บทที่ 2
มาตรฐาน โพรโทคอลและทฤษฎีที่เกี่ยวข้อง

การทำงานของระบบเครือข่ายอินเทอร์เน็ตนั้น อาศัยการทำงานของมาตรฐานการสื่อสารแบบ TCP/IP ซึ่งสามารถสรุปโดยย่อ เปรียบเทียบกับมาตรฐานลักษณะการสื่อสารบนระบบเครือข่าย ตาม ISO/OSI Model ได้ดังนี้

Layer	ISO/OSI	TCP/IP (Internet)
7	Application	Telnet, FTP, SMTP, HTTP, DNS, BOOTP,DHCP,SNMP
6	Representation	
5	Session	
4	Transport	TCP , UDP
3	Network	IP , ICMP , IGMP
2	Data Link	Device Driver and Interface
1	Physical	Media

ภาพที่ 1 เปรียบเทียบมาตรฐาน ISO/OSI Model กับ มาตรฐาน TCP/IP

การสื่อสารบนระบบเครือข่ายอินเทอร์เน็ตนั้น จะอาศัย IP เป็นหลักโดยเครื่องคอมพิวเตอร์ และ อุปกรณ์ต่างๆ บนระบบเครือข่าย จะต้องมีตำแหน่ง IP เฉพาะของตัวเองที่ไม่ซ้ำกับใคร และบริการต่างๆ นั้นจะส่งข้อมูลถึงกันระหว่างเครื่องคอมพิวเตอร์ ผ่านทาง TCP หรือ UDP เป็นหลัก ทั้งนี้ขึ้นกับประเภทของการใช้งาน

ในที่นี้ Physical Layer และ Data Link Layer ใช้มาตรฐานของอีเทอร์เน็ต (IEEE802.3) ในขณะที่ TCP และ IP จะครอบคลุมการทำงานในระดับ Network และ Transport Layer ส่วนการทำงานของ HTTP หรือ เว็บเซิร์ฟเวอร์นั้นจะอยู่ในระดับ Session, Representation และ Application

2.1. แนวทางการพัฒนา Web Device

การทำให้อุปกรณ์ที่ต้องการควบคุม สามารถควบคุมได้ผ่านทางเครือข่ายเว็บนั้น คือ การทำให้อุปกรณ์ดังกล่าวฉลาด (มีโพรเซสเซอร์ ระบบปฏิบัติการ และ TCP) ซึ่ง Rodney

Snell (1999) ได้กล่าวสรุปใน Web-Based Device Monitoring and Control ว่าวิธีการเพื่อทำให้อุปกรณ์ฉลาด สามารถควบคุมได้ผ่านระบบเครือข่ายเว็บนั้น มีด้วยกัน 4 วิธี ดังนี้

- เว็บเซิร์ฟเวอร์แบบฝังตัว (Embedded Web Server) คือ การรวมอุปกรณ์ ในการเชื่อมต่อระบบเครือข่ายอีเทอร์เน็ต เข้ากับอุปกรณ์ที่ต้องการควบคุมโดยตรง ซึ่งจะทำให้อุปกรณ์เหล่านี้ สามารถสื่อสารได้โดยตรงผ่านทางโปรแกรมค้นผ่านเว็บ ประโยชน์ของการใช้วิธีนี้คือสามารถควบคุมได้ง่าย ไม่ต้องการอุปกรณ์ใดเพิ่มเติม อย่างไรก็ดีเนื่องจากเว็บเซิร์ฟเวอร์แบบฝังตัวนั้น มักมีข้อจำกัดในเรื่องหน่วยความจำ ทำให้ไม่สามารถเก็บรูปภาพหรือข้อมูลขนาดใหญ่ได้ นอกจากนี้ยังขาดสูญกลางของการควบคุมอุปกรณ์ ในกรณีที่อุปกรณ์หลายชิ้นต่อพ่วงอยู่กับระบบเครือข่าย และต้องการควบคุมพร้อมๆ กัน
- เว็บเซิร์ฟเวอร์แบบฝังตัว ร่วมกับเว็บเซิร์ฟเวอร์ภายนอกทั่วไป (Embedded Web Server + External Web Server) มีลักษณะคล้ายกับเว็บเซิร์ฟเวอร์แบบฝังตัว แต่จะมีการเสริมความสามารถในการจัดเก็บข้อมูลขนาดใหญ่ เช่น Applet, รูปภาพ หรือข้อมูลขนาดใหญ่ต่างๆ ไว้กับเซิร์ฟเวอร์ภายนอกเพื่อช่วยให้สามารถควบคุมสิ่งที่ซับซ้อนได้มากขึ้น อย่างไรก็ตาม ข้อเสียใหญ่คือค่าใช้จ่ายที่ต้องเพิ่มขึ้นของเว็บเซิร์ฟเวอร์ภายนอก
- เว็บเซิร์ฟเวอร์ภายนอกทั่วไปร่วมกับ CGI (External Web Server + CGI) การออกแบบและการใช้งานนั้น เหมือนกับการใช้งานเว็บเซิร์ฟเวอร์ทั่วไป โดยพัฒนาโปรแกรม CGI (Common Gateway Interface) เพื่อทำการติดต่อกับอุปกรณ์ที่ต้องการควบคุม ซึ่งลักษณะดังกล่าวนี้ ไม่เหมาะกับงานควบคุมที่มีการเปลี่ยนแปลงอย่างรวดเร็ว และมีข้อดีคือสามารถพัฒนาได้ง่ายและรวดเร็ว
- เว็บเซิร์ฟเวอร์ภายนอกที่มีการปรับเปลี่ยนลักษณะบางประการให้เหมาะสม (Customize External Web Server) มีลักษณะคล้ายกับ การพัฒนาผ่านระบบ CGI แต่ เนื่องจาก ข้อเสียของระบบ CGI ดังกล่าว จึงดัดแปลงเซิร์ฟเวอร์ให้สามารถรับและทำการติดต่อกับอุปกรณ์ที่ต้องการควบคุมได้โดยตรง โดยไม่ต้องผ่าน โปรแกรมควบคุมพิเศษอื่น เช่นกรณีของ CGI

