บทที่ 2

ทฤษฎีและหลักการทำงาน

ในส่วนของทฤษฎีและหลักการทำงานแบ่งเนื้อหาหลักๆ ออกเป็น 6 หัวข้อสำคัญ โดยเริ่มต้นหัวข้อที่ 2.1 แนะนำการติดต่อสื่อสารแบบไร้สาย (Mobile Communication) หัวข้อที่ 2.2 กล่าวถึงระบบเครือข่ายไอพีรุ่นที่ 6 โดยอธิบายข้อแตกต่างจากระบบเครือข่ายไอพีรุ่นที่ 4 หัวข้อที่ 2.3 อธิบายรายละเอียดโครงสร้างของระบบเครือข่ายและการทำงานของโปรโตคอล MIP (Mobile IP) หัวข้อที่ 2.4 อธิบายรายละเอียด หน้าที่ โครงสร้าง และสัญญาณของโปรโตคอล SIP หัวข้อที่ 2.5 เป็นลักษณะการทำโมไบลิตี้รูปแบบต่างๆด้วยโปรโตคอล SIP สำหรับหัวข้อสุดท้ายเป็นการเปรียบเทียบความสามารถในการทำโมไบลิตี้ด้วยโปรโตคอล SIP และ Mobile IP เพื่อให้เห็นถึงขอบเขต ความสามารถ ข้อดีและข้อเสีย ของทั้ง 2 โปรโตคอลนี้

2.1 การติดต่อสื่อสารแบบไร้สาย

เมื่อคอมพิวเตอร์ถูกนำเข้ามาใช้ในชีวิตประจำวันมากขึ้น มนุษย์ต้องทำงานกับคอมพิวเตอร์และมีการแลกเปลี่ยนข้อมูลผ่านทางระบบเครือข่ายคอมพิวเตอร์หรือเครือข่ายโทรคมนาคมด้วยอุปกรณ์สื่อสารต่างๆ จึงทำให้เกิดแนวความคิดที่จะทำให้ผู้ใช้สามารถทำงานกับคอมพิวเตอร์ได้แม้ว่าผู้ใช้มีการย้ายที่อยู่หรือเคลื่อนที่ เพื่อให้ผู้ใช้อาจสามารถทำงานได้แม้ในวันหยุดหรือในขณะเดินทางไกล ระบบไร้สาย (Wireless Network) ถูกคิดขึ้นเพื่อให้อุปกรณ์สื่อสารหรือคอมพิวเตอร์สามารถเคลื่อนย้ายได้ การที่คนจำนวนมากต้องมีการเคลื่อนที่นี้เองทำให้เกิดแนวความคิดของการสื่อสารแบบเคลื่อนที่ (Mobile Communication)

แนวความคิดในการทำงานการสื่อสารแบบเคลื่อนที่มีหลักการ 2 หลักการที่ต่างกันเพื่อให้เกิดโมไบลิตี้ขึ้น นั่นคือ User Mobility และ Device Portability

User Mobility คือการที่ผู้ใช้สามารถใช้บริการการสื่อสารข้อมูลได้ดังเดิมแม้ว่าผู้ใช้มีการเคลื่อนย้าย และการบริการต่างๆที่มียังคงสามารถทำงานได้เมื่อผู้ใช้เคลื่อนที่ ตัวอย่างการทำงานอย่างง่ายในการทำ User Mobility คือ การทำ call-forward ซึ่งรู้จักกันดีในระบบโทรศัพท์ เช่น เมื่อผู้ใช้ A ไม่อยู่บ้าน แต่ขณะนี้ผู้ใช้ A กำลังทำงานอยู่ห้องทำงานในสำนักงานแห่งหนึ่ง เมื่อผู้ใช้ B โทรหาผู้ใช้ A ที่บ้านแล้วเครื่องโทรศัพท์ที่บ้านจะทำการส่งต่อหรือโอนสายอัตโนมัติไปยังเครื่องโทรศัพท์ ณ ห้องทำงานของผู้ใช้ A ทันที เป็นต้น

Device Portability เป็นการอ้างอิงความสามารถของอุปกรณ์สื่อสารหรือคอมพิวเตอร์เมื่อมีการเคลื่อนที่หรือย้ายตำแหน่งจะยังคงรักษาการเชื่อมต่อในระบบเครือข่ายนั้นๆได้ กล่าวคือไม่เพียงแต่บริการหรือระบบจะถูกพัฒนาขึ้นเท่านั้น ความสามารถของอุปกรณ์สื่อสารต้องมีการพัฒนาขึ้นตามไปด้วย ดังนั้นภายในตัวอุปกรณ์เหล่านี้จะต้องมีอัลกอริทึมการทำงานที่ดีพอที่สามารถรองรับการทำงานสอดคล้องกับเทคโนโลยีระบบที่มีการพัฒนาขึ้นได้ ตัวอย่างของระบบที่สนับสนุน Device Portability คือระบบโทรศัพท์เคลื่อนที่ ซึ่งระบบนี้ให้บริการโดยอุปกรณ์สื่อสารถูกเคลื่อนที่แต่ยังสามารถรับสัญญาณคลื่นวิทยุ (Radio Signal) จากสถานีฐาน (Base Station) แม้ว่าเมื่อระยะทางไกลมากขึ้นสัญญาณจะอ่อนลง เป็นต้น

อุปกรณ์แบบไร้สายจึงมีบทบาทเพิ่มมากขึ้น แม้ว่าระบบการสื่อสารแบบมีสายจะถูกเปลี่ยนเป็นการส่งข้อมูลผ่านทางอากาศด้วยคลื่นอิเล็กทรอนิกส์โดยไม่ใช้สาย แต่ในโลกของการสื่อสารจำเป็นต้องมีการเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างเครือข่ายและระหว่างอุปกรณ์สื่อสารที่แตกต่างชนิดกันด้วย จึงจะทำให้การสื่อสารมีประสิทธิภาพสูงสุด คุณสมบัติของอุปกรณ์สื่อสารประเภทต่างๆในโลกของการสื่อสารสามารถสรุปได้ดังนี้

Fixed and wired: อุปกรณ์ที่มีการทำงานเชื่อมต่อกับด้วยสายส่งข้อมูล (Medium) ซึ่งได้แก่ ระบบเครือข่ายคอมพิวเตอร์แบบ Desktop เป็นต้น

Mobile and wired: อุปกรณ์ที่ยังคงมีการทำงานเชื่อมต่อกับระบบแบบมีสาย (Wired) แต่อุปกรณ์นี้สามารถเคลื่อนย้ายได้ เช่น Notebook/Laptop computer เป็นต้น ซึ่งเมื่อมีการย้ายที่อยู่ผู้ใช้สามารถทำงานเชื่อมต่อเข้าระบบเครือข่ายได้โดยผ่าน Modem และระบบโทรศัพท์

Fixed and wireless: อุปกรณ์ที่มีการทำงานลักษณะนี้เป็นประโยชน์ในการติดตั้งหรือทำการกำหนดค่าต่างๆจากต่างสถานที่ได้ ตัวอย่างการใช้งานอุปกรณ์ประเภทนี้ ได้แก่ ความต้องการใช้งานภาย

ในสิ่งก่อสร้างอาคารที่ไม่ต้องการใช้สาย การจัดงานแสดงต่างๆ แต่ยังคงสามารถเชื่อมต่อกับระบบเครือข่ายได้ด้วยระบบเครือข่ายไร้สาย

Mobile and wireless: อุปกรณ์ในลักษณะนี้เป็นที่น่าสนใจมากที่สุด เพราะผู้ใช้สามารถทำการสื่อสารได้อย่างอิสระ ไร้สาย สามารถเคลื่อนที่ไปในที่ต่างๆได้ตามต้องการ

การที่จะสามารถทำการเชื่อมต่อระหว่างระบบเครือข่ายต่างชนิดกันด้วยอุปกรณ์ที่แตกต่างกันได้นั้น จำเป็นต้องมีการกำหนดรูปแบบและโครงสร้างในการติดต่อ รวมถึงควรมีการนิยามมาตรฐานและโปรโตคอลที่ใช้เพื่อสนับสนุนการทำงานของแต่ละระบบเครือข่ายและเพื่อให้เกิดประโยชน์ในการเข้าถึงข้อมูลในแต่ละระบบได้อย่างมีประสิทธิภาพสูงสุด

2.2 ระบบเครือข่ายไอพีรุ่นที่ 6

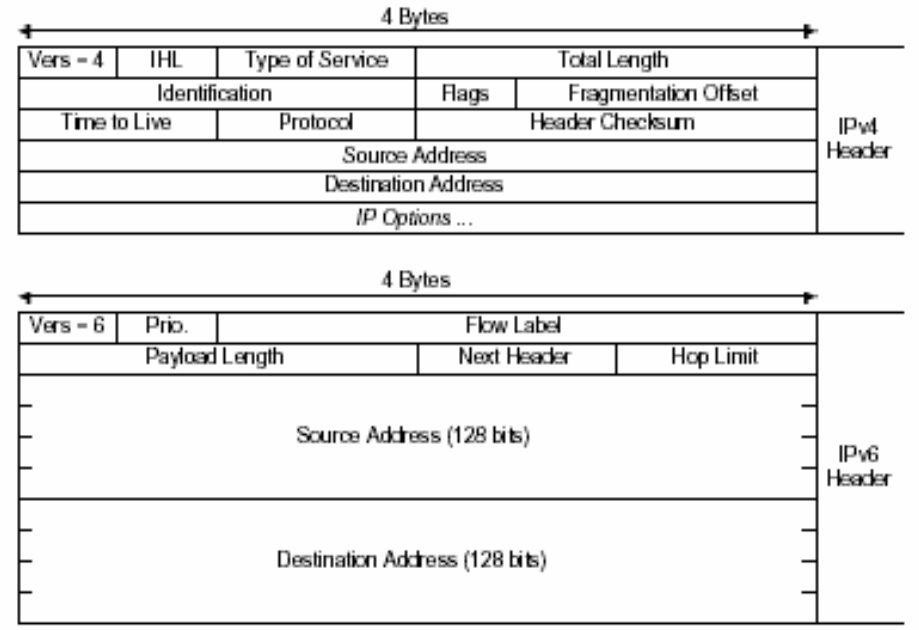
องค์กร IETF (Internet Engineering Task Force) ออกแบบโปรโตคอลไอพีรุ่นที่ 6 ขึ้นใช้งานแทนที่โปรโตคอลไอพีรุ่นที่ 4 เพื่อตอบสนองความต้องการการใช้หมายเลขไอพีตามจำนวนผู้ใช้ที่เพิ่มมากขึ้น โดยในที่นี้จะอธิบายเฉพาะประเด็นของข้อแตกต่างระหว่างโปรโตคอลไอพีรุ่นที่ 6 และโปรโตคอลไอพีรุ่นที่ 4 และจุดสำคัญของในการทำโมไบลิตี้บนโปรโตคอลไอพีรุ่นที่ 6 (สามารถศึกษาข้อมูลโดยละเอียดของโปรโตคอลไอพีรุ่นที่ 6 ได้จาก RFC 2460)

ข้อแตกต่างหลักระหว่างรูปแบบโปรโตคอลไอพีรุ่นที่ 6 กับไอพีรุ่นที่ 4 มี 3 ประการด้วยกัน ดังนี้

