่ละครั้งที่ทางฝ่ายผู้รับจะสามารถรับได้ เนื่องจากในการรับข้อมูลนั้น ทางผู้รับจะต้องจัดเตรียมหน่วยความจำในการพักข้อมูลที่มากจาก TCP และทำการ Demultiplex ออกมา หากไม่มีการตกลง ถึงขนาดที่ทางฝ่ายรับสามารถรับได้ ก็จะทำให้การสื่อสารข้อมูลไม่สมดุล และฝ่ายรับอาจจะประมวลผลทัน ซึ่งจะส่งผลให้ต้องส่ง ข้อมูลซ้ำหลายครั้ง</td></tr>
<tr><td>Checksum</td><td>ฟิลด์ที่ใช้ในการตรวจสอบความถูกต้องของข้อมูลใน TCP เซกเมนต์ใช้ระบุหมายเลข Sequence Number ของ TCP เซกเมนต์ล่าสุดที่อยู่ในโหมด Urgent</td></tr>
</table>

ตารางที่ 2.6 (ต่อ) TCP Header

ชื่อ	อธิบาย
Urgent Pointer	ข้อมูลเพิ่มเติมซึ่งจะอยู่ใน TCP Header เมื่อมีการตั้งค่า option บางอย่างที่ต้องการข้อมูลเพิ่มเติมซึ่งไม่มีใน TCP Header เช่น MSS, Strict Route

Connection Establishment



รูปที่ 2.17 3-way handshake

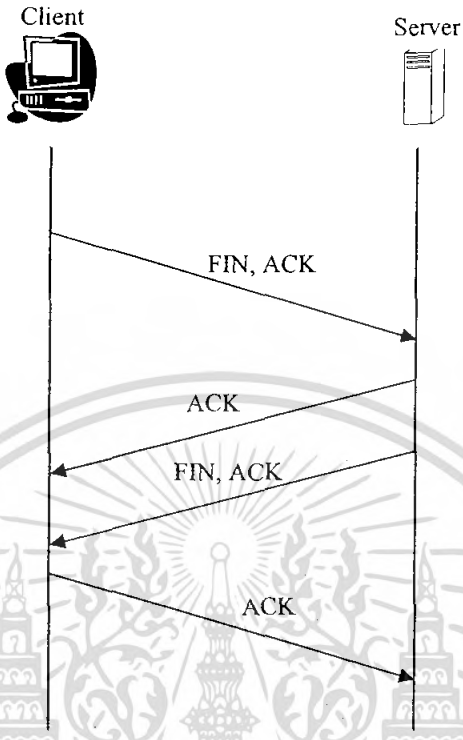
ก่อนที่จะเริ่มต้นการสื่อสาร จะต้องมีการส่งสัญญาณเพื่อบอกโฮสต์อีกฝั่งหนึ่งให้เตรียมตัวติดต่อ ซึ่งกระบวนการที่ใช้มีชื่อเรียกว่า 3-Way Hand Shake มีขั้นตอนคือ

1. เครื่องไคลเอนต์จะทำการส่งเซกเมนต์ โดยเปิด SYN Flag ระบุหมายเลขพอร์ตที่ต้องการติดต่อบนเซิร์ฟเวอร์และระบุหมายเลข ลำดับของข้อมูล (ISN - Initial Sequence Number)

2. เครื่องเซิร์ฟเวอร์เมื่อได้รับข้อมูลเซกเมนต์จากข้อ 1 ก็จะตอบกลับด้วยการเพิ่มค่า ISN ที่ได้รับขึ้นอีก 1 พร้อมทั้งระบุหมายเลขลำดับ (ISN) ของตนเอง และเปิด SYN กับ ACK Flag

3. ไคล์เอนต์เมื่อได้รับการตอบกลับจากเซิร์ฟเวอร์ตามข้อ 2 ก็จะทำการตอบรับกลับไปโดยการเพิ่มค่า ISN ของเซิร์ฟเวอร์ขึ้นอีก 1 และเปิด ACK Flag เมื่อผ่านการสร้าง connection ทั้ง 3 ขั้นตอนแล้ว ตอนนี้ทั้งไคล์เอนต์ และเซิร์ฟเวอร์เปรียบเสมือนมีการเชื่อมต่อถึงกันแล้ว สถานะของการเชื่อมต่อในขณะนี้เรียกว่า Established

Connection Termination



รูปที่ 2.18 TCP Header

เมื่อการสื่อสารของทั้งสองฝั่งจบลง และไม่ต้องการรับส่งข้อมูลอีกต่อไป จะต้องทำตามขั้นตอนการยุติการสื่อสารเพื่อให้การสื่อสารจบลงอย่างสมบูรณ์ ซึ่งมีอยู่ 4 ขั้นตอนคือ

1. ไคลเอนต์ทำการส่ง ISN พร้อมกับ FIN ACK Flag ไปยังเซิร์ฟเวอร์
2. เซิร์ฟเวอร์ทำการตอบรับ ISN และบวกค่า ISN อีก 1 พร้อม ACK Flag
3. เซิร์ฟเวอร์ทำการส่ง ISN พร้อมกับ FIN ACK Flag ไปยังไคลเอนต์
4. ไคลเอนต์ทำการตอบรับ ISN และบวกค่า ISN อีก 1 พร้อม ACK Flag

การยุติการเชื่อมต่อ โดยส่ง FIN ACK ออกไปมีความหมายคือ โฮสต์ที่ส่งไม่มีข้อมูลจะส่งไปอีก มิใช่ต้องการปิดการสื่อสารทั้งหมดในทันที ดังนั้นจึงต้องทำทั้งสองทาง การสื่อสารจึงจะยุติลงอย่างสมบูรณ์ ในการใช้งานจริง อาจมีการยุติการสื่อสารเพียงด้านเดียว คือหยุดส่งข้อมูล แต่ยังคงเปิดพอร์ตไว้รอรับข้อมูลจากอีกด้านหนึ่ง ทั้งนี้ขึ้นอยู่กับลักษณะการใช้งาน การปิดพอร์ตสื่อสารเพียงด้านเดียวเช่นนี้เรียกว่า Half-Close

2.2 Voice over IP (VoIP)

2.2.1 วิวัฒนาการการสื่อสารผ่านอินเตอร์เน็ต

ในปัจจุบันการใช้อินเทอร์เน็ตมีบทบาทกับชีวิตประจำวันมากขึ้น และใช้งานกันอย่างกว้างขวาง โดยเฉพาะอย่างยิ่งความจำเป็นที่จะต้องติดต่อสื่อสาร อินเตอร์เน็ตจึงได้รับการพัฒนาโครงสร้างพื้นฐานเพื่อรองรับการสื่อสารรูปแบบต่างๆ เช่น การใช้จดหมายอินเล็กทรอนิกส์ การติดต่อด้วยเสียง ระบบ VDO Conference การใช้โทรศัพท์บนเครือข่ายซึ่งก็มีวิวัฒนาการตามลำดับเบื้องต้นดังนี้

E-mail

หรือ จดหมายอิเล็กทรอนิคส์เป็นบริการอย่างหนึ่งที่นิยมใช้กันอย่างแพร่หลายมาก จนทำให้บางคนคิดว่า E-mail คือ อินเตอร์เน็ต และอินเตอร์เน็ตคือ E-mail วิธีใช้งานอีเมลล์ก็ง่ายและมีประโยชน์มาก การทำงานของ E-mail มีลักษณะคล้ายกับระบบไปรษณีย์ปกติ (หมายถึงระบบที่ใช้กระดาษในการเขียนจดหมาย) กล่าวคือในระบบไปรษณีย์ปกติมีหน่วยงานที่ทำหน้าที่ในการรับส่งจดหมายคือเป็นบรุษไปรษณีย์ ถ้าเป็นในอินเตอร์เน็ตสิ่งที่ทำหน้าที่คอยรับส่งจดหมายคือบรรดาคอมพิวเตอร์ทั้งหลายที่ทำหน้าที่เป็น E-mail Server (คอมพิวเตอร์ที่ทำหน้าที่ให้บริการด้านจดหมายอิเล็กทรอนิคส์)

Chat

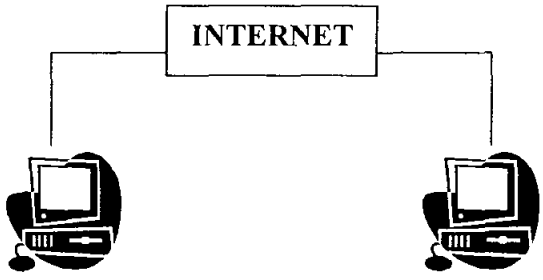
คือ การส่งข้อความสั้นๆ ระหว่างบุคคลที่อยู่หน้าเครื่องคอมพิวเตอร์ในเวลาเดียวกัน และสามารถเขียนโต้ตอบกันไปมาคล้ายกับการคุยกัน ซึ่งก็ได้มีการพัฒนโปรแกรมสำหรับหาร Chat ออกมามากมายที่เป็นที่นิยมและใช้กันอย่างแพร่หลายก็คือ MSN Messenger

และสิ่งหนึ่งที่มีการพัฒนาต่อมา คือระบบการสื่อสารด้วยเสียงผ่านเครือข่าย IP ที่เรียกว่าเทคโนโลยี Voice over IP หรือที่รู้จักกันโดยทั่วไปว่า "VoIP" จนสามารถใช้งานได้ดีขึ้น เพื่อให้ได้รับประโยชน์และมีความสะดวกมากที่สุด VoIP ถูกเริ่มต้นใช้งานกันอย่างกว้างขวาง เพื่อให้เครื่องคอมพิวเตอร์ส่วนบุคคลสามารถสนทนา ระหว่างกัน ได้ รวมถึงการสนทนากับโทรศัพท์พื้นฐานอีกด้วย โดยไม่เสียค่าบริการแต่อย่างใด และคุณภาพของบริการก็ถูกพัฒนาขึ้นมาเรื่อยๆจนเทียบเท่าระบบโทรศัพท์พื้นฐาน

ซึ่ง VoIP สามารถแบ่งได้เป็น 3 ลักษณะคือ

1. คอมพิวเตอร์ส่วนบุคคล ไปยัง คอมพิวเตอร์ส่วนบุคคล (PC to PC)

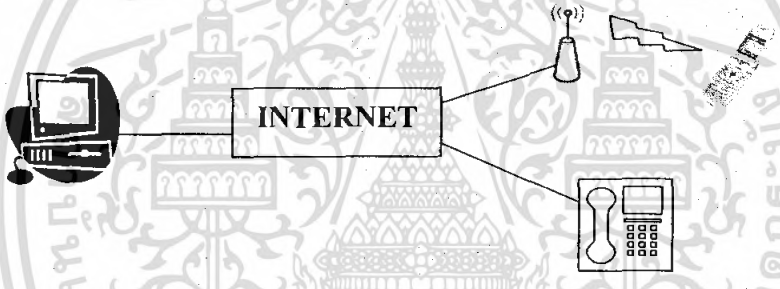
PC มีการติดตั้ง sound card และไมโครโฟน ที่เชื่อมต่ออยู่กับเครือข่าย IP การประยุกต์ใช้ PC และ IP-enabled telephones สามารถสื่อสารกันได้แบบจุดต่อจุด หรือ แบบจุดต่อหลายจุด โดยอาศัย software ทางด้าน IP telephony



รูปที่ 2.19 PC to PC

2. คอมพิวเตอร์ส่วนบุคคล ไปยัง โทรศัพท์พื้นฐาน (PC to Phone)