ลักษณะดังกล่าวข้างต้นนั้น มักเหมาะสมกับงานในรูปแบบที่แตกต่างกันไป ทั้งนี้ขึ้นอยู่กับปัจจัยต่างๆ เช่น ความเร็วของข้อมูลและการควบคุมที่ต้องการ ชนิดของอุปกรณ์ที่ต้องการควบคุม ความสามารถของอุปกรณ์ควบคุม และ ระบบเครือข่าย อย่างไรก็ดีทุกวิธี สามารถนำมาประยุกต์ใช้งานร่วมกันได้ ในงานวิจัยนี้มุ่งเน้นที่การพัฒนาระบบเว็บเซิร์ฟเวอร์แบบฝังตัวเท่านั้น

2.2. อีเทอร์เน็ต (IEEE 802.3)

การเชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่ายแบบท้องถิ่น(Local Area Network) ในปัจจุบันนั้น นิยมใช้มาตรฐานอีเทอร์เน็ต ซึ่งเป็น Broadband Network ในการเชื่อมต่อ อย่างไรก็ตามในวิทยานิพนธ์ฉบับนี้มิได้มุ่งเน้นที่การทำงานของอีเทอร์เน็ต หากแต่มุ่งเน้นที่การเชื่อมต่ออีเทอร์เน็ตเข้าสู่ไมโครคอนโทรลเลอร์ การเชื่อมต่อตามมาตรฐานอีเทอร์เน็ตโดยทั่วไปนั้นจะอาศัยการทำงานของ Network Interface Controller หรืออุปกรณ์ควบคุมที่มีความสามารถในการจัดรูปแบบ เข้ารหัส และ ถอดรหัสตามมาตรฐาน Manchester ที่ความเร็ว 10Mbs ซึ่งเป็นความเร็วที่สูง เมื่อเปรียบเทียบกับความเร็วของไมโครคอนโทรลเลอร์ที่ใช้ในงานควบคุมทั่วไป

จากการเชื่อมต่อไมโครคอนโทรลเลอร์เข้าสู่ระบบเครือข่ายโดยอาศัย NIC (Network interface Controller) ดังกล่าว หน่วยประมวลผลหลัก จะได้รับข้อมูลที่ผ่านการตรวจสอบความถูกต้องจาก NIC แล้ว และข้อมูลที่ส่งออกจะได้รับการสร้าง Check sum และ เติม Header ให้โดย NIC เช่นกัน ลักษณะการทำงานดังกล่าวสามารถอธิบายได้ดังภาพที่ 2

	PRE	SFD	DES	SRC	TYPE	DATA	FCS
	62b	2b	6B	6B	2B	46B - 1500B	4B
การรับ	ควบคุมโดย NIC		ได้รับข้อมูลผ่าน DMA				
การส่ง	ควบคุมโดย NIC		ได้รับข้อมูลผ่าน DMA				คำนวณโดย NIC

"B" – Bytes

"b" – bits

ภาพที่ 2 ลักษณะเฟรมของ Ethernet

จากภาพที่ 2 พบว่า ข้อมูลบางส่วนได้รับการประมวลผลโดย NIC และ บางส่วนจะถูกประมวลผลโดยหน่วยประมวลผลหลักผ่านระบบ DMA โดย PRE (PREAMBLE) และ SFD นั้น เป็นข้อมูลที่ใช้ในการสื่อสารระหว่าง NIC เพื่อให้ทราบซึ่งการส่งและตำแหน่งเริ่มต้นของข้อมูล ซึ่ง NIC จะทำการตัดข้อมูลเหล่านี้ทิ้งก่อนดำเนินการตรวจสอบความถูกต้องของข้อมูลที่รับส่ง โดยอาศัย FCS (Frame Check Sum) นั้นเป็นตัวคำนวณที่ช่วยในการตรวจสอบความถูกต้องของข้อมูลที่ทำการรับส่ง สำหรับข้อมูลที่ไม่ได้ดูแลโดย NIC ซึ่งได้แก่ DES (ตำแหน่ง MAC ของผู้รับ)