1) IPv6 Base Header

2) IPv6 Extension Header

3) IPv6 Address Types



รูปที่ 1 IPv6 Base Header vs IPv4 Header

(ที่มา: R. Ait Yaiz, 2000)

จากรูปที่ 1 แสดงถึงความแตกต่างของ IPv6 Base Header กับ IPv4 Header จะพบว่า IPv6 Header รวมเอา Next Header field และ Address fields เก็บไว้ใน IPv6 Base Header เป็นผลให้ขนาดของ IPv6 Base Header มีขนาดใหญ่กว่า IPv4 Header สำหรับ Next Header Field ในโปรโตคอลไอพีรุ่นที่ 6 นั้นสามารถเป็น Extension Header เพียงรูปแบบเดียวจากทั้งหมดดังนี้

Extension Header:

- Hop-by-Hop Option Header

เป็น Header ซึ่งระบุ Option ที่ใช้ในการทดสอบโดยทุกๆ Router เมื่อผ่านเส้นทางหนึ่ง

- Destination Option Header

เป็น Header ซึ่งระบุ Option ที่ใช้เพียงการทดสอบปลายทาง

- Routing Header

เป็น Header ซึ่งถูกใช้ในกรณีการทำ source routing

- Fragment Header

เป็น Header ซึ่งถูกใช้โดย source node เมื่อแพ็กเกตมีขนาดใหญ่กว่าค่า Path Maximum Transfer Unit ในการส่งข้อมูลแต่ละแพ็กเกต

- IP authentication Header

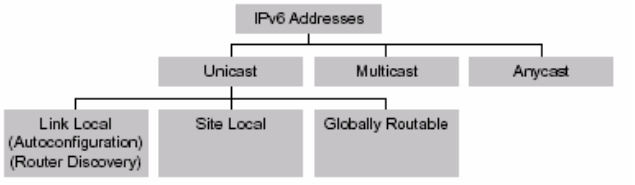
เป็น Header ซึ่งถูกใช้ในการจัดให้ authentication

- IP Encapsulation Security Payload

เป็น Header ใช้เพื่อรับรองความปลอดภัยของการจัดรูปแบบข้อมูลของ IP Payload

- Upper-Layer Header

ใช้เก็บค่าข้อมูลของ TCP Header หรือ UDP Header



รูปที่ 2 IPv6 Address Type
(ที่มา: R. Ait Yaiz, 2000)

จากรูปที่ 2 แสดง IPv6 Address Type ซึ่งแตกต่างจากโปรโตคอลไอพีรุ่นที่ 4 โดยโปรโตคอลไอพีรุ่นที่ 6 มีการจัดให้การส่งข้อมูลแบบ Broadcast เป็นกรณีพิเศษของ Multicast จึงเป็นผลให้ไม่มี Broadcast Address Type ในโปรโตคอลไอพีรุ่นที่ 6 แต่มีการนิยามใหม่เป็น Anycast Address ซึ่งเมื่อมีการใช้ Anycast Address ข้อมูลทุกๆแพ็กเกตจะถูกส่งเพียงภายในกลุ่มหนึ่งๆที่ระบุไว้ใน Anycast Address นี้เท่านั้น นอกจากนี้โปรโตคอลไอพีรุ่นที่ 6 ยังมีการกำหนดรูปแบบของ Unicast Address แบ่งออกเป็น 3 ชนิดแตกต่างกันดังนี้

- Link Local Address

เป็นเพียงสัญลักษณ์จำเพาะ Local link (Local Link Significance) ซึ่งหมายถึงแพ็กเกตใดๆที่กำลังใช้ Link Local Address จะไม่ถูก forward โดย Router ความสำคัญของ Link Local Address ถูกใช้ในกรณีการทำ Auto configuration และ Router Discovery

- Site Local Address

เป็นเพียงสัญลักษณ์เฉพาะ Site Local นั้น (Site Local Significance) ซึ่งหมายถึงแพ็กเกตใดๆที่กำลังใช้ Site Local Address จะสามารถถูก forward โดยทุกๆ Router ระหว่าง site ยกเว้น egress Router ที่กำลังติดต่อกับเครือข่ายอินเตอร์เน็ตทั่วไป (Global Internet)

- Globally Routable address

ใช้ระบุค่าจำเพาะของ Global Network นั้น

หากคำนึงความสามารถในการทำโมไบลิตี้บนโปรโตคอลไอพีรุ่นที่ 6 เมื่อพิจารณาข้อแตกต่างหรือข้อดีข้อเสียที่ได้ระหว่างโปรโตคอลไอพีรุ่นที่ 6 กับโปรโตคอลไอพีรุ่นที่ 4 สามารถสรุปคุณสมบัติที่อาจเป็นประโยชน์ในการทำ Mobile IPv6 ได้ดังนี้ (สำหรับรายละเอียดการทำงานของโปรโตคอล Mobile IP อย่างละเอียดจะถูกอธิบายไว้ในหัวข้อที่ 2.3)

-จำนวนหมายเลขไอพีที่เพิ่มมากขึ้น เป็นผลให้สามารถรองรับเทคโนโลยีใหม่ในการระบุตำแหน่งหรืออ้างอิงหมายเลขไอพีแบบ Care-Of-Address ที่ใช้ในการระบุตำแหน่งของโหนดเคลื่อนที่ (Mobile Node) ได้ และเนื่องจากมีหมายเลขไอพีมากเพียงพอสำหรับทั้งโหนดเคลื่อนที่และโหนดคงที่ (Fixed Node) ตัว Foreign Agent หรือ Router ในระบบเครือข่ายใหม่สามารถยกเลิกการใช้งาน Care-Of-Address ได้ตามความต้องการ

- การที่โปรโตคอลไอพีรุ่นที่ 6 มีการใช้ Routing Header ทำให้โปรโตคอลไอพีรุ่นที่ 6 สามารถทำ Source Routing ได้ในขณะที่โปรโตคอลไอพีรุ่นที่ 4 ทำไม่ได้

- การที่โปรโตคอลไอพีรุ่นที่ 6 มีการใช้ Authentication Header กับสัญญาณ Binding Message ได้ ดังนั้นการทำ Binding Update จึงสามารถทำ Authentication ได้

- การที่โปรโตคอลไอพีรุ่นที่ 6 มีการใช้ Destination Options Header ซึ่งอนุญาตให้ใช้ Option นี้ได้โดยไม่เกิดการลดถอยของประสิทธิภาพการทำงาน (Performance degradation) เนื่องจากการลดถอยของประสิทธิภาพการทำงานของโปรโตคอลไอพีรุ่นที่ 4 เกิดขึ้นเมื่อทุก Router ตามเส้นทางจะต้องมีการ

ตรวจสอบค่า options จากทุกแพ็กเกตทันทีที่แต่ละ Router ได้รับ แทนที่จะส่งแพ็กเกตนั้นๆไปยังปลายทางต่อไป

จากคุณสมบัติที่กล่าวเป็นตัวช่วยให้ความสามารถของ Mobile IP บนระบบเครือข่ายไอพีรุ่นที่ 6 มีความสามารถและมีสมรรถนะการทำงานเพิ่มมากขึ้น ซึ่งจะกล่าวรายละเอียดในหัวข้อถัดไป

2.3 Mobile IP

Mobile IP เป็นโปรโตคอลมาตรฐานที่ถูกเสนอขึ้นโดยทำงานอยู่บนโปรโตคอลไอพีเพื่อให้เกิดความสามารถของโมไบลิตี้โดยซ่อนการทำงานทั้งหมดภายในระดับ Network ดังนั้นโปรโตคอลในระดับชั้นที่สูงกว่าจะสามารถรับรู้การทำงานของโปรโตคอล Mobile IP ได้ เช่น โปรโตคอล TCP ในระดับชั้นทรานสพอร์ท เป็นต้น ด้วยความสามารถของโปรโตคอล Mobile IP จึงทำให้เครื่องคอมพิวเตอร์ในระบบสามารถอ้างอิงตำแหน่งที่อยู่ได้อย่างถูกต้องและแน่นอนแม้เกิดการเปลี่ยนแปลงตำแหน่งที่อยู่ก็ตาม (สามารถศึกษารายละเอียดเพิ่มเติมได้อ้างอิง RFC 2002)

2.3.1 Mobile IP Network Component

Home Agent (HA)

หมายถึงโหนดที่ทำหน้าที่เสมือน Proxy ในขณะที่โหนดเคลื่อนที่ (Mobile Node) ทำการเคลื่อนที่ออกจาก Home Network โดยทำการดักข้อมูลแพ็กเกต (Interception) และ ทำช่องสัญญาณเชื่อมต่อ (Tunneling) ข้อมูลที่ส่งผ่านระหว่างโหนดคงที่ (Correspondent Node) และโหนดเคลื่อนที่ (Mobile Node) นอกจากนี้ Home Agent เป็นโหนดที่เก็บข้อมูลตำแหน่งหรือหมายเลขไอพีทั้งหมดของโหนดเคลื่อนที่

Correspondent Node (CN)

หมายถึงโหนดที่ทำการติดต่อไปยังโหนดเคลื่อนที่และเป็นโหนดที่ไม่มีการเคลื่อนที่หรือย้ายตำแหน่งออกจาก Home Network

Foreign Agent (FA)

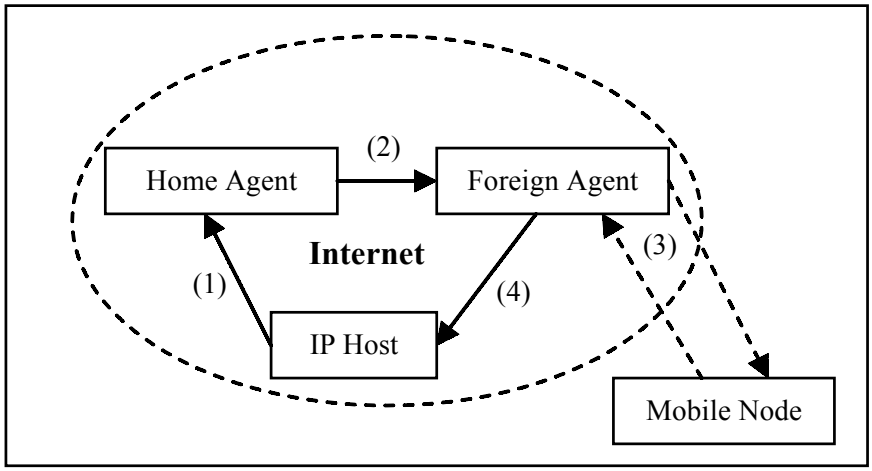
หมายถึงโหนดที่ทำหน้าที่เสมือน Proxy ของระบบเครือข่ายที่โหนดเคลื่อนที่ทำการเคลื่อนที่ไปยังระบบเครือข่ายนี้หรือเรียกว่า Foreign Network ดังนั้น Foreign Agent จะทำการ ถอดช่องสัญญาณเชื่อมต่อ (De-Tunneling) ข้อมูลที่ได้รับจาก Home Agent และส่งต่อไปยังโหนดเคลื่อนที่

Mobile Node (MN)