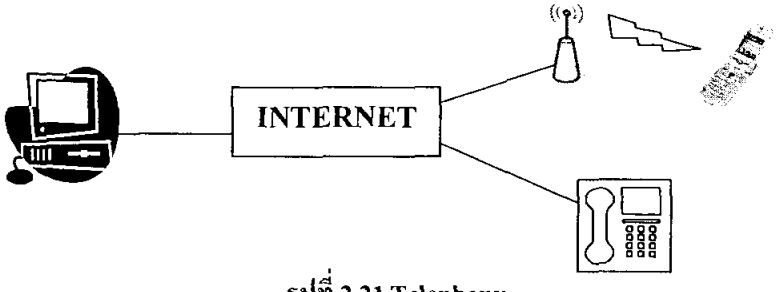
เป็นการเชื่อมเครือข่ายโทรศัพท์เข้ากับ เครือข่าย IP ทำให้โดยอาศัย Voice trunks ที่สนับสนุน voice packet ทำให้สามารถใช้ PC ติดต่อกับ โทรศัพท์ระบบปกติได้



รูปที่ 2.20 PC to phone

3. โทรศัพท์กับโทรศัพท์ (Telephony)

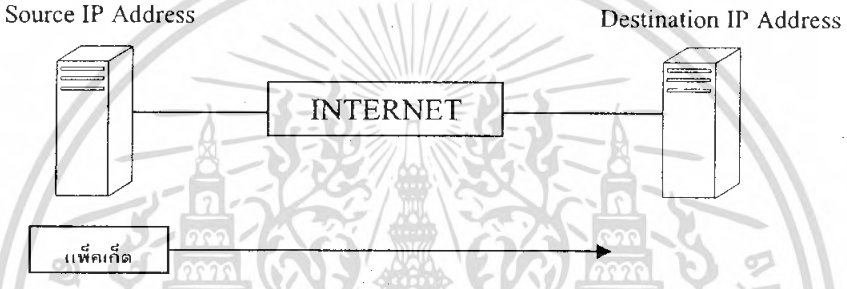
เป็นการใช้โทรศัพท์ธรรมดา ติดต่อกับโทรศัพท์ธรรมดา แต่ในกรณีนี้จริงๆแล้วประกอบด้วยขั้นตอนการส่งเสียงบนเครือข่าย Packet ประเภทต่างๆซึ่งทั้งหมดติดต่อกันระหว่างชุมสายโทรศัพท์ (PSTN) การติดต่อกับ PSTN หรือ การใช้โทรศัพท์ร่วมกับเครือข่ายข้อมูลจำเป็นต้องใช้ gateway



รูปที่ 2.21 Telephony

2.2.2 หลักการพื้นฐานของเครือข่าย IP

เครือข่ายไอพี (Internet Protocol) มีพัฒนามาจากรากฐานระบบการสื่อสารแบบ Packet โดยระบบมีการกำหนด Address ที่เรียกว่า IP Address จาก IP Address หนึ่ง ถ้าต้องการส่งข่าวสารไปยังอีก IP Address หนึ่ง ใช้หลักการบรรจุข้อมูลใส่ใน Packet แล้วส่งไปในเครือข่าย ระบบการจัดส่ง Packet กระทำด้วยอุปกรณ์สื่อสารจำพวก Router โดยมีหลักพื้นฐานการส่งเป็นแบบ DATAGRAM หรือ Packet ซึ่งมีความหมายว่า "เป็นที่เก็บข้อมูลที่เป็นอิสระ ซึ่งมีสารสนเทศเพียงพอในการเดินทางจากแหล่งข้อมูลไปยังคอมพิวเตอร์ปลายทาง โดยปราศจากความเชื่อมั่นของการเปลี่ยนครั้งก่อนระหว่างแหล่งข้อมูลกับคอมพิวเตอร์ปลายทางและเครือข่ายการส่งข้อมูล"



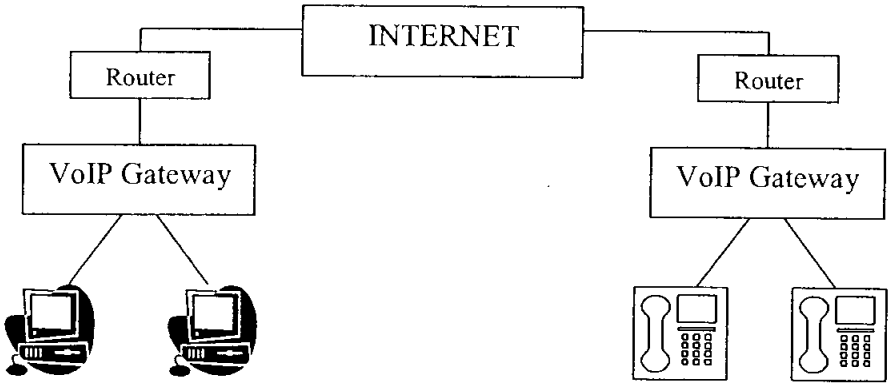
รูปที่ 2.22 หลักการพื้นฐานของเครือข่าย IP

ซึ่งจะเห็นว่าการส่งแบบ Packet เข้าไปในเครือข่ายนั้น จะไม่มีการประกันว่า Packet นั้นจะถึงปลายทางเมื่อไร ดังนั้นรูปแบบของเครือข่ายไอพีจึงไม่เหมาะสมกับการสื่อสารแบบต่อเนื่องเช่น การส่งสัญญาณเสียง หรือวิดีโอ เมื่อเครือข่าย IP กว้างขวางและเชื่อมโยงกันมากขึ้น ความต้องการส่งสัญญาณข้อมูลเสียงที่ได้คุณภาพจึงเกิดขึ้น ก็เลยมีการพัฒนาเป็น VoIP

2.2.3 Voice over IP (VoIP) คืออะไร

VoIP-Voice Over IP หรือที่เรียกกันว่า "VoIP Gateway" หมายถึง การส่งเสียงบนเครือข่ายไอพี เป็นระบบที่แปลงสัญญาณเสียงในรูปของสัญญาณไฟฟ้ามาเปลี่ยนเป็นสัญญาณดิจิตอล คือ นำข้อมูลเสียงมาบีบอัดและบรรจุลงเป็นแพ็กเก็ต ไอพี (IP) แล้วส่งไปโดยมีเราเตอร์ (Router) ที่เป็นตัวรับสัญญาณแพ็กเก็ต และแก้ปัญหาบางอย่างให้ เช่น การบีบอัดสัญญาณเสียงให้มีขนาดเล็กลงการแก้ปัญหาเมื่อมีบางแพ็กเก็ตสูญหายหรือได้มาล่าช้า(delay)

การสื่อสารผ่านทางเครือข่ายไอพีต้องมีเราเตอร์ (Router) ที่ทำหน้าที่พิเศษเพื่อประกันคุณภาพช่องสัญญาณไอพีนี้ เพื่อให้ข้อมูลไปถึง ปลายทางหรือกลับมาได้อย่างถูกต้อง และอาจมีการให้สิทธิพิเศษก่อนแพ็กเก็ตไอพีอื่น (Quality of Service : QoS) เพื่อการให้บริการที่ทำให้เสียงมีคุณภาพ



รูปที่ 2.23 หลักการพื้นฐาน VoIP

นอกจากนั้น Voice over IP (VoIP) ยังเป็นการส่งข้อมูลเสียงแบบ 2 ทางบนระบบเครือข่ายแบบ packet-switched IP network. ซึ่งข้อมูลนี้จะถูกส่งผ่านเครือข่ายอินเตอร์เน็ตสาธารณะ เพื่อสื่อสารระหว่าง VoIP ด้วยกัน โดยที่ยังคงความเป็นส่วนตัวไว้ได้

สำหรับการใช้งานเทคโนโลยี VoIP นั้น จริงๆ แล้วทุกๆ องค์กรสามารถนำเทคโนโลยีนี้มาประยุกต์ใช้งานได้ แต่สำหรับกลุ่มเป้าหมายที่ตรงและน่าจะได้รับประโยชน์จากการนำเทคโนโลยี VoIP มาประยุกต์ใช้งานมากที่สุด ได้แก่กลุ่มธุรกิจขนาดย่อม หรือ SME (Small/Medium Enterprise) รวมถึงกลุ่ม ISP (Internet Service Provider) ต่างๆ สำหรับกลุ่มธุรกิจ SME อาจจะต้องเป็นกลุ่มที่มีระบบเครือข่ายข้อมูลของตนเองอยู่แล้ว ไม่ว่าจะเป็นเครือข่าย Leased Line, Frame Relay, ISDN หรือแม้กระทั่งเครือข่าย E1/T1 ก็ตาม รวมถึงมีระบบตู้สาขาโทรศัพท์ในการใช้งานด้วย การนำเทคโนโลยี VoIP มาใช้งานนั้นจะทำให้องค์กรลดค่าใช้จ่ายในการใช้งานการสื่อสารสัญญาณเสียงไปได้อย่างมาก และเนื่องด้วยในปัจจุบันการขยายตัวของระบบเครือข่ายสัญญาณข้อมูล หรือ Data Network มีอัตราการเติบโตที่รวดเร็วกว่าการขยายตัวของเครือข่ายสัญญาณเสียงค่อนข้างมาก จึงทำให้มีการนำเทคโนโลยีที่สามารถนำสัญญาณเสียงเหล่านั้นมารวมอยู่บนระบบเครือข่ายของสัญญาณข้อมูลและมีการรับ-ส่งสัญญาณทั้งคู่ได้ในเวลาเดียวกัน เพื่อเป็นการสะดวกและประหยัดค่าใช้จ่าย ไม่ว่าจะเป็นค่าโทรศัพท์ทางไกลต่างจังหวัด หรือรวมถึงค่าโทรศัพท์ทางไกลต่างประเทศด้วยถ้าหากองค์กรนั้นมีสาขาอยู่ในต่างประเทศด้วย

สำหรับกลุ่มธุรกิจ ISP นั้นสามารถที่จะนำเทคโนโลยี VoIP นี้มาประยุกต์ใช้งานเพื่อเป็นการเพิ่มโอกาสในธุรกิจของตนเองมากยิ่งขึ้น โดยทาง ISP ต่างๆ นั้นสามารถให้บริการ VoIP เพื่อเป็นบริการเสริมเพิ่มเติมขึ้นมาจากการให้บริการระบบเครือข่าย Internet แบบปกติธรรมดา หรือที่เราเรียกว่า Value Added Services ซึ่งถือว่าเป็นการสร้างความแตกต่างและเพิ่มทางเลือกในการให้บริการกับกลุ่มลูกค้าด้วย

2.2.4 เทคโนโลยีและการทำงานของ VoIP

สำหรับมาตรฐานที่มีการใช้งานอยู่บนเทคโนโลยี VoIP นั้น โดยทั่วไปจะมีอยู่ 2 มาตรฐาน ด้วยกัน ได้แก่มาตรฐาน H.323 และมาตรฐาน SIP มาตรฐานเหล่านี้ สามารถเรียกได้อีกอย่างหนึ่งว่า "Call Control Technologies" ซึ่งถือว่าเป็นส่วนประกอบสำคัญสำหรับการนำเทคโนโลยีVoIPมาใช้งาน