SRC (ตำแหน่ง MAC ของผู้ส่ง) TYPE (ประเภทของข้อมูลที่ส่ง) และ Data (ข้อมูล) นั้น ผู้พัฒนาจะต้องทำการพัฒนาซอฟต์แวร์เพื่อดูแลข้อมูลในส่วนเหล่านี้เอง ก่อนส่งผ่านข้อมูลให้กับ IP หรือ ARP เพื่อทำการประมวลผลต่อไป

2.3. IP

IP (Internet Protocol) เป็นโพรโทคอลพื้นฐานของโพรโทคอลทั้งหมดใน TCP/IP การทำงานทุกอย่างบนอินเทอร์เน็ต ไม่ว่าจะเป็น TCP UDP ICMP หรือ IGMP ก็ตามล้วนแต่ต้องอาศัย IP ทั้งสิ้น อย่างไรก็ดีการทำงานของ IP เป็นลักษณะ Connectionless กล่าวคือไม่มีการยืนยันของการได้รับข้อมูลให้แก่ผู้ส่ง ดังนั้นในการใช้งาน IP จึงทำหน้าที่เพียงระบุหมายเลขเครือข่ายของผู้รับและผู้ส่งเท่านั้น

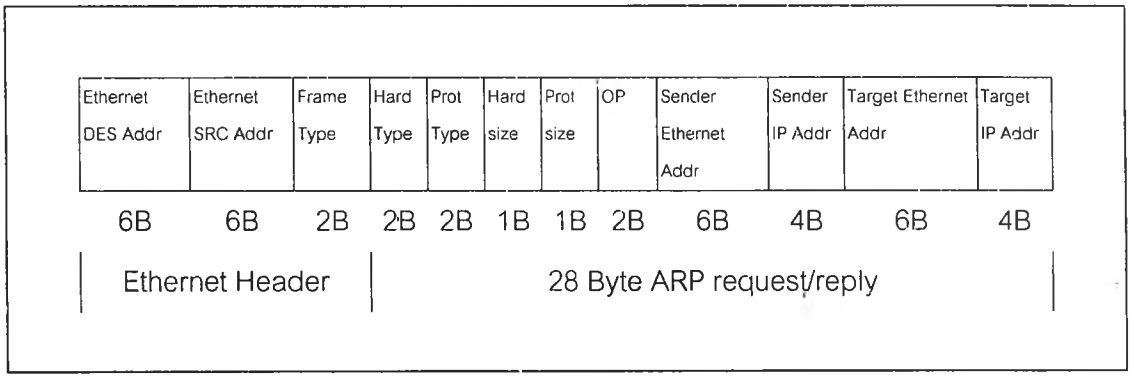
จุดมุ่งหมายของ IP คือการแสดงเครื่องและเครือข่ายที่ระบบต่อพ่วงอยู่ ซึ่งจะเป็นประโยชน์ในการหาทิศทางและการส่งผ่านข้อมูลผ่านระบบเครือข่าย โครงสร้างของ IP ประกอบด้วย Type of Service, Length, Time to Live, Protocol, Checksum และ IP Address ของผู้ส่งและผู้รับตามลำดับ จากนั้นจึงจะต่อด้วยข้อมูลส่วนอื่นๆ เช่น ICMP TCP หรือ UDP เพื่อส่งผ่านข้อมูลที่ซับซ้อนยิ่งขึ้น

2.4. ARP

ARP (Address Resolution Protocol) เป็นเกณฑ์วิธีจำแนกเลขที่อยู่ หรือมาตรฐานในการหาหมายเลขตำแหน่ง IP บนระบบเครือข่ายแบบต่างๆ ซึ่งในที่นี้มุ่งเน้นเพียงมาตรฐานของระบบเครือข่ายแบบอีเทอร์เน็ตเท่านั้น รายละเอียดเพิ่มเติมของ ARP นั้นสามารถหาอ้างอิงได้จาก RFC 826 ซึ่งสามารถกล่าวโดยสรุปได้ว่า ARP จะทำหน้าที่ในการจับคู่ระหว่างหมายเลขตำแหน่ง IP และ Physical Address ของมาตรฐานระบบเครือข่ายต่างๆ ซึ่งในที่นี้หมายเลขตำแหน่ง MAC ของเครือข่ายอีเทอร์เน็ต