หมายถึงโหนดที่เคลื่อนที่ได้หรือสามารถย้ายตำแหน่งจาก Home Network ไปยัง Foreign Network ได้ ซึ่งอาจหมายถึงอุปกรณ์สื่อสารเคลื่อนที่ (Wireless Device) ชนิดต่างๆ ได้แก่ คอมพิวเตอร์เคลื่อนที่ (Notebook), คอมพิวเตอร์มือถือ (Pocket PC), โทรศัพท์เคลื่อนที่ (Mobile Phone) เป็นต้น

2.3.2 MIPv4

อัลกอริทึมการทำงานของ Mobile IP รุ่นที่ 4 หรือ MIPv4 เป็นไปดังนี้



รูปที่ 3 *Triangle routing*

จากรูปที่ 3 แสดงการลำดับการทำ Triangle routing (Tunneling) คือ การทำการติดต่อระหว่างโหนดทั่วไป (IP Host/Correspondent Node - CN) กับโหนดเคลื่อนที่ (Mobile Node - MN) ผ่านระบบเครือข่ายไอพี แต่ละข้อมูลแพ็กเกตจากโหนดทั่วไปสามารถเคลื่อนที่ไปยังปลายทางได้โดยใช้หลักการ Tunneling ผ่านทาง Mobility Agent ได้แก่ Home Agent (HA) และ Foreign Agent (FA)

โดยมีลำดับขั้นตอนการทำงานเป็นไปดังต่อไปนี้

1. IP Host หรือ CN รู้หมายเลขไอพีของ MN ซึ่งเป็นหมายเลขไอพีแบบคงที่ ซึ่งขึ้นอยู่กับ Home Network ดังนั้น CN จึงส่งข้อมูลแพ็กเกตไปยังหมายเลขไอพีนี้ นั่นคือแพ็กเกตถูกส่งโดยตรงไปยัง HA เมื่อ HA ได้รับแพ็กเกตจาก CN มันจะทำการแยกแยะข้อมูลในแพ็กเกตนั้นและทำการรวมกับเข้ากันอีกครั้งด้วยวิธี IP-within-IP Encapsulation หรือ Minimal Encapsulation ก่อนที่จะทำการส่งต่อไปยัง

หมายเลข Care-Of-Address (Care-Of-Address หมายถึง หมายเลขไอพีใหม่ที่ได้รับจาก FA ใน Foreign Network)

2. ข้อมูลแพ็กเกตที่ถูกทำ Encapsulation ใหม่แล้วจะถูกส่งต่อไปยัง Foreign Agent โดยอ้างอิงด้วย Care-Of-Address ของ MN ปลายทาง
3. เมื่อ FA ได้รับแพ็กเกตจะทำการ De-Tunnel ข้อมูลแพ็กเกตทั้งหมดแล้วจึงส่งต่อไปยัง MN
4. ข้อมูลแพ็กเก็ตจาก MN จะถูกส่งมายัง FA แล้วถูกทำการส่งต่อไปยัง IP Host หรือ CN

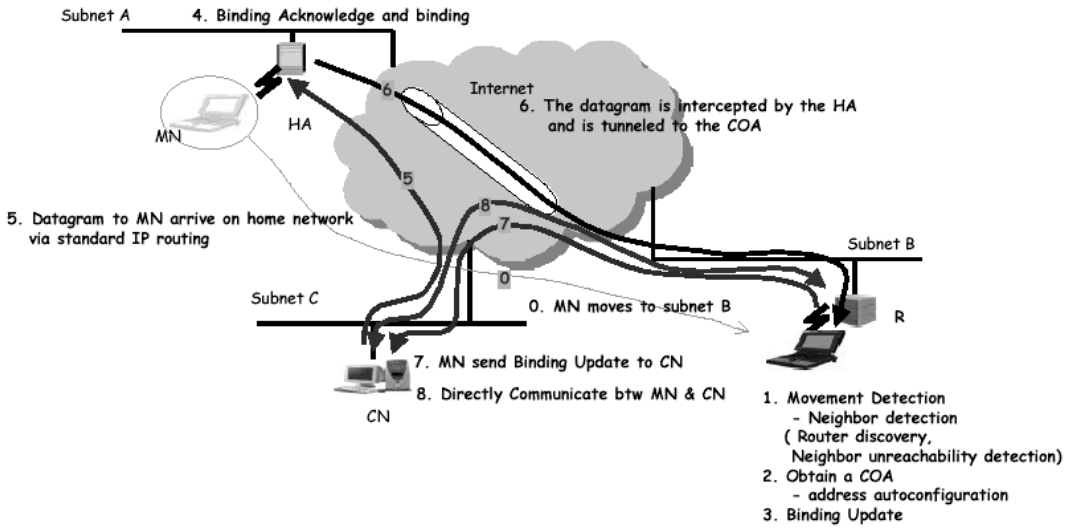
จากการทำงานของ MIPv4 ดังกล่าวทำให้เกิดความล่าช้าของข้อมูลในการส่งแพ็กเกตผ่านทาง HA และ FA และสูญเสียเวลาในการทำ Encapsulation และ De-Encapsulation ระหว่าง Agent ทั้ง 2 โดยปัญหาดังกล่าวได้ถูกแก้ไขและพัฒนาประสิทธิภาพมากขึ้นด้วย MIPv6

2.3.3 MIPv6

การทำงานของ MIPv6 มีการออกแบบระบบโมไบลิตี้แตกต่างจาก MIPv4 คือ ในระบบของ MIPv6 โหนด FA ถูกรวมการทำงานเข้าไว้กับ MN เป็นผลให้ FA ไม่มีในระบบโมไบลิตี้ของ MIPv6 การทำงานของ MIPv6 จะมีการทำ Binding Update ระหว่าง HA กับ MN ด้วยค่า COA (Care-of-Address) หรือหมายเลขไอพีที่ MN ได้รับบนระบบ Foreign Network

ระบบการทำงานของ MIPv6 ช่วยให้ MN สามารถเคลื่อนที่ไปยังระบบเครือข่ายใหม่ได้โดยไม่ถูกตัดขาดการเชื่อมต่อเดิม การทำงานของ MIPv6 มีจุดสำคัญอยู่ที่ HA ที่ทำหน้าที่ในการส่งสัญญาณควบคุมต่างๆและเก็บค่าข้อมูลของหมายเลขไอพีของ MN ไว้ การรวมส่วนการทำงานของ FA ไว้ที่ MN นั้นช่วยให้ระบบมีความซับซ้อนลดลงและมีประสิทธิภาพในการทำงานที่ดีขึ้น

รูปแบบการทำงานพื้นฐานเป็นดังนี้



รูปที่ 4 การทำงานพื้นฐานของ MIPv6

(ที่มา: Kyeong-Jin Lee, 2001)

1. เมื่อ MN ทำการเคลื่อนที่จาก Home Network มายัง Foreign Network ซึ่งสามารถทราบได้ว่า MN มีการเคลื่อนย้ายเปลี่ยนหรือข้ามระบบเครือข่ายเกิดขึ้นด้วยการตรวจสอบการเคลื่อนที่ (Movement Detection) ของ MN ซึ่งจะกล่าวถึงวิธีการตรวจสอบการเคลื่อนที่ในหัวข้อถัดไป
2. MN ได้รับหมายเลขไอพีใหม่ที่ใช้ภายใน Foreign Network ซึ่งอาจได้จากการทำ Address Auto-configuration เป็นต้น
3. MN ทำการส่งสัญญาณ Binding Update ไปยัง HA
4. HA ทำการส่งสัญญาณ Binding Acknowledge กลับมายัง MN และทำการปรับค่าข้อมูลหมายเลขไอพีที่เปลี่ยนแปลง
5. ข้อมูลแพ็กเกตจาก CN ที่ต้องการส่งไปยัง MN จะถูกส่งตรงไปยัง HA โดยอาศัยพื้นฐานการทำ IP Routing
6. เมื่อ HA ได้รับข้อมูลแพ็กเกตจะทำการดักข้อมูลของแพ็กเกตนั้น (Interception) และทำการ Tunneling โดยระบุปลายทางด้วย COA แล้วส่งต่อไปยัง MN
7. เมื่อ MN ได้รับข้อมูลแพ็กเกตจึงทำการ De-Tunneling และรับรู้หมายเลขไอพีของ CN ดังนั้นจึงทำการส่งสัญญาณ Binding Update ไปยัง CN
8. MN ส่งข้อมูลแพ็กเกตไปยัง CN โดยตรง

อย่างไรก็ตามการทำงานของ MIPv6 ยังคงมีการทำ Tunneling และ De-Tunneling ในทุกๆ ครั้งที่ MN มีการย้ายระบบเครือข่าย (Hand Over) ทำให้สูญเสียเวลาระยะหนึ่ง โดยแนวทางการแก้ไขปัญหาดังกล่าววิธีหนึ่งสามารถทำได้โดยเพิ่มความสามารถในการตรวจสอบการเคลื่อนย้ายเปลี่ยนระบบเครือข่าย (Movement Detection) ซึ่งหากมีการตรวจสอบได้อย่างรวดเร็วจะทำให้ช่วงเวลาการย้ายระบบเครือข่ายเป็นไปได้อย่างรวดเร็ว

Movement Detection

การตรวจสอบการเคลื่อนย้ายระบบเครือข่ายของ MN สามารถทำได้ 2 วิธี ดังนี้

1. Router Advertisement Detection

เมื่อมีการเชื่อมต่อภายในระบบเครือข่ายแล้ว MN สามารถได้รับสัญญาณ Router Advertisement Message ได้เมื่อ MN ทำการส่งสัญญาณ Router Solicitation Message ไปยัง Router ของระบบเครือข่าย โดยค่าข้อมูลใน Router Advertisement Message จะบ่งบอกถึง ค่า Prefix ของ Foreign Network และ Router Information ซึ่งจะถูกใช้โดย MN เมื่อมีการเคลื่อนที่อยู่ในระบบเครือข่ายนี้

ดังนั้นในขณะที่ MN ทำการเคลื่อนย้ายจาก Home Network จะเริ่มทำการตรวจสอบและเลือก Router จากนั้นเมื่อได้รับสัญญาณ Router Advertisement Message จาก Router ที่เลือกแล้วนั้น MN จะนำข้อมูล Prefix ที่ได้จากสัญญาณนี้มากำหนดค่า COA เพื่อใช้ในการทำ Binding Update ไปยัง HA และ CN ต่อไป

2. Neighbor Unreachable Detection (NUD)

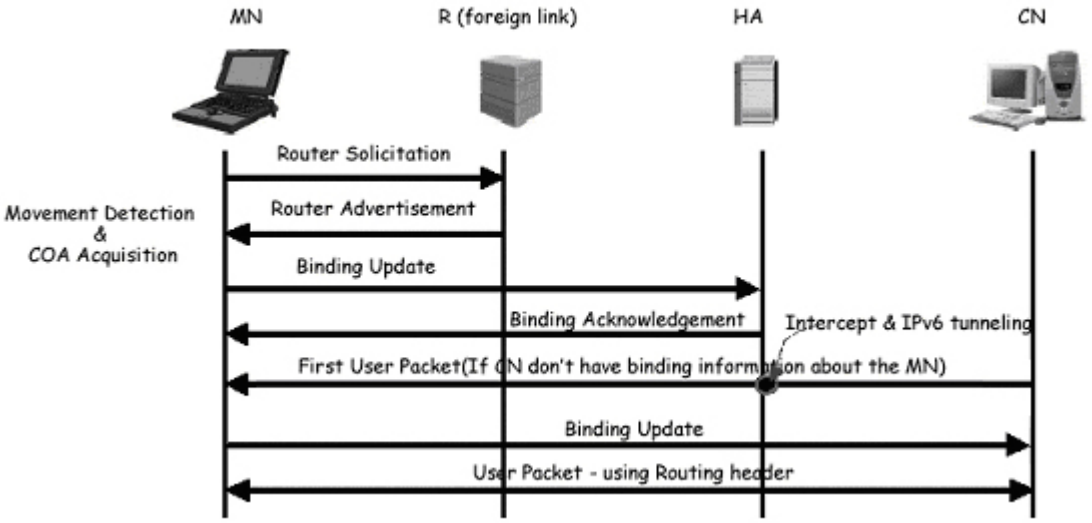
การทำงานด้วยวิธีนี้ถูกทำโดย MN ในขณะที่ทำการตรวจสอบว่า Router ที่ทำการเชื่อมต่ออยู่นั้น ถูกตัดขาดการเชื่อมต่อหรือไม่ การตรวจสอบว่าขาดการเชื่อมต่อ (Unreachable) นั้นอาจตรวจสอบได้จาก