H.323 Standard

สำหรับมาตรฐาน H.323 นั้น จริงๆ แล้วไม่ได้ถูกออกแบบมาให้ใช้งานกับระบบเครือข่ายที่ใช้ Internet Protocol (IP) นอกจากนั้นมาตรฐาน H.323 ยังมีการทำงานที่ค่อนข้างช้า โดยปกติแล้วเราจะเสนอการใช้งานมาตรฐาน H.323 ให้กับลูกค้า ก็ต่อเมื่อ ในระบบเดิม ของลูกค้า มีการใช้งาน มาตรฐานH.323 อยู่แล้วเท่านั้น

มาตรฐาน H.323 เป็นมาตรฐานภายใต้ ITU-T (International Telecommunications Union) Standard ในตอนแรกนั้น มาตรฐาน H.323 ได้ถูกพัฒนาขึ้นมาเพื่อเป็นมาตรฐานสำหรับการทำ Multimedia Conferencing บนระบบเครือข่าย LAN เป็นหลัก แต่มาในตอนหลังจึงถูกพัฒนาให้ครอบคลุมถึงการทำงานกับเทคโนโลยี VoIP ด้วย

มาตรฐาน H.323 สามารถรองรับการทำงานได้ทั้งแบบ Point-to-Point Communications และแบบ Multi-Point Conferences อุปกรณ์ต่างๆ จากหลากหลายยี่ห้อ หรือหลายๆ Vendors นั้นสามารถที่จะทำงานร่วมกัน (Inter-Operate) ผ่านมาตรฐานH.323ได้

SIP (Session Initiation Protocol) Standard

มาตรฐาน SIP นั้นถือเป็นมาตรฐานใหม่ในการใช้งานเทคโนโลยี VoIP โดยที่มาตรฐาน SIP นั้นได้ถูกออกแบบมาให้ใช้งานกับระบบ IP โดยเฉพาะ ซึ่งโดยปกติแล้วเราจะแนะนำให้ลูกค้าใหม่ที่จะมีการใช้งาน VoIP ให้มีการใช้งานอยู่บนมาตรฐาน SIP

มาตรฐาน SIP นั้นเป็นมาตรฐานภายใต้ IETF Standard ซึ่งถูกออกแบบมาสำหรับการเชื่อมต่อ VoIP มาตรฐาน SIP นั้นจะเป็นมาตรฐาน Application Layer Control Protocol สำหรับการเริ่มต้น (Creating), การปรับเปลี่ยน (Modifying) และการสิ้นสุด (Terminating) ของ Session หรือการติดต่อสื่อสารหนึ่งครั้ง มาตรฐาน SIP จะมีสถาปัตยกรรมการทำงานคล้ายคลึงการทำงานแบบ Client-Server Protocol เป็นมาตรฐานที่มี Reliability ที่ค่อนข้างสูง

Comparison of H.323 and SIP

H.323	SIP
Complex Protocol	Comparatively Simpler
Binary representation for its messages	Textual representation
Not very modular	Very modular
Not very scalable	Highly scalable
Complex signaling	Simplex signaling
Hundred of Header	37 Headers
Loop Detection is difficult	Loop detection is comparatively easy

รูปที่ 2.24 การเปรียบเทียบระหว่าง H.323 และ SIP

2.2.5 VoIP ทำงานอย่างไร

Conversion to PCM (Pulse Code Modulation)

→ 0110111000101001000101011011001 0

ในขั้นตอนแรกจะเป็นการแปลงสัญญาณ Analog ให้ไปอยู่ในรูปแบบสัญญาณ Digital หรือที่เรียกว่า PCM

Removal of Echo

0110111000101001000101011011001001101001001011

ขั้นตอนต่อไปจะเป็นการมีการแยกสัญญาณออกเป็นส่วนๆ เพื่อทำการตัดสัญญาณ Echo ออก ซึ่งกระบวนการนี้จะถูกจัดการโดย DSP (Digital Signal Processors)

Framing

01101110001	0100100010	10110110010	01101001001

ในส่วนของสัญญาณที่เหลือนั้น ก็จะถูกแบ่งและจัดรูปแบบขึ้นมาใหม่ในรูปของ Frame ซึ่งกระบวนการนี้จะถูกจัดการโดยรูปแบบการบีบอัดที่เรียกว่า CODEC หลังจากกระบวนการนี้แล้ว Frame ของสัญญาณเสียงจะถูกสร้างขึ้น

Packetisation

RTP	01101110001	0100100010	10110110010	01101001001

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

Address and Delivery

IP	UDP	RTP	01101110001	0100100010	10110110010	01101001001

หลังจากที่ได้แปลงสัญญาณให้อยู่ในรูปของ Packet แล้ว ข้อมูลนั้นจะถูกนำมาวิเคราะห์และใส่ค่า IP Address ปลายทาง

Conversion to Analog

01101110001010010001010110110010 

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

Error Correction

กระบวนการนี้จะเป็นกระบวนการที่ใช้ในการตรวจสอบและแก้ไขข้อผิดพลาดซึ่งอาจจะเกิดขึ้นระหว่างการส่งสัญญาณและนำมาซึ่งความผิดเพี้ยนหรือความเสียหายของสัญญาณจนทำให้เราไม่สามารถทำการสื่อสารอย่างถูกต้องได้

ระบบของ VoIP สามารถแบ่งได้เป็น 4 ส่วนคือ

1 Voice Processing module

ทำการสุ่มตัวอย่างสัญญาณเสียงเพื่อส่งผ่านเครือข่าย IP ซอฟต์แวร์นี้โดยทั่วไปทำงานบน DSP (Digital Signal Processing) Voice Processing module จะต้องประกอบด้วยโปรแกรมซึ่งทำหน้าที่ดังต่อไปนี้

1.1 PCM Interface

รับตัวอย่าง (สัญญาณสุ่ม) จาก telephony (PCM) interface และส่งต่อให้กับ VoIP Software module ปฏิบัติการต่อ PCM Interface จะทำการสุ่มตัวอย่างเฟสอีกครั้งจากตัวอย่างที่เป็นผลลัพธ์ของ analog interface ซึ่งจะมีการทำการบีบอัดเพื่อป้องกันสัญญาณรบกวน และทำการแปลงสัญญาณ Analog เพื่อไปเป็น Digital

1.2 Echo Cancellation Unit

เป็นหน่วยกำจัดการสะท้อนของสัญญาณข้อมูลเสียงที่ถูกสุ่มตัวอย่าง และรูปแบบของการสื่อสารเป็นแบบ full duplex ตามมาตรฐานของ ITU G.165 หรือG.168 echo cancellationจำเป็นกรณีที่ความล่าช้า 1รอบของVoIPมีค่ามากกว่า 50 ms

1.3 Voice Activity/Idle Noise Detector

มีหน้าที่ระงับการส่ง Packet เมื่อไม่มีสัญญาณเสียง ทำให้ประหยัดแถบความถี่ ถ้าตรวจจับได้ว่าไม่มีกิจกรรมเกิดขึ้นในช่วงเวลาหนึ่ง ผลลัพธ์ของ voice encoder จะถูกระงับไม่ให้ส่งผ่านเครือข่าย ระดับของเสียงว่างเปล่า (idle noise) จะถูกวัดและแจ้งให้ปลายทางทราบเพื่อที่จะแทรก "comfortable noise" เข้าไปในสายเพื่อไม่ให้คนฟังได้รับสายเงียบในโทรศัพท์

1.4 Tone Detector

ทำหน้าที่ตรวจจับการได้รับ DTMF tones (Dial Tone Multi-Frequency; กลุ่มของ tones ที่ตรงตามมาตรฐานและถูกเขียนทับ ใช้ในสัญญาณโทรศัพท์ซึ่งกำเนิดโดย touch tone pad) และแยกสัญญาณว่าเป็นเสียง หรือ แฟกซ์

1.5 Tone Generator

มีหน้าที่กำเนิด DTMF tones และ call progress tones ภายใต้คำสั่งของระบบปฏิบัติการ(OS)

1.6 Facsimile Processing module

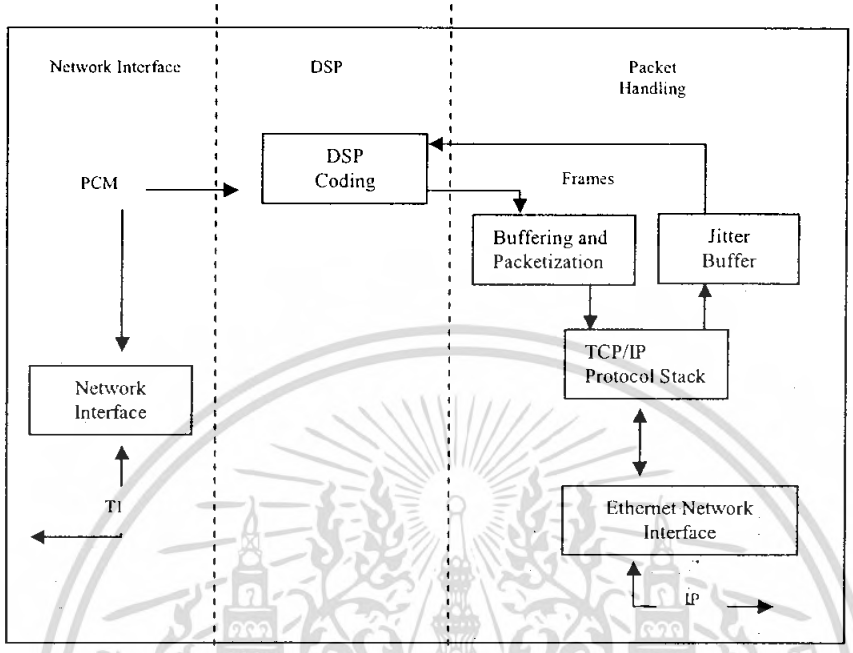
มีหน้าที่ถ่ายถอดแฟกซ์โดย Stimulate สัญญาณ PCM และแยกข่าวสารออกมา และบรรจุข้อมูลที่สแกนแล้วลงใน Packet

1.7 Packet Voice Protocol module

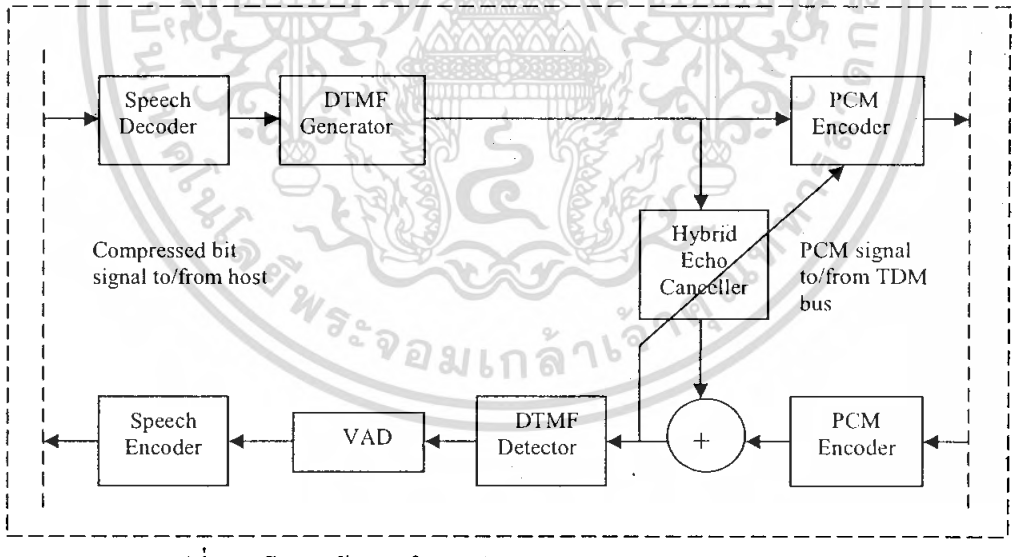
มีหน้าที่รวบรวมสัญญาณเสียงที่ถูกบีบอัด และข้อมูลแฟกซ์ เพื่อส่งผ่านเครือข่ายข้อมูล แต่ละ Packet มีลำดับเลขที่ทำให้ Packet ที่ได้รับถูกส่งเรียงกามลำดับถูกต้อง และสามารถตรวจจับ Packet ที่หายได้