หากวิเคราะห์จากลักษณะโครงสร้างของเฟรมบนมาตรฐานอีเทอร์เน็ต และ IP แล้ว จะพบว่าขนาดของหมายเลขตำแหน่งหรือ Address ซึ่งใช้บ่งบอกถึงที่อยู่บนระบบเครือข่ายของทั้งสองมาตรฐานนี้ มีความยาวแตกต่างกัน โดยหมายเลขตำแหน่ง MAC ของอีเทอร์เน็ตนั้นมีขนาด 48 บิต ในขณะที่หมายเลขตำแหน่ง IP มีขนาดเพียง 32 บิต จากลักษณะดังกล่าวจึงเป็นที่มาของโพรโทคอล ARP เพื่อใช้ในการแปลงและค้นหาหมายเลขตำแหน่ง MAC ของอีเทอร์เน็ตหรือของ Data Link Layer บนมาตรฐานเครือข่ายแบบอื่น ของหมายเลขตำแหน่ง IP ที่ระบบต้องติดต่อสื่อสารด้วย

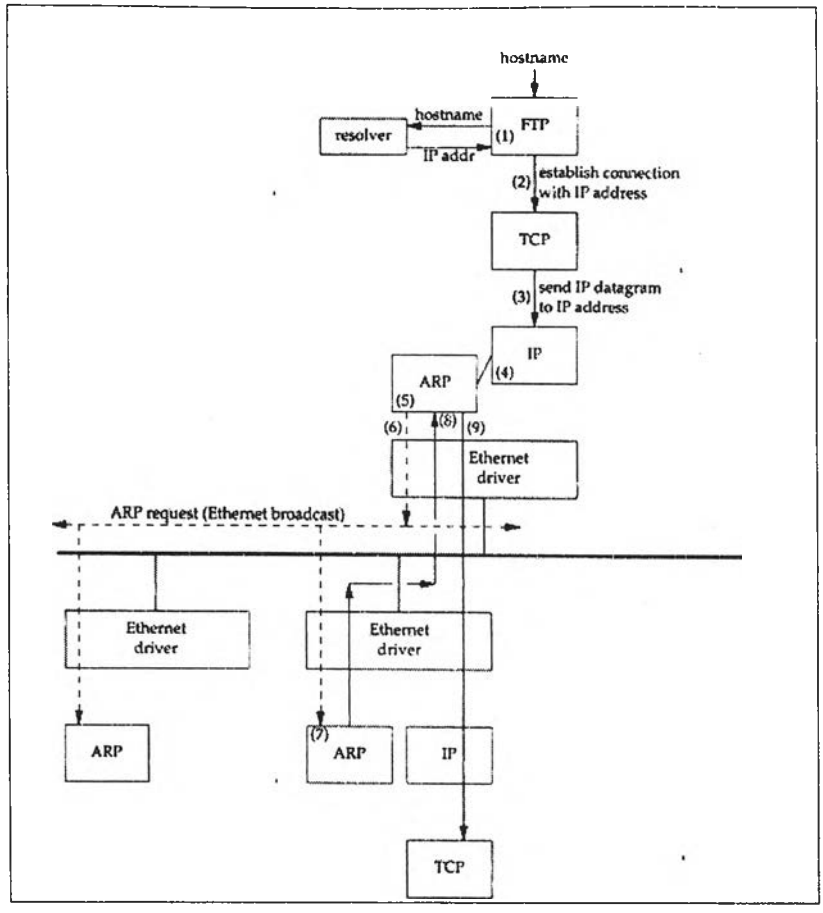
การทำงานของ ARP นั้นประกอบด้วยการขอ (Request) และการตอบ (Reply) โดยการขอ คือการขอทราบหมายเลขตำแหน่ง MAC ของหมายเลขตำแหน่ง IP ที่ระบุและการตอบ คือ การตอบหมายเลขตำแหน่ง MAC ให้กับผู้ขอทราบหมายเลขตำแหน่ง IP นั้น ลักษณะของเฟรมที่ใช้ในการรับส่ง ARP Request และ Reply นั้นสามารถแสดงได้ดังภาพที่ 3



ภาพที่ 3 ลักษณะเฟรมของ ARP

จากโครงสร้างเฟรมของ ARP ดังกล่าวสามารถอธิบายความหมายของคำต่างๆ ได้ดังนี้ Ethernet DES Addr และ SRC Addr คือหมายเลขตำแหน่ง MAC ของเครื่องคอมพิวเตอร์ปลายทางและต้นทางตามลำดับ ซึ่งในกรณีของการขอนั้น หมายเลขตำแหน่ง MAC ของเครื่องคอมพิวเตอร์ปลายทางจะเป็นหมายเลขตำแหน่ง MAC แบบ Broadcast หรือเป็นหมายเลขตำแหน่ง MAC ที่ระบุถึงเครื่องคอมพิวเตอร์ทุกเครื่องบนระบบเครือข่าย ส่วน Hard Type, Prot Type, Hard Size, Prot Size นั้น จะมีค่าเป็น 0x0001, 0x0800, 6 และ 4 ตามลำดับสำหรับการหาหมายเลขตำแหน่ง IP บนระบบเครือข่ายอีเทอร์เน็ต