กรณีที่ 1: เมื่อการทำงานในระดับ upper-layer ไม่สามารถทำการติดต่อใดๆได้ เช่น การทำ Re-Transmit ของโปรโตคอล TCP นั้นหมดอายุ (Expire) เป็นต้น

กรณีที่ 2: เมื่อ MN ทำการส่งสัญญาณ Neighbor Solicitation Message ไปยัง Router แล้วไม่สามารถรับสัญญาณ Neighbor Advertisement Message ได้

ดังนั้นในทำนองเดียวกัน MN สามารถใช้วิธีการเดียวกันในการตรวจสอบหา Router ถัดไปทันทีเมื่อพบว่าขาดการเชื่อมต่อกับ Router เดิม ซึ่งอาจจะทำการส่งสัญญาณ Neighbor Solicitation Message ไปยัง Router อื่นๆ เป็นต้น

กระบวนการลงทะเบียนของ MIPv6 (Registration Procedure)



รูปที่ 5 แสดงลำดับการทำ Registration หรือ Binding Update

(ที่มา: Kyeong-Jin Lee, 2001)

จากรูปที่ 5 แสดงลำดับสัญญาณในการ Registration เป็นไปดังนี้

1. เริ่มการทำงานเมื่อ MN ทำการเคลื่อนที่จาก Home Network ไปยัง Foreign Network จากนั้น MN ทำการส่งสัญญาณ Router Solicitation ไปยัง Router ตัวใหม่ใน Foreign Network ทันทีที่มีการตรวจสอบว่ามีการเคลื่อนที่แล้ว (Movement Detection)

2. เมื่อ MN ได้รับสัญญาณ Router Advertisement จาก Router บน Foreign Network จะทำการดึงค่าข้อมูลจากค่าสัญญาณนี้เพื่อใช้กำหนดเป็น COA (COA Acquisition)

3. จากนั้น MN จึงส่งสัญญาณ Binding Update ไปยัง HA เมื่อ HA ได้รับสัญญาณ Binding Update จึงทำการปรับค่าข้อมูลหมายเลขไอพีใหม่

4. HA ทำการส่งสัญญาณ Binding Acknowledgement กลับไปยัง MN

5. สำหรับในกรณีนี้ CN เป็นผู้เริ่มส่งข้อมูลไปยัง MN ดังนั้นข้อมูลแพ็กเกตแรกจะถูกส่งไปยัง MN โดยการทำ Tunneling ที่ HA เนื่องจาก CN ไม่มี Binding Information ใหม่ของ MN

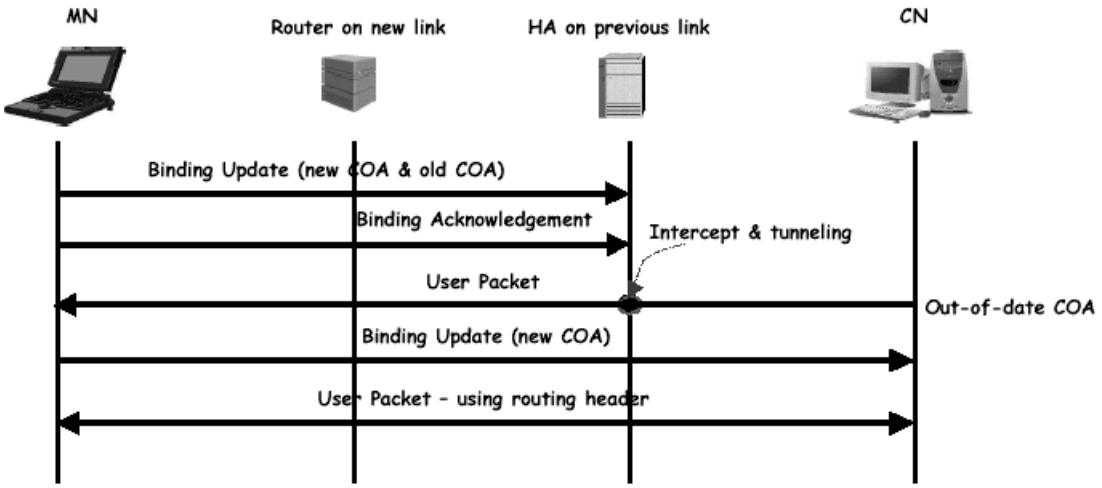
6. เมื่อ MN ได้รับข้อมูลแพ็กเกตแรกนี้ ทำให้สามารถรับรู้ได้ว่า CN ไม่มีข้อมูล Binding ปัจจุบันจึงทำการส่งสัญญาณ Binding Update ไปยัง CN

7. ดังนั้นข้อมูลแพ็กเกตต่อมานี้จะถูกส่งโดยตรงระหว่าง MN และ CN โดยไม่จำเป็นต้องผ่าน HA อีกต่อไป

เนื่องจากโปรโตคอลไอพีรุ่นที่ 6 มีการเพิ่ม Destination Option Header ขึ้นใหม่ใน IP Header ของโปรโตคอลไอพีรุ่นที่ 6 ทำให้ในการทำ Registration ของ MIPv6 สามารถกำหนดปลายทางของแต่ละแพ็กเกตไปยังหมายเลขไอพีอื่นได้ ซึ่งช่วยให้การทำ Registration ของ MIPv6 เป็นไปได้ง่ายในการส่งแพ็กเกตไปยังปลายทางที่ต้องการได้อย่างถูกต้อง

การเคลื่อนที่เปลี่ยนระบบเครือข่าย (Handover)

เมื่อ MN มีการเคลื่อนย้ายข้ามระหว่างระบบเครือข่ายอย่างต่อเนื่อง สามารถทำได้ด้วยอัลกอริทึมการทำงานและลำดับสัญญาณดังเดิม โดยใช้การอ้างอิงค่า COA ใหม่เปลี่ยนจากค่า COA เก่า ดังนี้



รูปที่ 6 แสดงการทำ Handover ด้วย MIPv6

(ที่มา: Kyeong-Jin Lee, 2001)

จากรูปที่ 6 แสดงการทำ Handover ด้วย MIPv6 โดย MN ทำการเคลื่อนย้ายจาก Foreign Network เดิม ไปยัง Foreign Network ใหม่ ลำดับการส่งสัญญาณและรูปแบบการทำงานยังคงเป็นไปตามมาตรฐานของ MIPv6 ซึ่งที่แตกต่างไปจากรูปแบบการทำงานพื้นฐานคือ การส่งสัญญาณเพื่อทำการ Registration นั้นมีจุดมุ่งหมายในการเปลี่ยนค่า COA จาก COA เก่าเป็น COA ใหม่

1. เมื่อ MN ทำการเคลื่อนย้ายจาก Foreign Network ไปยัง Foreign Network ใหม่ MN ทำการส่งสัญญาณ Binding Update ไปยัง HA เพื่อเปลี่ยนแปลงค่า COA ทันทีที่ MN ทำการตรวจสอบและรับรู้ว่ามีการเคลื่อนย้ายเปลี่ยนระบบเครือข่าย (Movement Detection)
2. เมื่อ HA ได้รับสัญญาณ Binding Update จาก MN ซึ่งมีทั้งค่า COA เก่าและใหม่ HA ยังคงเก็บค่าข้อมูล COA ทั้งหมดไว้
3. HA ส่งสัญญาณ Binding Acknowledgement กลับไปยัง MN
4. CN ไม่ทราบว่า MN มีการเปลี่ยนแปลง COA จึงยังคงส่งข้อมูลแพ็กเกตไปยัง MN ด้วยค่า COA เก่า ดังนั้นข้อมูลแพ็กเกตนี้จะถูกดักและทำ Tunneling โดย HA และส่งต่อไปยัง MN
5. เมื่อ MN ได้รับข้อมูลแพ็กเกตนี้ จึงส่งสัญญาณ Binding Update ไปยัง CN เพื่อบอกค่า COA ใหม่
6. ค่า COA ได้รับการ update จึงสามารถทำการส่งข้อมูลได้โดยตรงระหว่าง MN และ CN

การลำดับการทำงานดังกล่าวทำให้ในทุกๆครั้งที่มีการ Hand Over เกิดขึ้น MN จะต้องทำการ Binding Update ไปยัง HA และ CN เพื่อทำการปรับค่า COA ใหม่ โดยที่ค่า COA เก่ายังคงถูกเก็บไว้ที่ HA แม้ว่าจะมีการเปลี่ยนแปลงค่า COA เนื่องด้วยอาจมีบางแพ็กเกตที่มีการระบุหมายเลขไอพีปลายทางด้วย COA เก่า จึงทำให้แพ็กเกตเหล่านั้นยังคงสามารถส่งต่อไปยัง MN ได้อย่างถูกต้อง

2.3.4 MIPv4 vs MIPv6

จากคุณสมบัติและการทำงานที่แตกต่างกันระหว่าง MIPv4 และ MIPv6 สามารถสรุปความแตกต่างได้ ดังนี้

ตารางที่ 1 แสดงความแตกต่างระหว่าง MIPv4 และ MIPv6

MIPv4	MIPv6
- ประกอบด้วย Mobile Node, Home Agent, Home Network, Foreign Network	- เหมือนกัน
- Mobile Node อ้างอิงหมายเลขไอพีด้วย Home Address ซึ่งได้จาก Router ของ Home Network นั้น	- หมายเลขไอพีที่ได้เป็น Home Address ถูกกำหนดออกเป็น 2 แบบคือ Globally Routable Home Address และ Link-Local Home Address ตามมาตรฐานของไอพีรุ่นที่ 6
- ระบบประกอบด้วย Foreign Agent เพื่อใช้ทำ Tunneling กับ Home Agent	- ไม่มี Foreign Agent โดยใน MIPv6 ได้รวมการทำงานของ Foreign Agent ไว้ใน Mobile Node
- การทำงานทุกอย่างเป็นไปตาม Agent ของระบบเครือข่ายนั้น	- การทำงานขึ้นอยู่กับ Home Agent และ Router ของแต่ละระบบ
- การทำ Authentication ขึ้นอยู่กับ Home Agent เนื่องจากการส่งข้อมูลจะผ่าน Home Agent ทุกครั้ง	- การทำ Authentication ขึ้นอยู่กับ Home Agent และ Correspondent Node เนื่องจากการส่งข้อมูลจะผ่าน Home Agent เพียงครั้งแรกหากยังไม่มีการ Update COA แต่หลังจากนั้นข้อมูลทุกแพ็กเกตจะถูกส่งโดยตรงระหว่าง Mobile Node และ Correspondent Node
- การ Route ข้อมูลทุกๆแพ็กเกตไปยัง Mobile Node จะถูกทำ Tunneling	- การ Route ข้อมูลทุกๆแพ็กเกตไปยัง Mobile Node จะผ่านการทำ Tunneling และ Source Routing
- มีการนิยามการทำ Route Optimization เพิ่มเติมจากมาตรฐาน MIPv4 เพื่อให้สามารถส่งข้อมูลโดยตรงระหว่าง Mobile Node และ Correspondent Node ได้	- การปรับปรุงระบบของ MIPv6 ทำให้สนับสนุนเกิดการ Route Optimization