1.8 Voice Playout module

ที่ปลายทาง ทำหน้าที่บัฟเฟอร์ Packet ที่ได้รับ และส่งต่อให้กับเครื่องเข้ารหัสเสียง เพื่อเล่นเสียงออกมา



รูปที่ 2.25 Block diagram ของ Voice Processing Module



รูปที่ 2.26 โครงสร้างภายในตัวประมวลผลสัญญาณดิจิตอล (DSP)

2 The Call Processing module

ทำหน้าที่เป็น signaling gateway ยอมให้มีการสร้าง call ผ่านเครือข่าย Packet ซอฟต์แวร์นี้ support E&M (Ear & Mouth Signaling; สายส่งสัญญาณระหว่าง PBX และ CO ใช้ในการจองสาย, ส่งต่อดิจิต และ เลิกสาย) และ loop, Call Processing module จะตรวจจับสัญญาณเรียกใหม่ที่เกิดขึ้น และเก็บข้อมูลเกี่ยวกับที่อยู่ ทำงานอ้างอิงตาม protocol H.323 มีฟังก์ชันที่ต้องปฏิบัติดังนี้

2.1 ตรวจสอบ interface ที่ต่อกับเครือข่ายโทรศัพท์เพื่อรับคำสั่ง และผลตอบที่จะเข้ามา

2.2 แยกข่าวสารออกมา และสิ้นสุดขั้นตอนการเข้าสัญญาณ (terminate signaling protocols เช่น E&M)

2.3 จัดการกับข่าวสารให้อยู่ในรูปแบบที่สามารถเปิดการประชุม (session) ผ่านเครือข่าย Packet แปลงเบอร์โทรศัพท์เป็น IP address ขั้นตอนการหมุนเรียก (dialing) มี 2 วิธีคือ

(1) single stage หมุนเรียกเบอร์ของปลายทาง และ ใช้วิธีเลือกเส้นทางแบบอัตโนมัติ

(2) two stage หมุนเรียกเบอร์ของ VoIP gateway แล้วหมุนเรียกปลายทางจริง

3 Packet Processing module

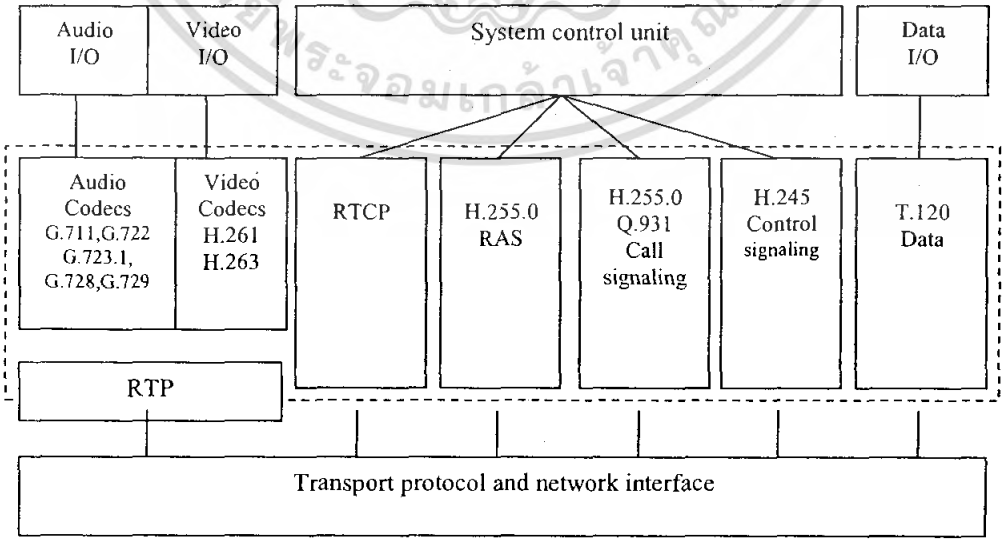
เป็นขั้นตอนการบรรจุสัญญาณข้อมูลเสียงลงใน Packet เพิ่ม transport headers ก่อนส่ง Packet ผ่านเครือข่าย IP (หรือเครือ Packet อื่นๆ) แปลงข่าวสารของสัญญาณจาก telephony protocol เป็น packet signaling protocol

VoIP ทำงานโดยอาศัย protocol ที่ชื่อว่า H.323 ซึ่งเป็นชุดของมาตรฐานที่เกี่ยวกับหลายเรื่องรวมกัน โดยคลอบคลุมทั้งการสื่อสารแบบ จุดต่อจุด และหลายจุดพร้อมๆกัน

(1) Terminal คือ client หรือจุดที่ข้อมูล H.323 ถูกสร้างหรือขึ้น หรือสิ้นสุดการเดินทาง ซึ่งอาจจะเป็น PC หรือว่า เครื่องโทรศัพท์ที่สนับสนุน เครือข่าย IP ซึ่งอาจจะสนับสนุนสัญญาณวีดีโอด้วยก็ได้ Gateway คือ ใช้สำหรับเชื่อมต่อเครือข่ายที่ต่างชนิดกัน เพื่อทำการแปลงชนิดของข้อมูลให้เข้ากันได้กับเครือข่ายที่จะเชื่อมต่อ

(2) Gatekeeper เป็นตัวช่วยบริการต่างๆในแต่ละฝั่งของเครือข่าย ซึ่งมีหน้าที่ในการ แปลง address ระหว่างหมายเลขโทรศัพท์ กับหมายเลข IP , จำกัดการใช้งานของแต่ละ terminal , บริหาร bandwidth และจัดการเกี่ยวกับการหาเส้นทางให้กับ Packet

Multipoint Control Unit (MCU) ใช้ในการติดต่อแบบ หนึ่งจุดกับหลายจุด โดยจะทำการสร้างวงจรเสมือน ขึ้นมา ให้กับ terminal แต่ละตัวที่ทำการสนทนากันอยู่



รูปที่ 2.27 ลำดับชั้นของ H.323 Terminal

4. Network management

จะควบคุมการจัดส่งข้อมูลไปให้ถึงปลายทาง สำหรับการสนทนาด้วยเสียงนั้นจำเป็นอย่างยิ่งที่จะต้องส่งข้อมูลแบบเวลาจริง แต่สำหรับ TCP/IP นั้น ไม่ได้ถูกออกแบบมาให้ทำเช่นนั้นได้ เราทำได้เพียงกำหนดนโยบายเพื่อให้ Packet ของ H.323 ผ่าน router แต่ละตัวไปให้เร็วที่สุด ซึ่งสามารถทำได้ดังนี้

4.1 TOS ซึ่งอยู่ใน header ของ IP Protocol จะถูกกำหนดให้เป็น high เพื่อระบุให้ Packet นั้นเป็น Packet ที่มีความสำคัญสูง ยิ่งให้ความสำคัญสูง Packet ยิ่งใกล้ถูกส่งออกไปใกล้เวลาจริงยิ่งขึ้น

วิธีการจัดแถวคอยของ Packet

1) FIFO (First in First Out) เป็นการส่งต่อ Packet ตามลำดับก่อน-หลัง ซึ่งเป็นวิธีที่ไม่ดีมากนัก

2) WFQ (Weighted Fair Queuing) วิธีนี้จะกำหนดให้มีความเสมอภาคกันของแต่ละ service เพื่อไม่ให้มี service ตัวใดตัวหนึ่งใช้ช่องสัญญาณมากเกินไป

3) CQ (Custom Queuing) วิธีนี้ให้ผู้ใช้งานเป็นผู้กำหนดความสำคัญของ Packet แต่ละชนิดด้วยตัวเอง

4) PQ(Priority Queuing) วิธีนี้จะสร้างแถวคอยขึ้นมามากกว่า 1 แถว ซึ่งแต่ละแถวจะมีความสำคัญที่แตกต่างกัน โดยการส่งต่อ จะเริ่มส่งที่ละแถว เมื่อแถวที่มีความสำคัญสูงสุดหมดแล้ว จึงจะเริ่มส่งแถวที่มีความสำคัญน้อยลงมา ตามลำดับ

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

4.2 ทำการกำหนดขนาด และจำกัด bandwidth ของแต่ละ terminal เพื่อรักษา bandwidth ให้ คงที่อยู่ตลอดเวลา ซึ่งทำได้โดยการ จำกัด Bandwidth ของการ download และการ upload

4.3 มีการตรวจสอบเพื่อป้องกันการคับคั่งของข้อมูล ซึ่งอาจจะใช้วิธี RED (Random Early Detection) เพื่อตรวจสอบ ปริมาณข้อมูล

2.2.6 การใช้ VoIP ให้เกิดประโยชน์

แน่นอนว่าเทคโนโลยีใหม่ย่อมนำสิ่งที่ดีกว่ามาให้เสมอ สำหรับ VoIP ก็เช่นเดียวกัน ประการสำคัญของประโยชน์ที่ได้รับจาก VoIP คงต้องเป็นเรื่องการลดค่าใช้จ่ายในการโทรศัพท์ขององค์กรลง ไม่ว่าจะเป็นการโทรในพื้นที่เดียวกันหรือโทรทางไกล แม้กระทั่งการโทรต่างประเทศ ทั้งโทรภายในองค์กรเองหรือโทรติดต่อกับหน่วยงานอื่นๆหรือลูกค้า ล้วนแล้วแต่ได้รับประโยชน์ในเรื่องค่าใช้จ่ายในการโทรศัพท์ทั้งสิ้น ซึ่งประโยชน์ที่ได้รับจากการนำ VoIP มาใช้อาจสรุปประเด็นเป็นข้อๆ ได้เช่น

1. ลดค่าใช้จ่าย (Cost Savings) ในการติดต่อสื่อสารทางโทรศัพท์ลง เนื่องจากเสียงได้ถูกเปลี่ยนให้อยู่ในรูปแบบเดียวกับข้อมูล จึงทำให้สามารถส่งสัญญาณเสียงไปในเครือข่าย LAN หรือ WAN ได้เลย ไม่ต้องผ่านเครือข่าย PSTN ที่มีค่าใช้จ่ายสูงกว่า

2. เพิ่มความยืดหยุ่นในการติดต่อสื่อสารให้กับองค์กร เช่น ในสาขาหรือ -Site งานชั่วคราว สามารถนำ VPN ร่วมกับ VoIP ประกอบกันเพื่อสร้างระบบการติดต่อสื่อสารเต็มรูปแบบภายในองค์กรได้อย่างง่ายดายและรวดเร็ว

3. จัดการระบบเครือข่ายได้ง่ายขึ้น เนื่องจากเครือข่ายการติดต่อสื่อสารทั้งหมด สามารถยุบรวมกันให้เหลือเพียงเครือข่ายเดียวได้ อีกทั้งในกรณีที่มีการโยกย้ายของหน่วยงานหรือพนักงาน การจัดการด้านหมายเลขโทรศัพท์และอื่นๆ สามารถทำได้โดยไม่จำเป็นต้องเดินสายสัญญาณใดๆขึ้นมาใหม่