การทำงานของ ARPนั้นเริ่มต้นจากการที่เครื่องต้นทางตรวจสอบตาราง ARP ของตนเองก่อน หากพบหมายเลขตำแหน่ง MAC ของตำแหน่ง IP ที่จะติดต่อสื่อสารด้วย ระบบก็จะข้ามการทำงานของ ARP ไป แต่หากไม่พบเครื่องต้นทางจะทำการร้องขอหมายเลขตำแหน่ง MAC จากเครื่องคอมพิวเตอร์ทุกเครื่องที่อยู่บนระบบเครือข่ายอีเทอร์เน็ตเดียวกันด้วยการส่งข้อมูลประเภท Broadcast ไป ดังแสดงในภาพที่ 4 ซึ่งเป็นการขอทราบหมายเลขตำแหน่ง MAC จากเครื่องคอมพิวเตอร์หมายเลข 5 ไปยังเครื่องคอมพิวเตอร์ทุกเครื่อง ด้วย ARP request (Ethernet broadcast)



ภาพที่ 4 การทำงานของ ARP

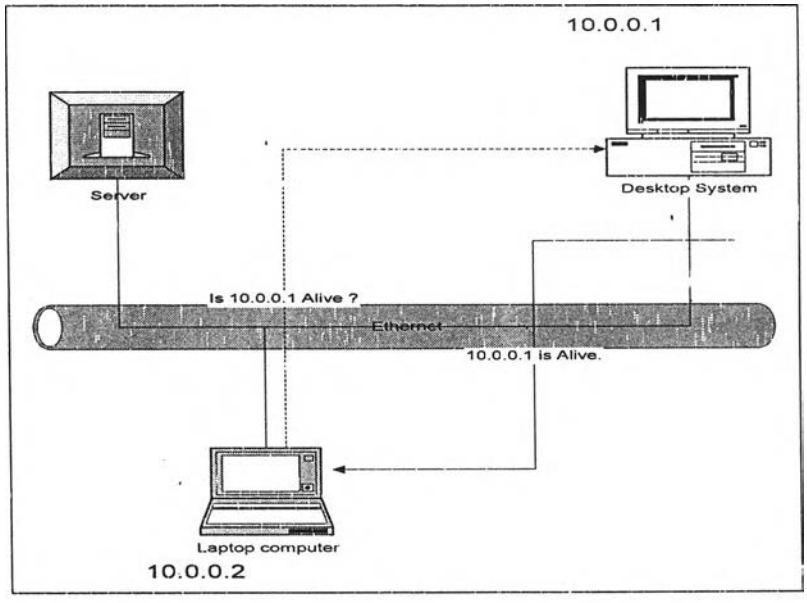
เมื่อเครื่องปลายทางได้รับ ARP เครื่องปลายทางก็จะเปรียบเทียบหมายเลขตำแหน่ง IP ที่ได้รับ ว่าตรงกับหมายเลขตำแหน่ง IP ของตนหรือไม่ หากพบว่าหมายเลขตำแหน่ง IP ดังกล่าวเป็นของตน ก็จะตอบรับ ARP Reply พร้อมทั้งระบุหมายเลขตำแหน่ง MAC ของตนเข้าไปกับ เฟรมตอบรับดังกล่าว เพื่อให้เครื่องต้นทางทราบหมายเลขตำแหน่ง Mac ของตนเอง จากลักษณะการทำงานที่กล่าวมา พบว่า ARP จะถูกเรียกใช้งานก็ต่อเมื่อ เครื่องคอมพิวเตอร์ต้นทางไม่ทราบ หมายเลขตำแหน่ง MAC ของเครื่องคอมพิวเตอร์ปลายทางเท่านั้น

ในกรณีที่ไม่มีการทำงานของการขอและการตอบรับ ARP แล้ว ผู้ใช้งานเครื่องคอมพิวเตอร์ต้นทางจะต้องปรับแต่ง ARP Table ของเครื่องคอมพิวเตอร์ต้นทางด้วยตนเองเพื่อให้เครื่องคอมพิวเตอร์ดังกล่าวทราบหมายเลขตำแหน่ง Mac โดยการใช้คำสั่ง ARP (ซึ่งจะกล่าวถึงในบทที่ 7 ต่อไป)

2.5. ICMP

ICMP (Internet Control Message Protocol) มีการทำงานในระดับเดียวกันกับ IP โดยทำหน้าที่ในการรายงานข้อผิดพลาดหรือสถานะการทำงานของ IP ซึ่งเราสามารถจัดกลุ่มของประเภท Message ใน ICMP ได้เป็นกลุ่มตามลักษณะการทำงาน แต่กลุ่มที่สำคัญคือและใช้ในการดำเนินงานวิจัยครั้งนี้คือ กลุ่ม echo request หรือที่เรียกกันโดยทั่วไปว่า ping request