จากการเปรียบเทียบการทำงานระหว่าง MIPv4 และ MIPv6 ทำให้พบว่า MIPv6 ถูกออกแบบครอบคลุมการทำงานของ MIPv4 เดิมและปรับปรุงความสามารถในเรื่อง Route Optimization ของ MIPv4 เป็นผลให้ระบบ MIPv6 มีสมรรถนะและประสิทธิภาพการทำงานที่ดีขึ้นกว่าระบบ MIPv4 เดิม

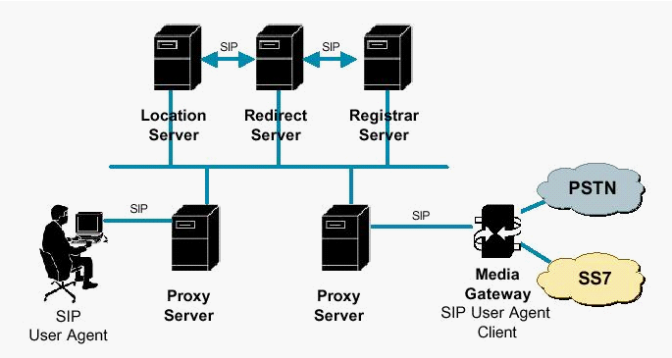
2.4 SIP (Session Initiation Protocol)

โปรโตคอล SIP เป็นโปรโตคอลระดับ Application ถูกพัฒนาโดย IETF (Internet Engineering Task Force) โดยออกแบบให้ใช้ในการตกลงกันระหว่างคู่สนทนาหรือระหว่างผู้ใช้บริการเพื่อทำการเริ่มต้นการโทร (Establish call), เปลี่ยนแปลงรูปแบบการโทร (Modify) และสิ้นสุดการโทรหรือจบการสนทนา (End call/Terminate call) ดังนั้นโปรโตคอล SIP มีหน้าที่รับผิดชอบในส่วนการส่งสัญญาณควบคุม (Control Signaling) ก่อนและจบการสนทนาเท่านั้น นอกจากนี้การทำงานอย่างเป็นระบบตามมาตรฐาน SIP ทำให้เกิดความยืดหยุ่นและความสะดวกในการใช้งานแก่ผู้ใช้บริการมากยิ่งขึ้น

2.4.1 คุณสมบัติของ SIP

1. เป็นโปรโตคอลระดับ Application ซึ่งอยู่เหนือโปรโตคอลระดับ Transport โดยอนุญาตให้สามารถทำการส่งสัญญาณโดยใช้โปรโตคอลระดับ Transport ได้ทั้งชนิด TCP (Transmission Control Protocol) และ UDP (User Datagram Protocol)
2. รูปแบบสัญญาณที่นิยามตามมาตรฐาน SIP มีลักษณะเป็นข้อความ (Text-Based) ซึ่งถูกเรียกว่า SIP Message โดยรูปแบบและไวยากรณ์ของสัญญาณมีลักษณะคล้ายกับรูปแบบสัญญาณของโปรโตคอล HTTP (Hypertext Transfer Protocol) ทำให้ผู้พัฒนาสามารถพัฒนาได้ง่าย และเหตุที่มีการใช้สัญญาณ SIP Message ตลอดขั้นตอนการส่งสัญญาณควบคุมรวมถึงลำดับขั้นตอนการส่งสัญญาณตามมาตรฐาน SIP ไม่ซับซ้อนจึงทำให้โปรโตคอล SIP สามารถทำงานได้รวดเร็วกว่ามาตรฐาน H.323
3. ตามมาตรฐานของ SIP จะรับผิดชอบขั้นตอนการส่งสัญญาณควบคุมในส่วนก่อนและหลังการสนทนาเท่านั้น โดยในขั้นตอนการส่งข้อมูลมัลติพหุสื่อ (Media Stream) จะใช้โปรโตคอล RTP (Real-Time Transfer Protocol) และในขั้นตอนการแลกเปลี่ยนความสามารถในการส่งข้อมูลมัลติพหุสื่อ (Media Capabilities Exchange) จะใช้โปรโตคอล SDP (Session Description Protocol) ทำงานร่วมด้วย
4. สถาปัตยกรรมตามมาตรฐาน SIP เป็นแบบ Client/Server โดยมีการอ้างอิงตัว SIP Client โดยใช้ชื่ออ้างอิงถึงที่อยู่ของตัว SIP Client นั้นๆซึ่งถูกเรียกว่า SIP URL (Uniform Resource Locators) ทำให้เกิดความสะดวกและความยืดหยุ่นในการใช้บริการเพิ่มมากขึ้น รวมถึงการให้บริการแบบ User Mobility ซึ่งจะกล่าวถัดไป

2.4.2 องค์ประกอบสำคัญในระบบ SIP (SIP Component)



รูปที่ 7 องค์ประกอบสำคัญในระบบ SIP

จากรูปที่ 7 แสดงภาพรวมของระบบ SIP ที่ประกอบด้วยส่วนต่างๆที่ทำงานร่วมกันอย่างเป็นระบบ เนื่องจากโปรโตคอล SIP มีการทำงานแบบ Client/Server ดังนั้นจึงสามารถแบ่งออกเป็น 2 ส่วนหลัก คือ User Agent (SIP Client) และ Network Server (SIP Server)

2.4.2.1 User Agent

เป็นนิยามของ SIP Client ภายในระบบ SIP โดยสามารถแยกเป็น 2 รูปแบบการทำงาน คือ

- UAC (User Agent Client) ทำหน้าที่ในการสร้างหรือเริ่มต้นการโทรโดยส่งสัญญาณร้องขอ (Request Signal) ไปยังปลายทาง
- UAS (User Agent Server) ทำหน้าที่ในการตอบรับการโทรและส่งสัญญาณตอบกลับ (Response Signal)

โดยปกติแล้ว SIP Client จะทำหน้าที่เป็นได้ทั้ง UAC และ UAS เพื่อให้สามารถทำงานได้ทั้งเป็นผู้โทร (Caller) และผู้ถูกเรียก (Callee)

2.4.2.2 Network Server

เป็นนิยามของ SIP Server ที่มีรูปแบบการทำงานแบบต่างๆ ได้แก่

- Registrar Server ทำหน้าที่รับการลงทะเบียนจากผู้ใช้บริการ (SIP Client) เพื่อเก็บข้อมูลที่อยู่ ชื่อ SIP URL และข้อมูลสำคัญๆของผู้ใช้บริการ
- Proxy Server ทำหน้าที่เป็นตัวกลางในการส่งสัญญาณระหว่างผู้โทร (Caller) และผู้ถูกเรียก (Callee) โดยรับผิดชอบการส่งสัญญาณตลอดขั้นตอนการส่งสัญญาณตามมาตรฐาน SIP

- Redirect Server ทำหน้าที่ระบุที่อยู่ของผู้ถูกเรียก (Callee) ที่ได้ทำการลงทะเบียนไว้ โดยจะส่งที่อยู่ที่ค้นหาได้กลับไปยังผู้โทร (Caller)

นอกจาก User Agent และ Network Server แล้วภายในระบบ SIP ยังมีส่วนการทำงานอื่นๆ ได้แก่

- Location Server ทำหน้าที่ในการเก็บข้อมูลหรือเป็นฐานข้อมูลผู้ใช้บริการให้กับตัว Network Server ได้ ทำให้ป้องกันปัญหาเรื่องของขนาดฐานข้อมูลไม่เพียงพอและความปลอดภัยของข้อมูลได้ ตามมาตรฐาน SIP อนุญาตให้สามารถพัฒนาตัว Location Server ไว้เป็นตัวเดียวกันกับตัว SIP Server ได้
- SIP Gateway ทำหน้าที่ในการแปลงสัญญาณและข้อมูลมัลติพหุสื่อระหว่างระบบเครือข่ายที่แตกต่างกัน เช่น การเชื่อมต่อไปยังระบบ PSTN (Public Switching Telephone Network), ระบบ SS7 (Signaling System 7) เป็นต้น

2.4.3 SIP Message

ในการติดต่อระหว่างเอนทิตี้จะติดต่อโดยการใช้ SIP Message ซึ่งตามมาตรฐานของ SIP มีการนิยาม SIP Message ออกเป็น 2 ชนิดคือ SIP Message ร้องขอ (Request Message) และ SIP Messageตอบสนอง (Response Message) โดยการส่งสัญญาณ SIP Message อาจจะใช้โปรโตคอล UDP หรือ TCP ในการเชื่อมต่อก็ได้ เอนทิตี้ที่ทำหน้าที่เป็น SIP Client จะส่ง SIP Message ร้องขอเพื่อทำการร้องขอไปยังเอนทิตี้ที่เป็น SIP Server ซึ่งจะตอบสนองต่อ SIP Message ที่ได้รับด้วยการส่ง SIP Messageตอบสนอง รูปแบบทั่วไปของ SIP Message จะประกอบด้วย Start-Line Header บรรทัดว่าง และ Message Body โดยตามมาตรฐาน SIP อนุญาตให้สามารถใช้การ Encryption Authorization หรืออัลกอริทึมที่ใช้ในโปรโตคอลอื่น เช่น HTTP มาช่วยในเรื่องความปลอดภัยได้

SIP Header

ฟิลด์Headerใช้สำหรับระบุรายละเอียดของ การเรียก เช่น ผู้เรียก ผู้ถูกเรียก เส้นทางของ SIP Message ชนิดและความยาวของ Message Body เป็นต้น Header บางชนิดจะมีอยู่ในทุก SIP Message แต่บางชนิดอาจจะใช้ในบาง SIP Message เท่านั้น เอนทิตี้ไม่จำเป็นจะต้องเข้าใจ Header ทั้งหมดโดยที่ Header ที่ไม่เข้าใจ เอนทิตี้จะไม่สนใจ Header นั้น โดย Header จะมีทั้งหมด 37 Header โดยแบ่งเป็น 4 ชนิดดังรูปที่ 8 Header ทั้ง 4 ประเภทมีดังนี้

- General Header เป็น Header ทั่วไป ซึ่งจะอยู่ในทั้ง SIP Message ร้องขอและตอบสนอง

- Entity Header ใช้ระบุข้อมูลเกี่ยวกับ Message Body ถ้าไม่มี Message Body จะเป็นการระบุทรัพยากรที่อ้างอิงถึงโดย SIP Message ร้องขอ

- Request Header ใช้ใน SIP Message ร้องขอของ SIP Client และสามารถส่งข้อมูลเพิ่มเติมเกี่ยวกับการร้องขอของ SIP Client