4. รองรับการขยายตัวของระบบในอนาคต หากในอนาคตองค์กรขยายตัวใหญ่ขึ้น VoIP สามารถรองรับผู้ใช้งานได้เพิ่มมากขึ้นในทันทีโดยการเพิ่ม "Virtual" User เข้าไปในระบบเท่านั้นเอง

5. ลดค่าใช้จ่ายในการดูแลและจัดการระบบ (Reduce Operating Expenses) เนื่องจากใช้ซอฟต์แวร์ในการจัดการ ทำให้ VoIP นั้นง่ายในการจัดการและบำรุงรักษา

6. เพิ่มประสิทธิภาพการทำงาน (Increase Productivity) พนักงานสามารถส่งเอกสารผ่านเครือข่ายควบคู่ไปกับการสนทนา หรืออาจจัดการประชุมออนไลน์ (Conference Call) ทั้งภาพและเสียง และแม้กระทั่งส่งเอกสารการประชุมให้กับผู้เข้าร่วมประชุมผ่านทางเครือข่ายได้อีกด้วย

7. ใช้ร่วมกับการสื่อสารไร้สายได้ ทำให้อุปกรณ์สื่อสารไร้สายต่างๆ เช่นโทรศัพท์มือถือหรือ PDA สามารถติดต่อผ่าน VoIP เข้ามาในเครือข่ายขององค์กรได้

8. เพิ่มประสิทธิภาพในการติดต่อกับลูกค้า (Improved Level of Services) โดยใช้ความสามารถของแอพพลิเคชั่นต่างๆ ของ VoIP เช่น "Click-to-talk" เพื่อเพิ่มความสะดวกและรวดเร็วในการติดต่อกับลูกค้า

2.2.7 ตัวอย่าง Application การใช้งานเทคโนโลยี VoIP

1. PBX to PBX Connection

ทั้ง 2 ฝั่งของสำนักงานจะสามารถใช้งานตู้สาขา PBX ของสำนักงานอีกฝั่งเปรียบเสมือนตู้สาขา PBX ของฝั่งตัวเอง ผู้ใช้ภายในไม่จำเป็นต้องทำการ Dial-out ออกไปบนระบบโทรศัพท์ PSTN เพื่อทำการเชื่อมต่อเข้ากับตู้สาขา PBX ของสำนักงานอีกฝั่ง

2. Long Line PBX Extension

เป็นการเชื่อมต่อที่สำนักงานใหญ่ขยายการเชื่อมต่อตู้สาขา PBX ไปที่สำนักงานสาขาที่ไม่มีตู้ PBX ใช้งานอยู่ โดย ทางสำนักงานสาขาสามารถใช้งานตู้ PBX ผ่านทางสำนักงานใหญ่ได้เสมือนกับเป็นตู้สาขา PBX ของฝั่งตนเอง

3. Teleworker / Local Access

เป็นการเชื่อมต่อที่ยินยอมให้ Remote User ฝั่งสำนักงานใหญ่สามารถใช้งานโทรศัพท์เข้ามาที่สำนักงานใหญ่ แล้วใช้ระบบเครือข่ายของสำนักงานใหญ่เชื่อมต่อไปยังสำนักงานสาขาผ่านเทคโนโลยี VoIP เพื่อสามารถใช้งานโทรศัพท์ในพื้นที่ของสำนักงานสาขาได้โดยเสียค่าบริการในอัตราของพื้นที่ของสำนักงานสาขานั้นๆ

4. Service Provider CPE

ผู้ให้บริการต่างๆ เช่น ISP สามารถที่จะเสนอบริการเสริมต่างๆ ทางด้าน VoIP บนระบบเครือข่ายความเร็วสูงที่มีการใช้งานอยู่เดิมแล้ว

2.2.8 อนาคตของ และแนวโน้มของ VoIP

Voice over IP เกิดขึ้นพร้อมๆ กับการให้บริการอินเทอร์เน็ต และได้กลายเป็นบริการยอดนิยมของผู้ที่เชี่ยวชาญด้านคอมพิวเตอร์ และนักศึกษา ซึ่งมีเวลาแต่ไม่มีเงิน เมื่อไม่นานมานี้ และในปัจจุบัน Voice over IP ก็กำลังได้รับความนิยมจากผู้ใช้เพิ่มมากขึ้นเรื่อยๆ การไม่สามารถเปิดให้บริการโทรศัพท์ด้วยเสียงผ่านอินเทอร์เน็ตจากเครือข่ายที่มีอยู่เดิม อาจทำให้ผู้ให้บริการ เช่น เวอริซอน, เอสบีซี และเบลล์เซาธ์ ต้องสูญเสียส่วนแบ่งในตลาดโทรคมนาคมมูลค่า 200,000 ล้านดอลลาร์ได้ เนื่องจาก เมื่อใช้ Voice over IP ลูกค้ามีอิสระในการใช้เครือข่ายของผู้ให้บริการเดิม หรือจะเปลี่ยนผู้ให้บริการใหม่ อย่างเช่น บริษัทผู้ให้บริการทีวีตามสาย (เคเบิล ทีวี) หรือธุรกิจเกิดใหม่ อย่าง Net2Phone และ Vonage ได้ ประกอบกับ การใช้งาน Voice over IP ไม่จำเป็นต้องโทรศัพท์ผ่านพีซีที่ใช้ไมโครโฟนเป็นอุปกรณ์เสริมอีกต่อไป แม้ว่าอุปกรณ์ดังกล่าว กำลังจะกลับมาอีกครั้งตามกระแสนิยมบริการ อย่าง Skype ซึ่งพัฒนาขึ้นโดยอาศัยสถาปัตยกรรมของคาซา และทำให้การโทรศัพท์แบบพีซีกับพีซีง่ายขึ้น ขณะที่คิดค่าธรรมเนียมเหมือนโทรศัพท์ทั่วไป คือ เพียง 100 ดอลลาร์เท่านั้น นับตั้งแต่เปิดตัวไปเมื่อเดือนเมษายนที่ผ่านมา โวเนจ

ผู้ให้บริการ Voice over IP ชั้นนำ สามารถดึงดูดให้ลูกค้า 85,000 คน จ่ายค่าบริการ 15 - 35 ดอลลาร์ต่อเดือน

เมื่อเร็วๆนี้ บริษัท นีเมอร์เทส รีเสิร์ช ในชิคาโก ทำสำรวจ 42 บริษัท ซึ่งคิดเป็น 70% ของบริษัทที่มีรายได้มากกว่า 1,000 ล้านดอลลาร์ และพบว่า ประชาชนเกือบ 2 ใน 3 ใช้โทรศัพท์ผ่านอินเทอร์เน็ต ขณะที่อีก 20% ที่เหลือ กำลังทดลองใช้เทคโนโลยีดังกล่าว จึงไม่แปลกใจว่าทำไมเมื่อเดือนธันวาคมที่ผ่านมา เอที แอนด์ ที, เควสต์, คอกซ์ คอมมิวนิเคชันส์, และไทม์ วอร์เนอร์ เทเลคอม จึงตบเท้าทยอยเปิดตัวบริการ Voice over IP ของตัวเอง

Voice over IP สร้างความตื่นเต้นให้กับลูกค้า นางแคธี มาร์ติน รองประธานอาวุโสเอที แอนด์ ที ผู้ซึ่งผลักดันให้บริการโทรศัพท์ผ่านอินเทอร์เน็ต ของมา เบลล์ กลายเป็นบริการยอดนิยม 100 อันดับแรกในตลาดผู้บริโภคทั่วไปและองค์กรธุรกิจของสหรัฐ กล่าว พร้อมเสริมว่า คำว่า แจ๋ว ไม่ได้ถูกนำมาใช้ในภาคโทรคมนาคมเลย นับตั้งแต่การมาถึงของโทรศัพท์ในทศวรรษ 1950 เป็นต้นมา แต่ความยืดหยุ่นของโทรศัพท์ผ่านอินเทอร์เน็ต อาจทำให้ผู้ใช้ต้องอุทานคำดังกล่าวเพื่อแสดงออกถึงความพอใจในการใช้งาน

ขณะที่นายเดวิด ไอเซนเบิร์ก ที่ปรึกษาด้านโทรคมนาคมอิสระ ขยายความเรื่องความยืดหยุ่นของบริการ Voice over IP ไว้ว่า โทรศัพท์ผ่านอินเทอร์เน็ต ทำงานบนมาตรฐานเปิด จึงแตกต่างจากเครือข่ายโทรศัพท์พื้นฐาน ที่ต้องถูกควบคุมอย่างเข้มงวดและเสียค่าใช้จ่ายสูงในการเพิ่มลูกเล่นใหม่ด้วย VoIP คุณสามารถพัฒนาฟังก์ชันใหม่ได้เร็วเท่ากับการเขียนโปรแกรม นายไอเซนเบิร์ก ซึ่งร่วมงานกับเบลล์ แลบส์ของเอที แอนด์ ที มากว่า 12 ปี กล่าว

ในปัจจุบันการส่งสัญญาณเสียงกับข้อมูล จะถูกส่งผ่านโครงข่ายที่แยกจากกัน แต่แนวโน้มของการสื่อสารโทรคมนาคมในอนาคตอันใกล้นี้ จะเป็นลักษณะการรวมบริการหลายๆ อย่างไว้ในโครงข่ายเดียว ซึ่งสามารถให้บริการได้ทั้งสัญญาณเสียง, ข้อมูล, ภาพ ภายใต้โครงข่าย แบบแพ็คเกจ โดยการส่งข้อมูลทั้งสัญญาณภาพ และเสียงเป็นชุดของข้อมูล ที่สัญญาณเสียง จะถูกแปลงเป็นข้อมูล ก่อนที่จะถูกส่งในโครงข่าย โดยใช้ไอพีโปรโตคอล (Internetworking Protocol: IP) ซึ่งกำลังเป็นสิ่งที่ได้รับ ความสนใจเป็นอย่างมาก ทั้งในส่วนขององค์กร ธุรกิจ และผู้ให้บริการโครงข่ายหลายราย ส่วนสิ่งที่ผลักดันให้ VoIP ภายใต้ ไอพี เทเลโฟนนี่ (IP Telephony) เป็นที่ต้องการทางด้านการตลาด คือ

ประการแรก โอกาสที่จะติดต่อ สื่อสารระหว่างประเทศ โดยผ่านเครือข่ายอินเทอร์เน็ต หรืออินทราเน็ต โดยมีราคาที่ถูกกว่าโครงข่ายโทรศัพท์ทั่วไป

ประการ 2 การพัฒนารูปแบบการสื่อสารใหม่ๆ เพิ่มขึ้นในปัจจุบัน โดยที่ส่วนหนึ่งถูกพัฒนาขึ้นให้สามารถใช้งานในVoIPทำให้สามารถติดต่อสื่อสารได้กว้างไกลมากขึ้น

ประการ 3 การเป็นที่ยอมรับ และรับเอาคอมพิวเตอร์เข้ามาใช้ในชีวิตประจำวัน ในช่วง 10 ปีที่ผ่านมาอย่างมากมาย รวมทั้งการเพิ่ม จำนวนขึ้นของผู้ใช้งานอินเทอร์เน็ตในปัจจุบัน เป็นส่วนหนึ่งที่ทำให้ VoIP ได้รับความนิยมในการติดต่อสื่อสาร

ประการ 4 มีการใช้ประโยชน์จากระบบ Network ที่มีการพัฒนาให้ดียิ่งๆ ขึ้นไปในปัจจุบัน ให้สามารถใช้งานได้ทั้งในการส่งข้อมูลและเสียงเข้าด้วยกัน