Ping นั้นเป็นชื่อที่ได้มาจากการทำงานของ Sonar เพื่อใช้ในการตรวจสอบที่หมายของเครื่องคอมพิวเตอร์บนอินเทอร์เน็ตว่าสามารถติดต่อได้หรือไม่ โดยปกติหากเครื่องคอมพิวเตอร์ที่ต้องการติดต่อไม่สามารถ Ping ได้นั้น สามารถดีความหม่ายได้ว่าเราไม่สามารถใช้บริการอื่นๆ จากเครื่องคอมพิวเตอร์นั้นได้เช่นกัน ในงานวิจัยนี้จึงมีการพัฒนา Ping Response เพื่อให้เครื่องคอมพิวเตอร์ต้นทางสามารถตรวจสอบในส่วน การเชื่อมต่อของระบบเว็บเซิร์ฟเวอร์แบบฝังตัวเข้ากับระบบเครือข่าย ดังตัวอย่างในภาพที่ 5 แสดงการส่ง Request จากเครื่อง 10.0.0.2 ไปยัง 10.0.0.1 และการตอบรับด้วย Ping Response จากเครื่อง 10.0.0.1 ไปยัง 10.0.0.2



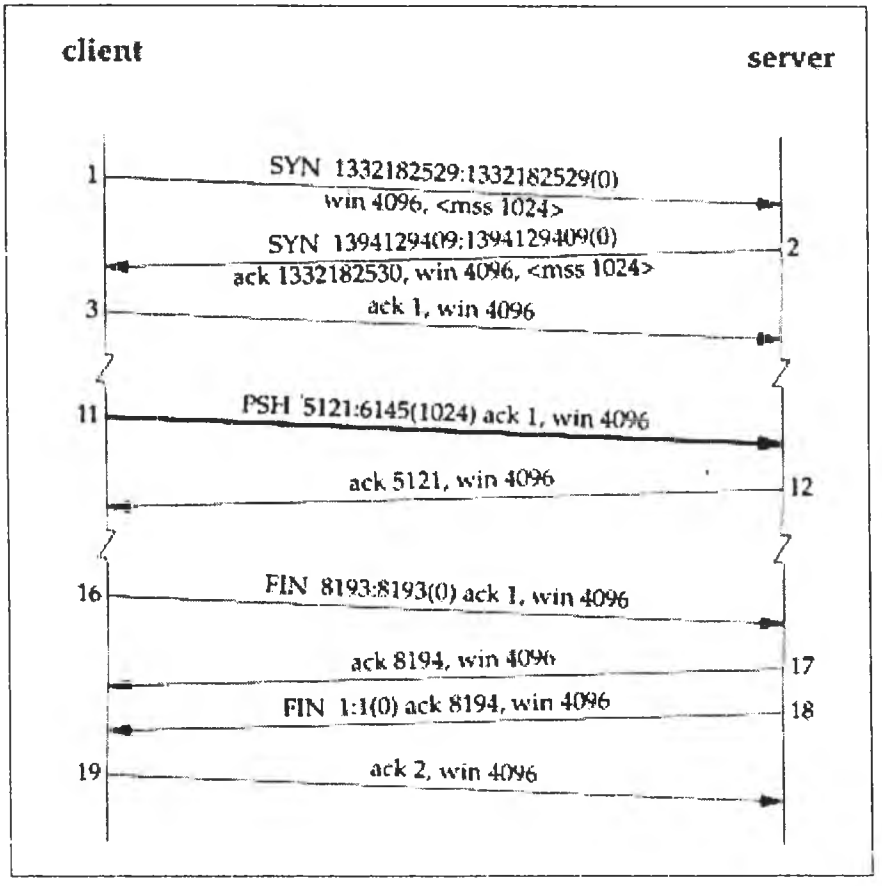
ภาพที่ 5 การทำงานของ Ping

2.6. TCP

TCP (Transmission Control Protocol) เป็นหัวใจของการทำงานบนระบบเครือข่ายอินเทอร์เน็ตทั้งนี้เนื่องจาก TCP จะทำหน้าที่ตรวจสอบความถูกต้องของข้อมูล รวมถึงยืนยันการรับและการส่งข้อมูลในลักษณะของ Sliding Window

ลักษณะโดยทั่วไปของ TCP จะประกอบด้วย Sequence Number เพื่อใช้แสดงหมายเลขของ Packet ที่ส่ง และ Acknowledgement Number เพื่อใช้ยืนยันการรับข้อมูลของ Sequence Number ที่ได้รับ เราจึงสังเกตได้ว่า Packet ทุกแบบจะต้องมีการตอบรับด้วย Packet ประเภท Acknowledgement (ACK) เสมอ นอกจากนี้ยังประกอบด้วย Checksum ซึ่งทำหน้าที่ตรวจสอบความถูกต้องของข้อมูลที่ได้รับ ข้อมูลในระดับ Application ต่างๆ ที่ทำงานบน TCP จะเป็นส่วนหนึ่งของการคำนวณ Checksum ของ TCP