- Response Header ใช้ใน SIP Message ตอบสนองของ SIP Server และสามารถส่งข้อมูลเพิ่มเติมในการตอบสนองกลับไปให้ SIP Client ได้

General-headers	Entity-headers	Request-headers	Response-headers
Call-ID	Content-Encoding	Accept	Allow
Contact	Content-Length	Accept-Encoding	Proxy-Authenticate
CSeq	Content-Type	Accept-Language	Retry-After
Date		Authorization	Server
Encryption		Contact	Unsupported
Expires		Hide	Warning
From		Max-Forwards	WWW-Authenticate
Record-Route		Organization	
Timestamp		Priority	
To		Proxy-Authorization	
Via		Proxy-Require	
		Route	
		Require	
		Response-Key	
		Subject	
		User-Agent	

รูปที่ 8 SIP header

Request message

SIP Message ร้องขอจะมีลักษณะดังนี้ ในบันทัดแรกจะประกอบด้วย ชื่อ SIP Method วรรคตามด้วยชื่อ Request-URI หรือชื่อ SIP URL ของผู้ใช้ปลายทางที่ต้องการติดต่อ วรรคและจบบันทัดด้วยเวอร์ชั่นของโปรโตคอล โดย SIP Method สำหรับการร้องขอจะมีดังนี้คือ

- Invite เป็น Method ที่ใช้ในการเชิญให้ผู้ถูกเรียกหรือ SIP Server เข้าร่วมในเซสชัน โดยภายใน SIP Message จะแสดงรายละเอียดความสามารถของพหุสื่อที่ใช้ได้รวมทั้งพารามิเตอร์หรือรายละเอียดของเซสชันซึ่งจะอยู่ใน Message Body

- Ack ใช้ในการยืนยันว่า SIP Client ได้รับ SIP Message ตอบสนองสุดท้าย (Final Response) สำหรับ SIP Message ร้องขอซึ่งใช้ Invite Method แล้ว โดยที่ภายใน Message Body อาจจะมีรายละเอียดเซสชัน (Session Description) ถ้าไม่มีข้อมูลใน Message Body ผู้ถูกเรียกจะใช้รายละเอียดเซสชันที่อยู่ในSIP Message ร้องขอที่ส่งมาก่อนหน้านี้ Ack Method นี้จะใช้ยืนยันสำหรับตอบสนองต่อ SIP Message ที่ใช้ Invite Method เท่านั้น

- Bye เป็น Method ที่ใช้ในการสิ้นสุด การโทร

- Cancel ใช้ในการยกเลิก การโทร ที่ยังไม่สมบูรณ์ การโทรที่ไม่สมบูรณ์คือ การโทรที่ผู้โทรยังไม่ได้รับการตอบกลับสุดท้าย (Final Response) จากผู้ถูกเรียก

- Option เป็น Method ที่ SIP Clientใช้สำหรับขอข้อมูลที่เกี่ยวกับความสามารถ (Capability) ของ SIP Server เช่น Method หรือ Header ที่ SIP Server เข้าใจ แต่ไม่ได้มีสร้างการเชื่อมต่อหรือสร้างเซสชันใดๆขึ้น

- Register เป็น Method ใช้สำหรับการส่งข้อมูลตำแหน่งของผู้ใช้ (User Location) หรือ Alias Name ให้กับ Registrar Server ซึ่งโดยปกติรวมอยู่ใน SIP Server เป็นผลให้ SIP Client แต่ละตัวมีชื่อ SIP URL อ้างอิงที่อยู่

เมื่อได้ระบุ Method เสร็จสิ้น ต่อไปจะเป็นส่วนของ Request-URI หรือก็คือ SIP URL ซึ่งใช้ระบุถึงผู้ถูกเรียกและจะตามด้วยเวอร์ชั่นของโปรโตคอล ซึ่งเป็นส่วนทั้งสามจะอยู่ใน Start-Line จากนั้นในส่วนต่อมาจะเป็น Header ต่างๆ ที่ใช้บอกเกี่ยวกับรายละเอียดของ การโทร และ SIP Message เช่น Caller, Callee และหัวข้อของการโทร เป็นต้น เมื่อระบุ Header ต่างๆ แล้วต่อไปจะเป็นบรรทัดว่างเพื่อเป็นการแยกระหว่าง Header และ Message Body โดย Message Body จะใช้แสดงความสามารถ เช่น พหุสื่อ หรือการเข้ารหัสที่ใช้ ของ SIP Client นั้นเพื่อกำหนดพารามิเตอร์ของเซสชัน โดยส่วนนี้ก็คือส่วนที่อธิบายรายละเอียดต่างๆของเซสชันที่จะใช้ สำหรับ Message Body จะสามารถอธิบายความหมายได้โดยดูจากที่ระบุไว้ใน Header Content-Type โดยทั่วไปแล้วจะใช้โปรโตคอล SDP (Session Description Protocol) ในการอธิบายดังรูปที่ 9

```
INVITE sip:pgn@example.se SIP/2.0
Via: SIP/2.0/UDP science.fiction.com
From: Fingal <sip:ffl@fiction.com
To: Patrik <sip:pgn@example.se>
Call-ID: 1234567890@science.fiction.com
CSeq: 1 INVITE
Content-Type: application/sdp
Content-Length: …

v=0
o=ffl 53655765 2353687637 IN IP4 123.4.5.6
s=Chorizo
c=IN IP4 science.fiction.com
m=audio 5004 RTP/AVP 0 3 5
```

รูปที่ 9 SIP request

Response message

เมื่อ SIP Server ได้รับ SIP Message จะทำการประมวลผล SIP Message แล้วจึงทำการตอบสนองโดยการส่ง SIP Message ในบรรทัดแรกของ SIP Message หรือเรียกว่า Status-Line จะแสดงผลของการร้องขอโดยใช้ Response Code คล้ายคลึงกับโปรโตคอล HTTP ซึ่งจะเป็นตัวเลข 3 ตัว ตัวเลขตัวแรกจะเป็น Response Class ตัวเลขที่ 2 และ 3 จะเป็นรายละเอียดของการประมวลผล สำหรับ Response Class จะแบ่งเป็น 2 ประเภทคือ Provisional Response เพื่อใช้บอกว่ายังอยู่ระหว่างรอการตอบรับจากผู้ถูกเรียกหรือ SIP Server อื่นซึ่งได้แก่ 1XX และอีกประเภทหนึ่งคือ Final Response เป็นการตอบสนองสุดท้ายของการร้องขอนั้น ซึ่งจะได้แก่ 2XX 3XX 4XX 5XX และ 6XX โดยการที่ได้รับ Final Response เท่านั้นจึงจะถือว่าทำให้ การโทรในครั้งนั้นสมบูรณ์ เอนทิตี้ไม่จำเป็นจะต้องเข้าใจ Response Code ทั้งหมด แต่จะต้องเข้าใจความหมายของ Response Class ทุกคลาส เมื่อเอนทิตี้ไม่เข้าใจใน Response Code จะตีความหมายเป็น Response Code เป็น X00 ของ Response Class X ซึ่ง Response Class จะเหมือนกับโปรโตคอล HTTP หลังจาก Response Code จะตามด้วยความหมายของ Code ซึ่งเป็นภาษาที่สามารถอ่านได้ เช่น OK โดยใน Status Line นี้จะประกอบด้วยเวอร์ชั่นของโปรโตคอล Response Code และความหมายของ Code ตามลำดับ หลังจาก Status Line แล้วต่อไปจะเป็น Headerต่างๆ ตามด้วยบรรทัดว่างและ Message Body ใน Message Body จะใช้บอกความสามารถของ SIP Server เพื่อใช้กำหนดพารามิเตอร์เซสชันเช่นเดียวกับ SIP Message ร้องขอ โดยพารามิเตอร์ที่ใช้ในเซสชันจะเป็นความสามารถร่วมของทั้ง 2 ฝ่าย ซึ่งตัวอย่างของ SIP Message ตอบสนองจะมีลักษณะดังรูปที่ 10 (สำหรับรายละเอียดของสัญญาณทั้งหมดสามารถศึกษาเพิ่มเติมได้จาก RFC3261)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP sippo.example.se
Via: SIP/2.0/UDP science.fiction.com
From: Fingal <sip:ffl@fiction.com
To: Patrik <sip:pgn@example.se>
Call-ID: 1234567890@science.fiction.com
CSeq: 1 INVITE
Content-Type: application/sdp
Content-Length: …