ประการ 5 ความก้าวหน้าทางด้านการประมวลผลของคอมพิวเตอร์ ช่วยลดต้นทุนในการสร้าง

เครือข่ายของ VoIP ในขณะที่ ความสามารถ การให้บริการมีมากขึ้น ส่งผลให้ธุรกิจต่างๆ เข้ามาร่วมใน VoIP มากขึ้น

ประการ 6 ความต้องการที่จะมีหมายเลขเดียวในการติดต่อสื่อสารทั่วโลก ทั้งด้านเสียง, แฟกซ์ และข้อมูล ถึงแม้ว่าบุคคลนั้น จะย้ายไปที่ใด ก็ตามก็ยังคงสามารถใช้หมายเลขเดิมได้ เป็นความต้องการของผู้ใช้งานและธุรกิจ

ประการ 7 การเพิ่มขึ้นอย่างมากมายของการทำรายการต่างๆ บน e-Commerce ในปัจจุบัน ผู้บริโภคต่างก็ต้องการการ บริการที่มีคุณภาพ และมีการโต้ตอบกันได้ระหว่างที่กำลังใช้ อินเทอร์เน็ตอยู่ ซึ่ง VoIP สามารถเข้ามาช่วยในส่วนนี้ได้

ประการ 8 การเติบโตอย่างรวดเร็วของ Wireless Communication ในปัจจุบัน ซึ่งผู้ใช้ในกลุ่มนี้ต้องการ การติดต่อสื่อสาร ที่ราคาถูกลง แต่มีความยืดหยุ่นในการใช้งาน ดังนั้น ตลาดกลุ่มนี้ถือว่า เป็นโอกาสของ VoIP

จากอดีตมีการส่งข้อมูลผ่านโครงข่ายวงจรของชุมสายโทรศัพท์ (Circuit Switching) ทำให้เกิดการใช้งานโครงข่ายได้ ไม่เต็มประสิทธิภาพ มากเท่าที่ควร เพราะแต่ละวงจร หรือเส้นทางถูกกำหนดให้ผู้ใช้เพียงคนเดียวเท่านั้น แม้ว่าวงจร หรือเส้นทางนั้นๆ จะว่างอยู่ก็ตาม แต่ในปัจจุบันเริ่มมีการใช้งานแบบแพ็คเกจสวิตชิ่ง (Packet Switching) มากขึ้น โดยการแบ่งข้อมูลที่จะส่งออกเป็นแพ็คเกจย่อยๆ และทำการส่งไปตามเส้นทางต่างๆ กัน อันเป็นการกระจายทราฟฟิก (Traffic) ทั้งหมดในโครงข่ายให้ใช้งานได้อย่างเต็มประสิทธิภาพ ทำให้โครงข่ายมีความยืดหยุ่นและคล่องตัวมากขึ้น ซึ่งหลักการของแพ็คเกจ สวิตชิ่งนี้ได้นำมาใช้เป็น Voice Over Packet เนื่องจากมีการปรับปรุง การทำงาน (Performance) บน Packet Switching ทำให้ Performance per Cost ของ Packet Switching ในอนาคตดีกว่า Circuit Switching

ทิศทางของการใช้บริการโทรศัพท์แบบเสียง มีแนวโน้มของการเจริญเติบโตค่อนข้างต่ำ ในขณะที่อัตราการเจริญ เพิ่มของการ ใช้โทรศัพท์แบบข้อมูลมีการเติบโตอย่างรวดเร็ว อันเนื่องจากการใช้งานที่แพร่หลายในทั่วโลกและนับจากที่เทคโนโลยีอินเทอร์เน็ตได้พัฒนามา

2.3 IP-PBX

IP-PBX เป็นอุปกรณ์ที่ใช้ในการเชื่อมโยง, ควบคุม และทำหน้าที่หลักของตู้ชุมสายโทรศัพท์ (เช่นระบบ Voicemail, IVR, Auto-Attendant) ในการสื่อสารทางเสียงผ่านระบบเครือข่าย intranet หรือ internet

2.3.1 ประโยชน์และข้อดี

1. ง่ายต่อการติดตั้ง, เนื่องด้วยการทำงานของ IP-PBX นั้น ต้องทำงานบนระบบ network ฉะนั้นจึงไม่จำเป็นต้องเดินสายโทรศัพท์เพิ่มเติม อีกทั้งยังสามารถทำการ ย้ายเครื่องโทรศัพท์ไปยังตำแหน่งใดๆก็ได้ที่อยู่บนระบบเครือข่ายเดิมโดยไม่ต้องเปลี่ยนแปลงค่าอะไรเลยบนเครื่องโทรศัพท์และระบบเครือข่าย

หากมีระบบ wireless-lan อยู่ในระบบเครือข่ายก็ยังสามารถเชื่อมต่อกับระบบ wireless ที่มีอยู่ได้โดยง่าย (wifi phone)

2. การเพิ่ม Phone ทำได้โดยง่าย เนื่องด้วยทำงานบนระบบ network ฉะนั้นการเพิ่มหัวเครื่องโทรศัพท์จึงเหมือนการติดเครื่อง PC ใหม่ในระบบเท่านั้น จะไม่ตายตัวกับจำนวนพอร์ทบนตู้ชุมสายเหมือนในระบบ legacy-PABX ทั้งนี้การเพิ่มเติมขึ้นอยู่กับเครื่อง IP-PBX ด้วยว่าสามารถรองรับการทำงานได้เพียงพอหรือไม่

3. ประโยชน์ของระบบ Internet และ intranet ระบบ IP-PBX ได้รับประโยชน์โดยตรงจากระบบเครือข่าย คือ หากมีการเชื่อมโยงระบบเครือข่ายเข้าด้วยกันแล้วนั้น ไม่ว่าเครื่องโทรศัพท์จะอยู่ในที่แห่งใดๆในระบบ ก็เสมือนว่าอยู่ในระบบโทรศัพท์เดียวกัน การโทรศัพท์จึงเป็นไปได้โดยง่าย และ ไม่มีค่าใช้จ่ายในการโทรศัพท์บนระบบ IP-PBX เดียวกันไม่มีจะอยู่ในที่ใดๆก็ตาม

4. รอบรับระบบ Video Call, สามารถรองรับการโทรศัพท์แบบเห็นภาพได้ทันทีหากมีอุปกรณ์ที่รองรับในทั้งสองคู่สนทนา

5. รองรับการเชื่อมต่อกับระบบ Database, ระบบ Computer เนื่องด้วย IP-PBX ส่วนใหญ่เป็น software ฉะนั้นการเพิ่มเติม feature ต่างๆ จึงเป็นไปได้โดยง่าย ฉะนั้น Application ต่างๆที่เป็นไปไม่ได้หรือเป็นไปได้ยากบนระบบ legacy-pbx จึงสามารถทำได้บนระบบ IP-PBX

6. การ Maintenance สามารถทำได้ง่ายกว่าระบบ legacy-pabx ทั่วไปในกรณีที่ IP-PBX นั้นๆ ทำงานบน server

7. รองรับระบบ High Availability เพื่อลดเวลาที่ระบบจะเกิดปัญหาและต้องหยุดให้บริการ

8. สามารถเชื่อมต่อให้กับผู้ให้บริการ VoIP-Operator ได้โดยตรงเพื่อทำให้สามารถโทรศัพท์ไปยังระบบโทรศัพท์ได้ในราคาที่ประหยัดกว่ามาก

9. รองรับอนาคตสามารถทำงานร่วมกันในทั้งระบบ Voice/data/Video

2.3.2 ข้อด้อยหรือสิ่งที่จะต้องมีเพิ่มเติมในระบบ

1. ราคาอุปกรณ์ที่สูงกว่าระบบเดิมๆ

2. จำเป็นต้องมีระบบเครือข่าย

3. จำเป็นต้องมีการ config ระบบเครือข่ายเพิ่มเติมในกรณีที่มี ข้อมูลวิ่งอยู่บนระบบมากๆเพื่อทำให้มั่นใจว่าคุณภาพเสียงจะไม่มีปัญหา

4. จำเป็นต้องใช้ไฟในทุกหัวเครื่องโทรศัพท์ ฉะนั้นอาจมีปัญหาในกรณีที่มีไฟฟ้าดับ ซึ่งแก้ปัญหาได้โดยใช้อุปกรณ์เครือข่ายที่สามารถจ่ายไฟฟ้าไปยังหัวเครื่องได้

2.4 Asterisk

2.4.1 ระบบ Asterisk คืออะไร และทำงานอย่างไร

Asterisk คือ opensource software ที่ทำหน้าที่หลักเป็น Softswitch, IP-PBX หรือที่เรียกว่าตู้ชุมสายโทรศัพท์ระบบ IP ซึ่งมีหน้าที่ในการควบคุมและจัดการบริหาร การเชื่อมต่อ ระหว่างอุปกรณ์โทรศัพท์ผ่านเครื่องข่ายเนทเวอร์ค อีกทั้งยังสามรถเพิ่มเติมประสิทธิ์ภาพและความสามารถในการทำงานได้โดยง่าย

2.4.2 ความสามารถของ Asterisk

1. Switch (PBX) ตู้ชุมสาย

Asterisk สามารถทำหน้าเป็นอุปกรณ์สลับสายโทรศัพท์ไม่ว่าจะเป็นระบบ IP หรือ hybridge, สามรถทำการตั้งค่าเส้นทางการของการโทรศัพท์โดยตัวเอง, สามารถเพิ่มเติม feature ได้เช่น (ระบบ Voicemail, IVR), รองรับการเชื่อมต่อกับระบบโทรศัพท์พื้นฐานไม่ว่าจะเป็นแบบ analog หรือ digital (ISDN)

2. Gateway

สามารถทำหน้าเป็นอุปกรณ์ที่ใช้ในการเชื่อมต่อระหว่าระบบโทรศัพท์พื้นฐานกับระบบ VoIP

3. Feature & Media Server

อีกความสามารถของ Asterisk คือสามารถทำเป็น ระบบตอบรับหรือระบบการประชุมทางโทรศัพท์ เพื่อให้ทำงานเข้ากับระบบโทรศัพท์ที่มีอยู่เดิม ได้อีกด้วย

ตัวอย่างการ Implementation เช่น สามารถทำเป็น IVR หรือระบบตอบรับ ให้กับตู้ชุมสาย (pabx) เดิมที่ไม่มีระบบตอบรับ

4. Call Center

รองรับการทำงานของระบบ Call-Center อย่างเต็มรูปแบบ เช่น ACD, Queue, IVR, Skill-based routing

2.4.3 จะเริ่มใช้งาน Asterisk ต้องมีอะไรบ้าง

การเริ่มใช้งาน Asterisk เริ่มจากการหาข้อมูลของระบบ asterisk ให้ตรงกับความต้องการใช้งานที่จะเกิดขึ้นในอนาคต ทั้งนี้ยังขึ้นอยู่กับการดูแลรักษาระบบ ซึ่งเป็นส่วนสำคัญของการใช้งาน open source software โดยทั่วๆไป

ซึ่งหากมีการใช้งานที่ไม่มากนักหรือไม่มีความสำคัญมากอาจทำการทดลองและใช้งานได้โดยตัวเองหรือผู้ดูแลระบบในบริษัท แต่หากว่าต้องการใช้งานในส่วนที่มีความสำคัญมาก การใช้ที่ปรึกษาหรือบริษัทภายนอกที่มีประสพการณ์มาจัดการติดตั้งระบบให้จะดูเป็นการเหมาะสมกว่า