ลักษณะการทำงานของ TCP นั้นสามารถอธิบายประกอบภาพที่ 6 ได้ดังนี้ เริ่มต้นด้วยการส่ง SYN Packet ไปยังฝ่ายที่ระบบต้องการติดต่อด้วยหรือเซิร์ฟเวอร์ จากนั้นฝ่ายเซิร์ฟเวอร์จะทำการตอบรับด้วย ACK และ SYN Packet มายังไคล์เอ็น (Client) ซึ่งไคล์เอ็นจะต้องตอบ ACK การ SYN ของเซิร์ฟเวอร์อีกครั้งหนึ่ง เมื่อเสร็จสมบูรณ์แล้ว ทั้ง 2 ฝ่ายจึงอยู่ในสถานะที่พร้อมทำการรับส่งข้อมูล โดยการแลกเปลี่ยนข้อมูลระหว่างกันนั้นจะกระทำด้วย PSH และ ACK Packet เพื่อใช้ส่งและยืนยันการได้รับตามลำดับ เมื่อการรับส่งข้อมูลเรียบร้อยสมบูรณ์แล้ว จึงส่ง FIN Packet และ ACK ระหว่างกันในทำนองเดียวกับการเปิด เพื่อเป็นการปิดการสื่อสาร

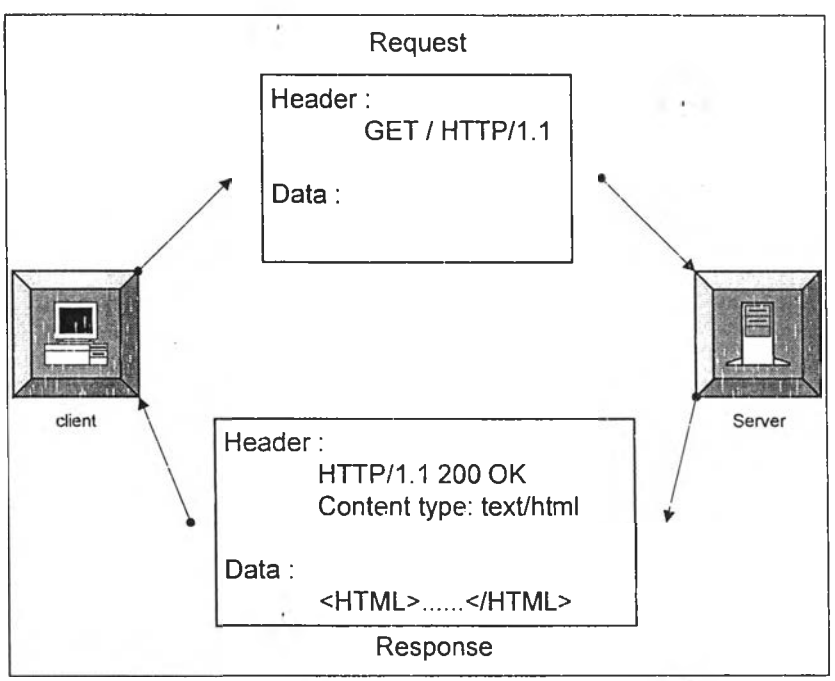


ภาพที่ 6 การทำงานของ TCP

2.7. HTTP

HTTP (HyperText Transfer Protocol) เป็นโพรโทคอลที่ทำงานในระดับ Application เพื่อใช้ในการขอ และบริการข้อมูลบนระบบเครือข่าย การทำงานของ HTTP สามารถแบ่งเป็นกลุ่มได้ 2 กลุ่ม คือ กลุ่ม Request และ กลุ่ม Response โดยในแต่ละกลุ่มจะประกอบด้วย Header และ Data

ส่วน HTTP Header นั้นใช้เพื่อแสดงรายระเอียดของประเภทข้อมูลที่ขอหรือให้บริการ ในขณะที่ส่วน Data นั้นใช้เพื่อรับส่งข้อมูล โดยการทำงานของ HTTP นั้น สามารถอธิบายได้ดังภาพที่ 7 คือ เมื่อผู้ใช้ต้องการข้อมูลโปรแกรมค้นผ่านเว็บจะทำการส่ง Request ไปยังผู้ให้บริการหรือเซิร์ฟเวอร์ โดยใน Header จะระบุถึงข้อมูลที่ต้องการ และอาจมีข้อมูลในส่วน Data ด้วย หากเป็นการ Request แบบ Post หลังจากที่เซิร์ฟเวอร์ได้รับการร้องขอแล้ว เซิร์ฟเวอร์จะทำการประมวลผลเพื่อสร้างผลลัพธ์ และ ส่งผลลัพธ์กลับด้วย Response โดยส่วน Header Response จะบุถึงประเภทของข้อมูลที่ระบบตอบรับ ขนาด ภาษา และรายเอียดอื่นๆ จากนั้นจึงตามด้วยข้อมูลผลลัพธ์ในส่วน Data