v=0
o=pgn 4858949 4858949 IN IP4 198.7.6.5
s=Ok
c=IN IP4 pepperoni.example.se
m=audio 5004 RTP/AVP 0 3
```

รูปที่ 10 SIP Response

2.5 ความสามารถในการเคลื่อนย้ายของโปรโตคอล SIP (SIP Mobility)

สำหรับการทำโมไบลิตี้ด้วยโปรโตคอล SIP นั้นมีการให้แนวความคิดในเรื่องของรูปแบบการทำโมไบลิตี้มากมาย แต่ไม่มีการระบุวิธีการหรืออัลกอริทึมในการพัฒนาโปรแกรมประยุกต์ที่สามารถทำงานตามรูปแบบโมไบลิตี้แบบต่างๆ ซึ่งสามารถสรุปรูปแบบการทำโมไบลิตี้ได้ดังต่อไปนี้

การบริการโมไบลิตี้สามารถแบ่งได้ 4 แบบด้วยกันดังนี้

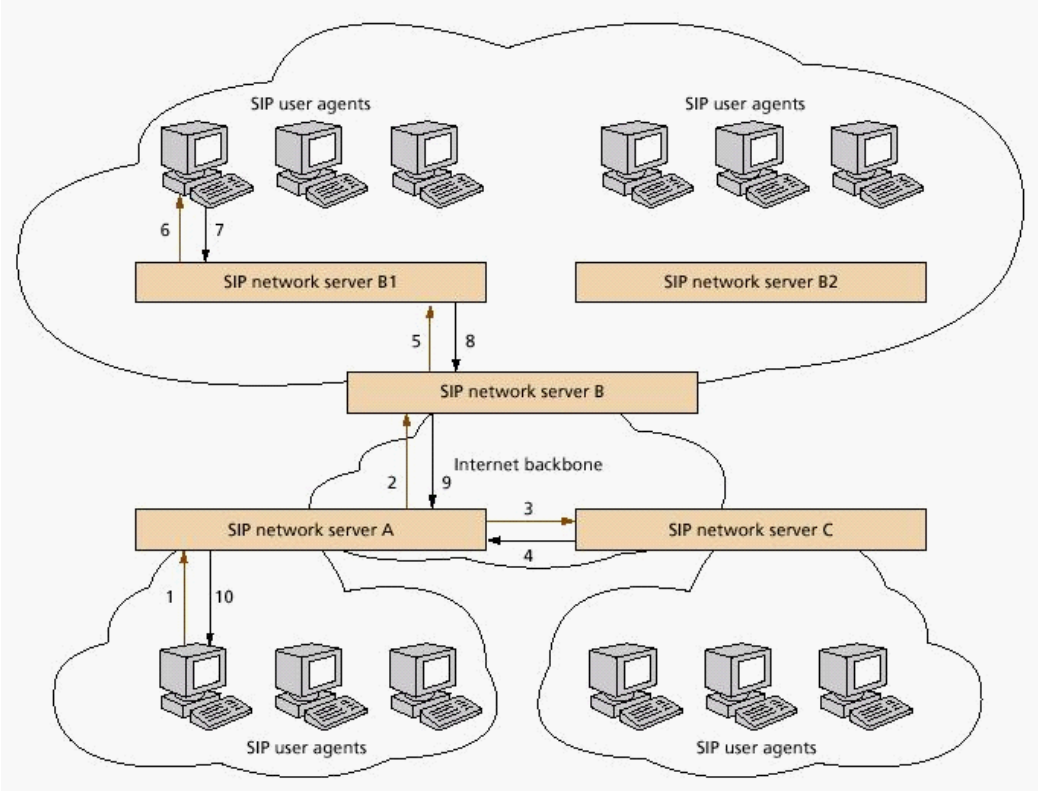
1. Terminal Mobility : เป็นการบริการหาที่อยู่ของผู้ใช้เมื่อมีการเปลี่ยนแปลงที่อยู่ โดยทั่วไปเป็นการใช้หลักการทำงานของ Redirect ในการติดต่อผ่านทางตัว SIP Server
2. Personal Mobility : เป็นการบริการเพื่อให้สามารถให้บริการ SIP Client ได้ไม่ว่า SIP Client จะใช้อุปกรณ์ใด เช่น คอมพิวเตอร์ โทรศัพท์ และโทรศัพท์มือถือ เป็นต้น โดยยังคงใช้ SIP URL เดียวกัน นั่นคือผู้ใช้ปลายทางสามารถใช้อุปกรณ์สื่อสารประเภทใดก็ได้ด้วยชื่อ SIP URL เดิมแต่ยังคงสามารถรับการติดต่อได้
3. Session Mobility : เป็นการบริการโดยระบบยังคงรักษาการส่งข้อมูลพหุสื่อ แม้ว่าจะมีการเปลี่ยนแปลงตำแหน่งหรือมีการเคลื่อนย้ายที่อยู่ของผู้ใช้ได้ ได้แก่ การโอนสายโทรศัพท์ เป็นต้น
4. Service Mobility : เป็นบริการที่เกิดขึ้นเมื่อมีการให้บริการโมไบลิตี้อยู่ นั่นคือ SIP Server จะทำการรักษาการบริการของผู้ใช้หากต้องมีการทำโมไบลิตี้ ซึ่งบริการเหล่านี้ได้แก่ ข้อมูลสมุดโทรศัพท์, ข้อมูลผู้ใช้ที่ออนไลน์, รายละเอียดของรูปแบบพหุสื่อที่ต้องการส่งข้อมูล เป็นต้น

2.5.1 ตัวอย่างการทำโมไบลิตี้แบบต่างๆ

- Terminal Mobility เนื่องจากเป็นหน้าที่ของ SIP Server หากเป็นแบบ Proxy Server ในการรับผิดชอบการหาที่อยู่ของผู้ถูกร้องขอการติดต่อ เมื่อพบว่าผู้ถูกร้องขอการติดต่อนั้นได้ทำการ Register ไว้มากกว่า 1 ที่อยู่ โดยอัลกอริทึมที่ใช้คือการแตกการทำงานออกไปเพื่อติดต่อไปยังทุกๆที่อยู่ที่มีนั้น เรียกว่า Forking โดยจะต้องทำการติดต่อไปยังแต่ละ SIP Server จนกว่าจะสามารถระบุอยู่ที่แน่นอนของผู้ถูกร้องขอการติดต่อได้

รูปที่ 11 แสดงตัวอย่างการสอบถามหาที่อยู่ของผู้ถูกร้องขอการติดต่อไปตาม SIP Server ที่ใกล้เคียงกัน โดย SIP Server ในรูปนี้จะทำงานเป็น Proxy Server นั่นคือจะเป็นตัวกลางในการติดต่อระหว่างผู้ร้องขอการติดต่อกับผู้ถูกร้องขอการติดต่อ จากรูปเริ่มแรก SIP Server A ได้รับ Request Message (1)

จาก SIP User Agent ซึ่งเป็นผู้ร้องขอการติดต่อ ตัว SIP Server A จะทำการติดต่อไปยัง SIP Server B (2) และ C (3)ปรากฏว่า SIP Server C ส่ง Response Message (4) ให้กับ SIP Server A เพื่อบอกว่าไม่พบที่อยู่ของผู้ถูกร้องขอการติดต่อในเครือข่ายของ SIP Server C แต่เนื่องจากยังมี SIP Server ถัดไปจาก SIP Server B จึงมีการถามต่อไปยัง SIP Server B1 (5)และ B2 แต่ SIP Server B1 สามารถพบที่อยู่ของผู้ถูกร้องขอการติดต่อก่อนโดย SIP Server B1 ทำการส่ง Request Message (6)ไปยัง SIP User Agent ที่เป็นผู้ถูกร้องขอการติดต่อ แล้วได้รับ Response Message (7) กลับมาจึงไม่จำเป็นต้องติดต่อไปยัง SIP Server B2 จากนั้น Response Message นี้ก็จะถูกส่งต่อไปจาก SIP Server B2 ไปยัง SIP Server B (8) แล้วจาก SIP Server B ไปยัง SIP Server A (9) ตามลำดับ สุดท้าย SIP Server A จะส่ง Response Message(10) ไปยัง SIP User Agent ที่เป็นผู้ร้องขอการติดต่อเพื่อแสดงว่าสามารถทำการติดต่อไปยังผู้ถูกร้องขอการติดต่อได้สำเร็จ



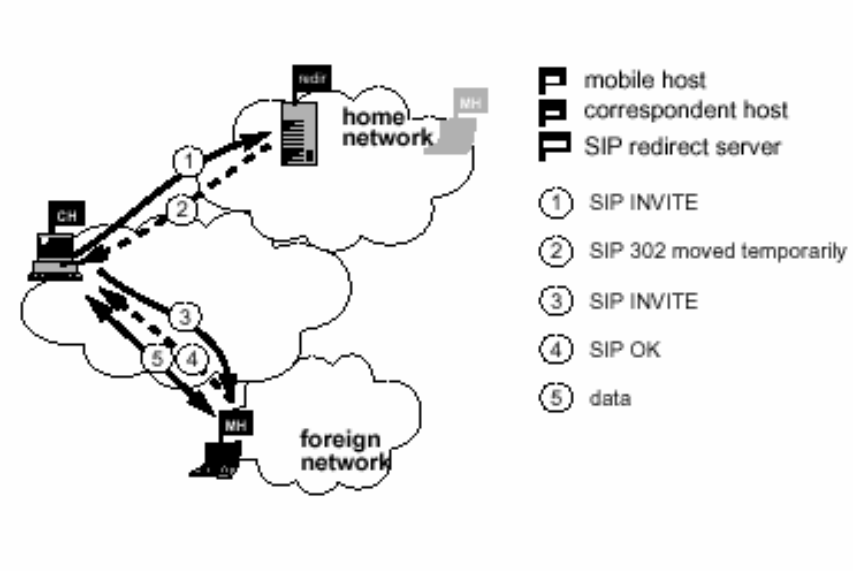
รูปที่ 11 แสดงการสอบถามหาที่อยู่ไปตามแต่ละ SIP Server

(ที่มา: H. Schulzrinne, 1998)

หมายเหตุ: หาก SIP Server A ทำงานเป็น Redirect Server เมื่อทำการสอบถามที่อยู่จาก SIP Server แต่ละตัวจะไม่มีการติดต่อไปยัง SIP Client ที่เป็นผู้ถูกร้องขอการติดต่อ แต่ SIP Server แต่ละตัว

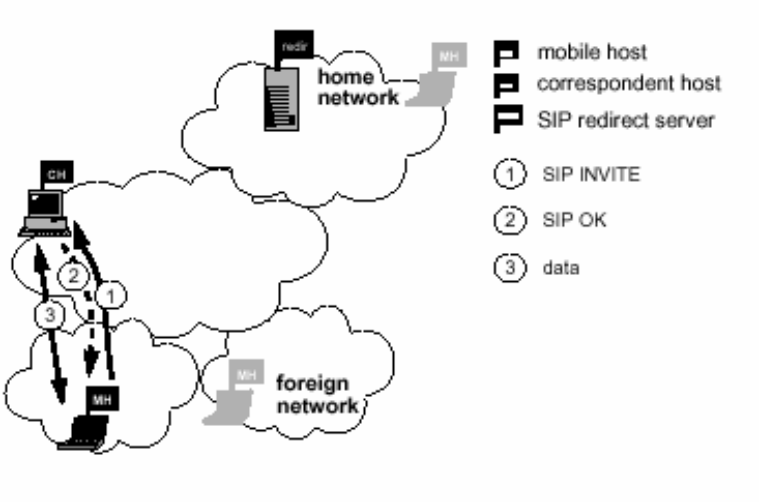
เมื่อสามารถหาที่อยู่ของผู้ร้องขอการติดต่อได้แล้วจะส่งมาให้ SIP Server A ทั้งหมด แล้ว SIP Server A จึงส่งที่อยู่ทั้งหมดที่หาได้ไปยัง SIP Client ที่เป็นผู้ร้องขอการติดต่อ

การให้บริการแบบ Terminal Mobility อาจเกิดขึ้นได้หลายกรณี เช่น ในกรณีที่ SIP Client ทำการ Register ไว้ที่ SIP Server มากกว่า 1 ที่อยู่หรือเกิดการเปลี่ยนแปลงที่อยู่ขณะที่ทำการติดต่ออยู่เป็นต้น ในกรณีที่พบที่อยู่มากกว่า 1 ที่อยู่ หากเป็น SIP Proxy Server จะทำการทำ Forking ติดต่อไปยังทุกๆที่อยู่นั้นเพื่อหาตำแหน่งปัจจุบันที่ต้องการ แต่หากเป็น SIP Redirect Server จะส่งที่อยู่ที่หาได้ทั้งหมดมาให้ SIP Client เป็นผู้ทำ Forking เอง สำหรับกรณีที่ในขณะทำการติดต่ออยู่เกิดการเปลี่ยนแปลงที่อยู่ SIP Client นั้นๆต้องทำการเริ่มขั้นตอนการทำงานใหม่ทั้งหมด นั่นคือต้องทำการส่ง INVITE Message ก่อน โดยสามารถทำการบอกที่อยู่ใหม่ได้ 2 วิธี คือ ทำการ Register ใหม่อีกครั้ง เพื่อบอกที่อยู่ปัจจุบัน และ ทำการบอกที่อยู่ใหม่ด้วย INVITE Message ที่ส่งไป



รูปที่ 12 แสดงตัวอย่าง Terminal Mobility ในขั้นตอน Call Setup

(ที่มา: H. Schulzrinne, 2000)



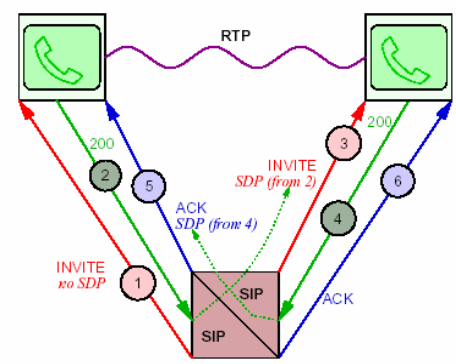
รูปที่ 13 แสดงตัวอย่าง Terminal Mobility เมื่อเกิดการเปลี่ยนแปลงที่อยู่

(ที่มา: H. Schulzrinne, 2000)

จากรูปที่ 12 และรูปที่ 13 เป็นการแสดงการทำ Terminal Mobility เมื่อ SIP Client เกิดการเปลี่ยนแปลงที่อยู่จากเดิม ในที่นี้ Server จะเป็นแบบ Redirect Server ดังจะเห็นได้ว่าเมื่อ SIP Client ทำการถามที่อยู่จาก SIP Redirect Server ได้แล้วก็จะทำการติดต่อไปยัง SIP Client ปลายทางเอง ดังรูปที่ 12 และทำตามขั้นตอนการทำงานต่อไป แต่เมื่อ SIP Client ที่เป็นผู้ถูกร้องขอการติดต่อเกิดการเปลี่ยนแปลงที่อยู่ SIP Client ที่เป็นผู้ถูกร้องขอการติดต่อเมื่อย้ายที่อยู่แล้วก็ต้องทำการส่ง INVITE Message ไปให้กับผู้ร้องขอการติดต่อใหม่อีกครั้งเพื่อบอกตำแหน่งที่อยู่ปัจจุบันนั่นเอง ดังรูปที่ 13