สำหรับมือใหม่ asterisk ควรเริ่มต้นการ software รวมหรือ free IP-PBX software ที่ได้มีการรวมระบบ asterisk พร้อมทั้งระบบจัดการต่างๆ สำหรับระบบ asterisk อยู่ในชุดเดียวกันซึ่งเป็นซึ่งที่ง่ายที่สุดในการเริ่มต้นการใช้งาน ซึ่งสิ่งที่จำเป็นสำหรับระบบ asterisk มีดังนี้

1. Software
2. Computer/Server
3. การ์ดสายนอก
4. softphone หรือ เครื่อง ip-phone

Software-Trixbox

Trixbox หรือ Asterisk@Home เป็นชุด software ที่มีการรวม application ต่างๆที่จำเป็นต่อระบบ asterisk ไว้เป็นจำนวนมาก ซึ่งสามารถนำมาใช้งานที่บ้านหรือในองค์กรณ์เป็น IP-PBX อย่างเต็มรูปแบบ ได้ทันที ทั้งนี้การติดตั้งก็มีความง่ายดาย และใช้เวลาติดตั้งไม่เกิน 2 ชั่วโมง ก็จะได้ เครื่อง IP-PBX แบบ full-feature ที่สามารถนำมาใช้งานได้จริงทันที

Trixbox ได้มีการรวม software คร่าวๆดังนี้

1.1 trixbox dashboard
1.2 โปรแกรม Asterisk
1.3 โปรแกรมสำหรับการตั้งค่าผ่านเวป "FreePBX"
1.4 โปรแกรม CRM "SugarCRM"
1.5 Munin
1.6 โปรแกรมแสดงสถานะการใช้งาน HUDLite
1.7 โปรแกรม IVRGraph
1.8 โปรแกรม phpMyAdmin
1.9 โปรแกรม Webmi

Software-AsteriskNOW

AsteriskNOW เป็น software สำเร็จรูปของผู้พัฒนาระบบ asterisk โดยมาพร้อมกับ web-interface และการติดตั้งที่ง่าย ซึ่งการใช้งานอาจดูง่ายกว่า Trixbox เนื่องจากการติดตั้งนั้นมาพร้อมกับ software ที่จำเป็นเท่านั้น

Computer/Server

เครื่อง Computer ที่จะนำมาใช้งานกับ asterisk ได้นั้นต้องเป็นเครื่องที่สามารถลงระบบปฏิบัติการ Linux ได้เท่านั้น อีกทั้งยังต้องรองรับการทำงานกับการ์ดสายนอกอีกด้วย

ความสามารถของเครื่องที่จะนำมาใช้งานขึ้นอยู่กับหลายปัจจัยเช่น

1. จำนวน Extension หรือ จำนวนเครื่อง VoIP phone ที่จะมาเชื่อมกับระบบ
2. Codec หรือ การเทคนิคการบีบอัดข้อมูลเสียงที่จะนำมาใช้งาน
3. Application ต่างๆที่จะใช้งาน เช่น conference, Voicemail, Voice Recorder etc.

ซึ่งในเบื้องต้น เราสามารถนำ Computer เก่าที่ไม่ได้ใช้งานแล้วมาใช้งานในช่วงแรกก่อนก็เป็นได้ โดย เครื่องระดับ celeron466 ก็สามารถรองรับการใช้งานในองค์กรหรือบ้านที่มีผู้ใช้งานได้ราว 10 คนแล้ว

การ์ดสายนอก

การจะทำให้ Asterisk สามารถคุยกับระบบโทรศัพท์ได้จริงนั้น จำเป็นต้องติดตั้ง การ์ดโทรศัพท์สายนอก หรือที่เรียกว่า FXO พอร์ดการ์ด ซึ่งใช้ในการเชื่อมต่อกับสายโทรศัพท์ที่มาจาก True, Tot, หรือ TT&T เพื่อที่จะให้ asterisk นั้นสามารถโทรศัพท์ออกไปยังที่อื่นๆได้

การ์ดสายนอกนั้นมีหลากหลายยี่ห้อ และ หลากหลายคุณสมบัติ แต่สำหรับการเริ่มต้นหรือการทดลองใช้งานอาจเริ่มต้นการ การ์ด 1 พอร์ทที่มีราคาไม่สูงมากก่อนก็เป็นได้

ซึ่งการ์ดสายนอกที่คุณภาพดี ราคาไม่สูงมากและติดตั้งได้ง่ายกับระบบ Asterisk มีเช่น card x100P compatible

softphone หรือ เครื่อง ip-phone

เครื่อง IP-PHONE สำหรับการ ลองใช้งานระบบ asterisk นั้นถ้าต้องการให้รองรับการใช้งาน IAX2 หรือ โปรโตคอลของ asterisk ที่มีความสามารถบางอย่างที่เหนือกว่า SIP ด้วยนั้น อาจจะขอแนะนำเป็นเครื่องโทรศัพท์ที่สามารถใช้งานได้กับทั้ง SIP และ IAX2 ซึ่งในท้องตลาดนั้นมีอยู่หลายยี่ห้อ แต่ที่มีขายในประเทศไทยจะเป็นของ ATCOM หรือ PLEXTEL ซึ่งอาจเป็นรุ่น AT-320 หรือ AT-530 ก็ได้โดย AT-320 นั้นเป็นรุ่นที่เก่ากว่า AT-530 โดยมีคุณภาพเสียงต่ำกว่า AT-530 แต่หากใช้แค่ test ระบบ AT-320 ก็ใช้งานได้แล้วในราคาที่ประหยัดกว่า

2.5 การแลกเปลี่ยนข้อมูลผู้ใช้งานด้วยคุ๊กกี้ (cookie)

คุ๊กกี้ เป็นวิธีการที่เราฝังข้อมูลขนาดเล็กๆ (ในรูปแบบแฟ้มข้อมูลขนาดไม่เกิน 4 KB) ไว้ในเครื่องของผู้ใช้งาน โดยข้อมูลที่ฝังอยู่ก็คือ ข้อมูลที่แลกเปลี่ยนกัน ผลัดกันอ่าน ผลัดกันเขียนข้อมูลนี้ได้

สำหรับคุ๊กกี้แต่ละตัวจะมีลักษณะการเก็บข้อมูลที่ประกอบด้วย 3 ส่วนหลักคือ

CookieName	คือ ชื่อ Cookie
Value	คือ ค่าของข้อมูลที่ Cookie เก็บ
ข้อมูลประกอบอื่นๆ	เช่น เวลาหมดอายุ ข้อมูลเกี่ยวกับ Host และ Path

สำหรับหลักการทำงานของ Cookie มีรายละเอียดดังนี้

รูปที่ 2.32 หลักการทำงานของ Cookie

1. เมื่อผู้ใช้งานเปิดหน้าเว็บไซต์ เว็ปบราวเซอร์จะร้องขอไฟล์เว็บเพจไปที่ server
2. Server จะส่งหน้าเว็บเพจกลับมาพร้อมกับส่งตัวแปร Cookie สำหรับเก็บข้อมูลเข้ามาเก็บที่คอมพิวเตอร์ของผู้ใช้งาน
3. เมื่อผู้ใช้งานมีการใช้งานเว็บเพจ เช่น กรอกข้อมูลผ่านฟอร์ม ก็จะมีการนำข้อมูลมาเก็บไว้ใน Cookie
4. เมื่อ Server ต้องการข้อมูลจากผู้ใช้ Server ก็จะไปอ่านมาจาก Cookies ที่อยู่ในเครื่องของผู้ใช้นำไปใช้

บทที่ 3

การคำนวณและการสร้าง

3.1 ขั้นตอนการออกแบบ

3.1.1 การติดตั้งและปรับแต่งการ์ด X100P

ติดตั้งการ์ดลงในเครื่อง Server และทำการปรับแต่งค่าดังนี้

ไฟล์ zaptel.conf

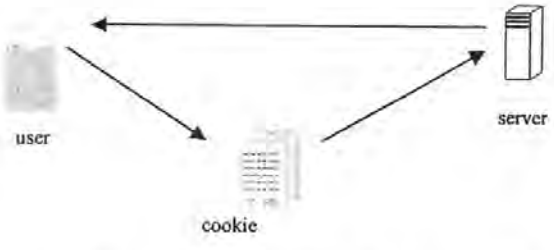
```
fxsks=1
loadzone=us
defaultzone=us
```

ไฟล์ zapata.conf

```
[channels]
    context=default
    echocancel=yes        (บรรทัดนี้เป็นการแก้ไขปัญหาเสียง echoที่เกิดขึ้น)
    echocancelwhenbridged=yes
    signaling=fxs_ks
    busydetect=yes
    busycount=4
    channel=>1
```

3.1.2 การออกแบบ script ทางด้านฝั่งผู้ใช้งานเพื่อส่งข้อมูลไปยังเซริฟเวอร์

ในการออกแบบ script ในการใช้งาน ใช้หลักการของการแลกเปลี่ยนข้อมูลด้วย Cookie ซึ่งเป็นวิธีการเขียนข้อมูลที่ต้องการติดต่อลงไป และทำการผลัดกันอ่านเขียนข้อมูลนี้ได้



รูปที่ 3.1 ขั้นตอนการแลกเปลี่ยนข้อมูลแบบ Cookie

Script ที่เขียนใช้ภาษา pHp ในการเขียน

```
<a href=logout.php>Clear Extension Info</a><br>
<?
if (!isset($_COOKIE['extension_info']))
{
echo $_COOKIE['extension_info'];
?>
   <body>
   <form method="POST" action="login.php">
   <h1>Enter your Extension Number</h1>
      <table border="0" width="auto">
      <tr>
       <td width="33%">Extension</td>
       <td width="33%"><input type="text" name="exten" size="20"></td>
       <td width="34%"><input type="hidden" name="number" value=<? echo $_REQUEST['number'];?>> </td>
      </tr>
     </table>
   <p><input type="submit" value="Submit" name="sub">
   <input type="reset" value="Reset" name="res"></p>
   </body>
   </form>
 <?php  }
else
{
 //Cookie is set and display the data
   $extension_info = explode("-", $_COOKIE['extension_info']);  //Extract the Data
   $name = $extension_info[0];
  //exit;
}

#ip address that asterisk is on.
$strHost = "127.0.0.1";

#specify the username you want to login with (these users are defined in /etc/asterisk/manager.conf)
#this user is the default AAH AMP user; you shouldn't need to change, if you're using AAH.
$strUser = "admin";

#specify the password for the above user
$strSecret = "amp111";

#specify the channel (extension) you want to receive the call requests with
#e.g. SIP/XXX, IAX2/XXXX, ZAP/XXXX, etc
$strChannel = $_COOKIE['extension_info'];

#specify the context to make the outgoing call from.  By default, AAH uses from-internal
#Using from-internal will make your outgoing dialing rules apply
$strContext = "from-internal";

#specify the amount of time you want to try calling the specified channel before hangin up
$strWaitTime = "30";

#specify the priority you wish to place on making this call
$strPriority = "1";
```

ตัวอย่าง Script ที่ใช้ (ดูเพิ่มที่ภาคผนวก)

3.2 ขั้นตอนการทดลอง

1. การทดสอบการ์ด ที่ command line เสั่งคำสั่ง ztcfg –v แล้วระบบจะแจ้งว่าพบการ์ดแล้วกี่ Channels
2. ทดสอบการรันชุดคำสั่ง เพื่อทดสอบการทำงาน