ภาพที่ 7 การทำงานของ HTTP

2.8. การเข้ารหัสแบบ Base 64

การเข้ารหัสแบบ Base 64 เป็นมาตรฐานการเข้ารหัสพื้นฐานที่นิยมใช้ในการสื่อสารผ่านระบบเครือข่ายอินเทอร์เน็ต โดยเฉพาะอย่างยิ่งการรับส่ง Email และระบบการพิสูจน์ตัวจริงแบบเบื้องต้นบนเว็บ (Basic Web Authentication) ซึ่งจะกล่าวถึงในบทที่ 5

การทำงานของ Base 64 นั้น จะทำการแปลงข้อมูล 3 ไบต์เป็น 4 ไบต์โดยอ้างอิงจากตารางแสดงผลของข้อมูล 6 บิตดังต่อไปนี้ (ตาราง 1)

ตาราง 1 การเข้ารหัสแบบ Base 64

ค่า HEX	String	ค่า HEX	String	ค่า HEX	String	ค่า HEX	String
0X00	"A"	0X10	"Q"	0X20	"g"	0X30	"w"
0X01	"B"	0X11	"R"	0X21	"h"	0X31	"x"
0X02	"C"	0X12	"S"	0X22	"I"	0X32	"y"
0X03	"D"	0X13	"T"	0X23	"j"	0X33	"z"
0X04	"E"	0X14	"U"	0X24	"k"	0X34	"0"
0X05	"F"	0X15	"V"	0X25	"l"	0X35	"1"
0X06	"G"	0X16	"W"	0X26	"m"	0X36	"2"
0X07	"H"	0X17	"X"	0X27	"n"	0X37	"3"
0X08	"I"	0X18	"Y"	0X28	"o"	0X38	"4"
0X09	"J"	0X19	"Z"	0X29	"p"	0X39	"5"
0X0A	"K"	0X1A	"a"	0X2A	"q"	0X3A	"6"
0X0B	"L"	0X1B	"b"	0X2B	"r"	0X3B	"7"
0X0C	"M"	0X1C	"c"	0X2C	"s"	0X3C	"8"
0X0D	"N"	0X1D	"d"	0X2D	"t"	0X3D	"9"
0X0E	"O"	0X1E	"e"	0X2E	"u"	0X3E	"+"
0X0F	"P"	0X1F	"f"	0X2F	"v"	0X3F	"/"

การเข้ารหัสทำได้โดยการดึงข้อมูลรหัสแอสกีที่ต้องการเข้ารหัสมาทีละ 3 ไบต์ จากนั้นทำการเขียนเป็นสายบิต (Bit Stream) ต่อกัน เมื่อได้แล้วให้ทำการแบ่งทีละ 6 บิต จะได้

ข้อมูลทั้งสิ้น 4 ชุด และทำการอ้างอิงข้อมูลทั้ง 4 ชุดจากตัวอักษรในตาราง BASE 64 ข้างต้น (ดูตัวอย่างภาพที่ 8)

ข้อมูลต้นฉบับ	"pok"
ค่า ASCII (Hex)	0x70 0x6F 0x6B
ทำการเขียนเป็น Bit Stream	01110000 01101111 01101011
ทำการตัดข้อมูลทีละ 6 Bit	011100 000110 111101 101011
ค่า Hex	0x1C 0x06 0x3D 0x2B
ผลลัพธ์ที่ได้จากการเข้ารหัส	"cG9r"

ภาพที่ 8 ตัวอย่างการเข้าและถอดรหัสแบบ Base64

หากความยาวของข้อมูลหารด้วย 3 ไม่ลงตัว ให้เติมตัวอักษรว่าง (Space) ต่อท้ายเข้าไปจนสามารถจัดกลุ่มได้ 3 ตัว เช่นกรณีข้อความตั้งต้นเป็น "pok;test" จะพบว่าข้อมีความยาว 8 ตัวอักษร และเพื่อให้ความยาวของข้อมูลหารด้วย 3 ลงตัว จึงต้องปรับข้อความตั้งต้นเป็น "pok:test " นอกจากนี้ในการใช้งานจริงยังพบว่ามีตัวอักษรอื่นบางตัวที่มิได้กล่าวถึงในตารางแต่มีการใช้งานอยู่จริง เช่น "?" แทน 0x00 เป็นต้น

การถอดรหัสนั้นทำในทำนองเดียวกันคือ แปลงข้อมูลที่ได้เป็น Hex จากนั้นเขียนเป็นสายบิต (Bit Stream) และจัดกลุ่มที่ละ 8 บิต แล้วจึงนำผลลัพธ์ที่ได้เปลี่ยนค่ากลับเป็นรหัสแอสกี