- สำหรับการทำ Service Mobility มักจะเป็นการให้บริการโดย SIP Server เมื่อ SIP Server ต้องทำการบริการแบบ Terminal Mobility ดังนั้นหาก SIP Server ใดที่สามารถให้บริการ Terminal Mobility ได้ควรจะสามารถให้บริการ Service Mobility ได้ด้วย

- สำหรับการบริการแบบ Session Mobility เป็นการอนุญาตให้ผู้ใช้รักษาสถานะการส่งข้อมูลพหุสื่อไว้ในขณะที่ทำงานเปลี่ยนแปลงอุปกรณ์สื่อสารได้ ตัวอย่างเช่น ผู้โทรอาจจะต้องการโทรศัพท์ต่อเนื่องจากโทรศัพท์มือถือเปลี่ยนไปเป็นเครื่องคอมพิวเตอร์ตั้งโต๊ะ (Desktop PC) เมื่อผู้ใช้เข้าไปยังห้องทำงาน เป็นต้น โดยการบริการรูปแบบนี้จะทำงานรักษาการส่งข้อมูลไม่ว่าจะเป็นข้อมูลภาพและเสียงไปยังอุปกรณ์สื่อสารตัวใหม่ได้ ซึ่งการทำงานในลักษณะนี้คล้ายกับการทำงานของระบบโทรศัพท์ที่สามารถทำการโอนสายไปยังอีกเครื่องหนึ่งได้ตามต้องการ

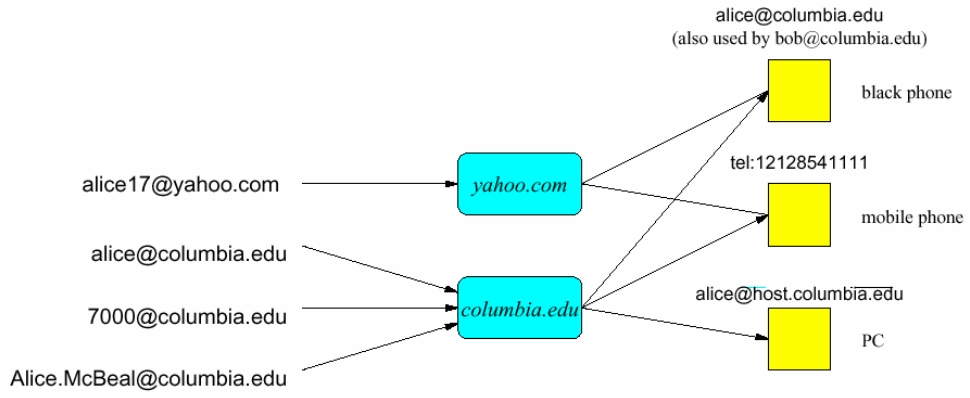


รูปที่ 14 แสดงตัวอย่างการส่งสัญญาณในรูปแบบการทำ Session Mobility

(ที่มา: H. Schulzrinne, 2000)

จากรูปที่ 14 แสดงลำดับสัญญาณของ SIP เมื่อมีการเปลี่ยนแปลง Session การส่งข้อมูลพหุสื่อใหม่ เริ่มต้นเมื่อผู้ใช้มีการย้าย Session การติดต่อไปยังอุปกรณ์ใหม่ ผู้ใช้จะจำเป็นต้องทำการส่งสัญญาณร้องขอการติดต่อตามลำดับสัญญาณของ SIP ใหม่ทั้งหมดเพื่อทำการกำหนดค่ารูปแบบการส่งข้อมูลพหุสื่อและกำหนดค่าต่างๆที่สำคัญบนอุปกรณ์ใหม่นั้นก่อน นั่นคือ ส่งสัญญาณ INVITE เพื่อร้องขอและแลกเปลี่ยนข้อมูลเกี่ยวกับพหุสื่อที่ต้องการ (1)(3) โดยมีตัวกลางจะการตกลงให้เข้าใจตรงกันทั้ง 2 ฝ่าย ในที่นี้อาจเป็นการทำงานโดยตัว SIP Server ที่ทำหน้าที่ควบคุมการโทรศัพท์ของคู่การติดต่อนี้ เมื่อทำการตกลงกันเรียบร้อยแล้วจะมีการส่งสัญญาณ 200 OK เพื่อตกลงการกำหนดค่า (2)(3)(4) และเมื่ออีกฝ่ายได้รับสัญญาณ 200 OK จะทำการยืนยันครั้งสุดท้าย (5)(6) ก่อนเริ่มการส่งข้อมูลพหุสื่อซึ่งในที่นี้คือการส่งข้อมูลเสียงผ่านโปรโตคอล RTP (Real-Time Transport Protocol)

- สำหรับการบริการแบบ Personal Mobility หน้าที่ในการให้บริการจะอยู่ที่ SIP Gateway ในการระบุความสัมพันธ์ระหว่าง SIP URL กับที่อยู่จริงๆของ SIP Client ซึ่งอาจจะเป็นโทรศัพท์มือถือหรือเครื่องคอมพิวเตอร์ เป็นต้น โดยยังคงใช้ SIP URL เดียวกัน ดังตัวอย่างรูปที่ 15 ด้านล่างนี้



รูปที่ 15 แสดงการทำ Personal Mobility

(ที่มา: H. Schulzrinne, 2000)

จากรูปที่ 15 สังเกตได้ว่า SIP Client มีการใช้อุปกรณ์แตกต่างกันได้แก่ โทรศัพท์ (Black Phone), โทรศัพท์เคลื่อนที่ (Mobile Phone) และ คอมพิวเตอร์ (PC - Personal Computer) นั่นคือหากมีการติดต่อไปยังClientด้วย SIP URL alice@columbia.edu หรือ alice17@yahoo.com ตัว SIP Server จะสามารถหาที่อยู่ของปลายทางได้มากกว่า 1 ที่อยู่ โดยแต่ละที่อยู่อ้างอิงอุปกรณ์ใช้งานที่แตกต่างกัน

2.6 เปรียบเทียบข้อแตกต่างระหว่างการทำโมไบลิตี้ด้วย Mobile IP และ SIP

จากหัวข้อที่ 2.4 และ 2.5 แสดงให้เห็นถึงความสามารถในการทำโมไบลิตี้ด้วยโปรโตคอล Mobile IP และโปรโตคอล SIP ซึ่งพบว่าการทำงานด้วยโปรโตคอลทั้ง 2 แบบมีความสามารถและความรับผิดชอบอยู่ในระดับชั้นแตกต่างกัน เป็นผลให้ความสามารถหรือรูปแบบการทำโมไบลิตี้เกิดขึ้นแตกต่างกันตามไปด้วย ซึ่งสามารถสรุปข้อแตกต่างในประเด็นที่สำคัญระหว่างทั้ง 2 โปรโตคอลโดยพิจารณาในแง่ของการทำโมไบลิตี้ได้ดังนี้

ตารางที่ 2 เปรียบเทียบความสามารถการทำ Mobility ของ SIP และ MIPv6

SIP Mobility	MIPv6 Mobility
- เป็นการทำงานในระดับ Application-Layer	- เป็นการทำงานในระดับ Network-Layer
- สนับสนุนการทำ Hierarchical Routing คือการค้นหาที่อยู่ของโหนดปลายทางตามชื่อ SIP URL แบบเป็นลำดับขั้น	- อาศัย Router และ Home Agent ในการติดต่อไปยังโหนดปลายทาง
- สนับสนุนการทำ Session Mobility, Service Mobility และ Personal Mobility	- ไม่มีการจัดการในส่วนของการทำ Session Mobility, Service Mobility และ Personal Mobility
- สามารถรองรับการเกิด Hand Over ขึ้นได้ โดยใช้ Terminal Mobility	- สนับสนุนการทำ Terminal Mobility/Smooth Hand Over

2.7 สรุป

เนื่องจากความต้องการของผู้ใช้ระบบเครือข่ายมีจำนวนเพิ่มมากขึ้นตลอดจนเทคโนโลยีการสื่อสารที่มีการพัฒนาก้าวล้ำอย่างรวดเร็ว เป็นผลให้ความต้องการหมายเลขไอพีเพิ่มมากขึ้นจนไม่เพียงพอต่อความต้องการของผู้ใช้ ดังนั้นจึงมีการนิยามโปรโตคอลไอพีรุ่นที่ 6 ขึ้นซึ่งสามารถให้จำนวนหมายเลขไอพีให้แก่ผู้ใช้ได้อย่างเพียงพอ การเกิดขึ้นของโปรโตคอลไอพีรุ่นที่ 6 เป็นผลให้เทคโนโลยีการสื่อสารในยุคต่อไปมีการเปลี่ยนแปลงและออกแบบให้รองรับโปรโตคอลไอพีรุ่นที่ 6 ได้ในอนาคต เมื่อมองถึงแง่ของการทำโมไบลิตี้เพื่อประโยชน์ในการทำงานในระบบไอพีเทเลโฟนนี่แล้ว พบว่ามี 2 โปรโตคอล ด้วยกันที่มีความสามารถในการทำโมไบลิตี้ในรูปแบบที่แตกต่างกัน นั่นคือ โปรโตคอล Mobile IP และโปรโตคอล SIP โดยทั้ง 2 โปรโตคอลนี้สามารถทำโมไบลิตี้ได้บนระดับชั้น Network และ Application ตามลำดับ

อย่างไรก็ตามทั้งโปรโตคอล SIP และโปรโตคอล Mobile IP ต่างมีข้อจำกัดในเรื่องขอบเขตการทำงาน ความสามารถ และบริการที่มีแตกต่างกัน ดังนั้นการจะทำให้การทำโมไบลิตี้ให้มีสมรรถนะสูงสุด อาจต้องมีการนำความสามารถของทั้ง 2 โปรโตคอลมาประยุกต์ใช้งานร่วมกัน ในหัวข้อถัดไปจะกล่าวถึงแนวทางในการนำทั้ง 2 โปรโตคอลมาสร้างเป็นระบบโมไบลิตี้ระบบใหม่ขึ้นเพื่อให้เกิดความสามารถและมีสมรรถนะสูงสุด