บทที่ 4

การทดลองและผลการทดลอง

4.1 ผลการทดลองต่อการ์ด X100P

หลังจากต่อเรียบร้อย ระบบจะแจ้งว่าพบการ์ดแล้ว 1 Channel (FXO Port)

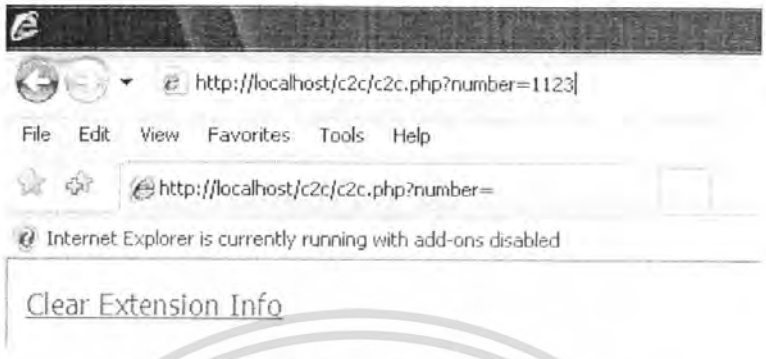
4.2 ผลการรันโปรแกรมด้วยชุดคำสั่ง

ทำการทดสอบโดยการเปิดหน้าเว็บเพจผ่านเครื่องคอมพิวเตอร์

รูปที่ 4.1 เมื่อทำการเปิดหน้าเว็บเพจ

รูปที่ 4.2 เมื่อทำการล็อกอินเข้าไปใช้งาน

เมื่อทำการล็อกอินเข้าไป จะได้รับ URL ซึ่งใช้กรอกหมายเลขที่ต้องการ



รูปที่ 4.3 URL ที่ได้รับ

รูปที่ 4.4 เมื่อทำการ Logout

รูปที่ 4.5 แสดงผลลัพท์เมื่อทำการเชื่อมต่อไม่สำเร็จ

บทที่ 5

บทสรุปและวิจารณ์

จากการทดสอบการใช้งาน ทำการ Login ผ่านหมายเลข Extension แล้ว จะได้รับ link เพื่อทำการเชื่อมต่อ และเมื่อทำการเชื่อมต่อ Server จะตอบกลับมายังหมายเลข Extension ที่ได้ทำการ Login ไว้ โดยทั้งนี้หากทำการโอนหมายเลข Extension ไปยังหมายเลขพื้นฐานก็สามารถทำได้ ซึ่งทำให้สะดวกในการใช้งาน และใช้งานได้กว้างขวางมากยิ่งขึ้น ทางด้านฝั่งตัว Server เองนั้น ก็สามารถทำงานได้ตามที่ต้องการ โดยเมื่อมีการ Login และสร้าง Cookie ขึ้นมา ตัว Server เมื่อได้รับข้อมูลจาก Cookie ก็สามารถที่จะทำการโทรออกตามข้อมูลที่ระบุมาได้

สำหรับการทดลองในครั้งนี้ ใช้คอมพิวเตอร์ เป็นตัว Login ทั้งนี้เนื่องจากยังไม่ได้มีการย้ายข้อมูลไปไว้บนอินเตอร์เน็ตจริง ซึ่งหากย้ายข้อมูลแล้ว จะสามารถเรียกหน้าเว็บเพจเพื่อทำการ Login ได้ผ่านทางโทรศัพท์มือถือโดยใช้บริการ GPRS นั่นเอง ซึ่งสามารถนำไปประยุกต์ใช้งานได้หลายรูปแบบ เช่น ระบบ Click to Call บนหน้าเว็บเพจ กล่าวคือ เมื่อผู้เข้าชมเว็บไซต์ต้องการติดต่อกับพนักงาน สามารถกรอกหมายเลขของตนเองลงไปแล้วส่งหมายเลขนั้นไปยัง Server ซึ่งจะทำการโทรกลับมายังหมายเลขที่กรอกไว้ และต่อสายไปยังพนักงาน ซึ่งอาจจะใช้หมายเลขบนระบบ SIP server อยู่ ทำให้สะดวก และประหยัดค่าใช้จ่าย

จะเห็นได้ว่า การใช้งาน IP PBX ในการจัดการการโทรออก และรับสาย สะดวก และง่าย รวมทั้งยังสามารถพัฒนาระบบต่อไปได้อีก เนื่องจากตัวโปรแกรมเป็นแบบ Open Source นั่นเอง

สำหรับการโทรออกผ่านระบบ VoIP นี้ จะช่วยลดค่าใช้จ่าย เมื่อมีการโทรออกไปยังหมายเลขโทรศัพท์ต่างประเทศ ทั้งนี้เนื่องจากปัจจุบันค่าโทรศัพท์ภายในประเทศยังมีราคาที่ถูกอยู่ ดังนั้น การนำมาใช้งานจริงกับผู้ที่ต้องการโทรออกไปยังหมายลเขปลายทางภายในประเทศจึงยังไม่เหมาะสม

ปัญหาที่พบ

1. การพัฒนาในเรื่องของ IP PBX ยังไม่แพร่หลาย ทำให้การสืบค้นข้อมูลเป็นไปได้ยาก
2. Server ต้องทำงานบน Linux เท่านั้น ทำให้ต้องมีการเรียนรู้การใช้งาน Linux เพิ่มเติม

แนวทางการพัฒนาต่อ

1. พัฒนา Server ให้รองรับหลายคู่สาย
2. ทำการ Login ผ่านมือถือได้โดยตรง
3. ทำระบบการลงทะเบียน ระบบ Billing แสดงให้ผู้ใช้งานเห็น

เอกสารอ้างอิง

[1] L.R. Rabiner, The impact of voice processing on modern telecommunications, Proceeding of the Speech Communication 17,p 217-226,1995

[2] A.Barberis,C.Casetti,J.C.De Martin,M.Meo, A simulation study of adaptive voice communications on IP networks, Proceeding of the Computer Communication 24,p 757-767,2001

[3] Alcatel Inc. , IP Telephony Design Guide ,Alcatel white paper, April 2003

[4] Voice Over IP Reference Page, Available on http://www.protocols.com/pbook/VoIP.htm(19 August 2004)

[5] Roberto Arcomano berto, VoIP Howto, August 7, 2002, Available on http://www.tldp.org/HOWTO/VoIP-HOWTO.html (19 August 2004)

[6] Alan Percy, Senior Sales Engineer, Understanding Latency in IP Telephony, Available on http://www.telephonyworld.com/training/brooktrout/iptel_latency_wp.html (19 August 2004)

[7] Asim Karim, Ohio State University , H.323 and Associated Protocols , Available on http://www.cis.ohio-state.edu/~jain/cis788-99/h323/index.html (19 August 2004)

[8] ปวีณ เขื่อนแก้ว.2004."โทรศัพท์บนเครือข่ายอินเตอร์เน็ต (Voice over Internet Protocol (VoIP)".ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่

[9] กรุงเทพธุรกิจ (กรุงเทพไอที) ฉบับวันที่ 16 สิงหาคม 2544

[10] บริษัท Allied Telesyn

[11] การสื่อสารด้วยระบบ Voice-over-IP (VoIP), Available on http://www.voipthailand.com/voip/articles/voip_articles_00002.html

[12] http://forum.voxilla.com/asterisk-support-forum/get-extention-continue-priorities-after-hangup-11414-3.html

[13] http://www.asteriskdiy.com

[14] http://www.asterisknow.org

ภาคผนวก

c2c.php

```
<a href=logout.php>Clear Extension Info</a><br>
<?
//Check if cookie is set
if (!isset($_COOKIE['extension_info']))
{
echo $_COOKIE['extension_info'];
?>
   <body>
   <form method="POST" action="login.php">
   <h1>Enter your Extension Number</h1>
      <table border="0" width="auto">
      <tr>
        <td width="33%">Extension</td>
        <td width="33%"><input type="text" name="exten" size="20"></td>
        <td width="34%"><input type="hidden" name="number" value=<? echo $_REQUEST['number'];?>> </td>
      </tr>
    </table>
   <p><input type="submit" value="Submit" name="sub">
   <input type="reset" value="Reset" name="res"></p>
   </body>
   </form>
<?php  }
else
{
//Cookie is set and display the data
  $extension_info = explode("-", $_COOKIE['extension_info']);  //Extract the Data
  $name = $extension_info[0];
 //exit;
}

#ip address that asterisk is on.
$strHost = "127.0.0.1";

#specify the username you want to login with (these users are defined in /etc/asterisk/manager.conf)
#this user is the default AAH AMP user; you shouldn't need to change, if you're using AAH.
$strUser = "admin";

#specify the password for the above user
$strSecret = "amp111";

#specify the channel (extension) you want to receive the call requests with
#e.g. SIP/XXX, IAX2/XXXX, ZAP/XXXX, etc
$strChannel = $_COOKIE['extension_info'];

#specify the context to make the outgoing call from.  By default, AAH uses from-internal
#Using from-internal will make your outgoing dialing rules apply
$strContext = "from-internal";

#specify the amount of time you want to try calling the specified channel before hangin up
$strWaitTime = "30";

#specify the priority you wish to place on making this call
$strPriority = "1";

#specify the maximum amount of retries
$strMaxRetry = "2";

$number=strtolower($_REQUEST['number']);
$pos=strpos ($number,"local");
if ($number == null) :
 exit() ;
endif ;
if ($pos===false) :
$errno=0 ;
$errstr=0 ;
$strCallerId = "Web Call <$number>";
$oSocket = fsockopen ("localhost", 5038, $errno, $errstr, 20);
 if (!$oSocket) {
  echo "$errstr ($errno)<br>\n";
} else {
```

```
fputs($oSocket, "Action: login\r\n");
fputs($oSocket, "Events: off\r\n");
fputs($oSocket, "Username: $strUser\r\n");
fputs($oSocket, "Secret: $strSecret\r\n\r\n");
fputs($oSocket, "Action: originate\r\n");
fputs($oSocket, "Channel: SIP/$strChannel\r\n");
fputs($oSocket, "WaitTime: $strWaitTime\r\n");
fputs($oSocket, "CallerId: $strCallerId\r\n");
fputs($oSocket, "Exten: $number\r\n");
fputs($oSocket, "Context: $strContext\r\n");
fputs($oSocket, "Priority: $strPriority\r\n\r\n");
fputs($oSocket, "Action: Logoff\r\n\r\n");
sleep(2);
fclose($oSocket);
 }
if (!isset($_COOKIE['extension_info']))
{
echo "";
} else {
echo "Extension $strChannel should be calling $number." ;
}
else :
 exit() ;
endif ;
?>
```

Login.php

```
<?php
   //Collect the details and validate
   $time = time();
if (empty($_POST['exten']))
{
echo "<a href=c2c.php>Enter your Extension Number.</a>";
}
else
{
   $name = $_POST['exten'];
   $number = $_POST['number'];
   {
      $cookie_data = $name;
      {
         if(setcookie ("extension_info",$cookie_data, $time+365*24*3600)==TRUE)
                        {
            echo "<a href=c2c.php?number=$number>Click to Call</a>";
   }else{
echo "Logged In";
   }
}
}
}
?>
```

Logout.php

```
<?php
$time = time();

if (isset($_COOKIE['extension_info']))
 {
 setcookie ("extension_info", "", $time - 365*24*3600);
 echo "Extension Logged Out<br>";
}
echo "<a href=c2c.php>Login Again?</a>";
?>
```