บทที่ 3
เทคนิคในการปรับปรุงระบบเครือข่ายคอมพิวเตอร์แบบสาธารณะ

3.1 หลักการในการสื่อสารข้อมูลระบบเครือข่ายคอมพิวเตอร์

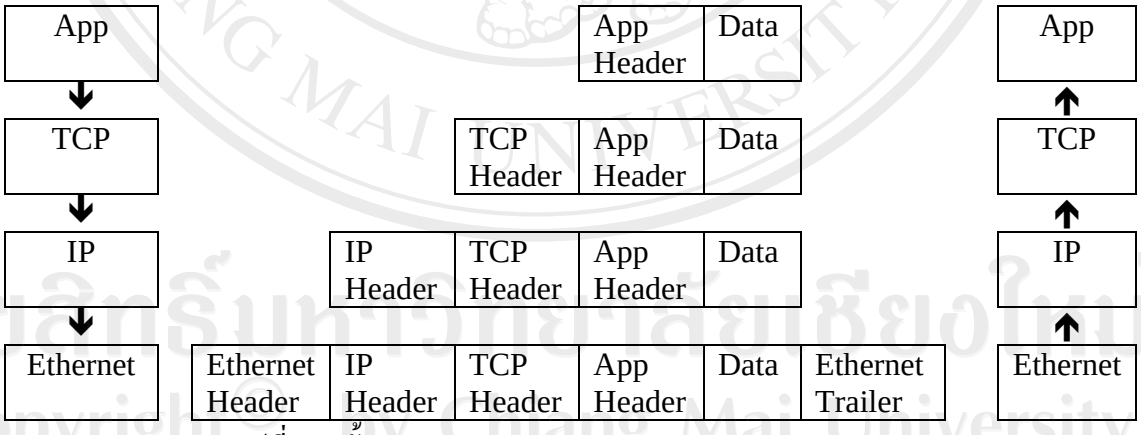
การสื่อสารข้อมูล (Data Communications) หมายถึง กระบวนของการถ่ายโอนหรือแลกเปลี่ยนข้อมูลระหว่างผู้ส่งและผู้รับ โดยผ่านช่องทางการสื่อสาร เช่น อุปกรณ์อิเล็กทรอนิกส์หรือคอมพิวเตอร์เพื่อเป็นตัวกลางในการส่งข้อมูล ทำให้ผู้ส่งและผู้รับเกิดความเข้าใจซึ่งกันและกัน การส่งข้อมูลนี้ ได้ทำการแปลงข้อมูลเป็นสัญญาณ หรือรหัสเสียก่อนแล้วจึงส่งไปยังผู้รับ เมื่อถึงปลายทางผู้รับก็จะต้องมีการแปลงสัญญาณนั้นกลับมาให้อยู่ใน รูปแบบที่สามารถจะเข้าใจได้ ในระหว่างการส่งอาจจะมีอุปสรรค์ที่เกิดขึ้นก็คือ สิ่งรบกวน (Noise) จากภายนอกทำให้ข้อมูลบางส่วนเสียหายหรือผิดเพี้ยนไปได้ซึ่งระยะทางก็มีส่วนเกี่ยวข้อง เนื่องด้วยระยะทางในการส่งยิ่งมากขึ้นก็อาจจะทำให้เกิดสิ่งรบกวนได้มากเช่นกัน จึงต้องมีการหาวิธีลดสิ่งรบกวนเหล่านี้ โดยใช้การพัฒนาตัวกลางในการสื่อสารที่จะทำให้เกิดการรบกวนน้อยที่สุด ส่วนประกอบพื้นฐานของการสื่อสารข้อมูล ได้แก่ ตัวส่งข้อมูล ช่องทางการส่งสัญญาณ ตัวรับข้อมูลและการสื่อสารข้อมูลในระดับเครือข่าย มาตรฐานกลางที่ใช้ในการส่งข้อมูลระหว่างคอมพิวเตอร์ในระบบเครือข่าย คือ มาตรฐาน OSI (Open Systems Interconnection Model) ซึ่งทำให้ทั้งคอมพิวเตอร์และอุปกรณ์เชื่อมต่อต่างๆ สามารถเชื่อมโยงในการใช้งานในเครือข่ายได้ ไม่แบ่งโครงสร้างออกในแต่ละชั้นจนมากเกินไป แต่ละชั้นมีหน้าที่การทำงานแตกต่างกัน หน้าที่การทำงานคล้ายกันจะถูกจัดให้อยู่ในชั้นเดียวกัน เลือกเฉพาะการทำงานที่เคยใช้ได้ผลประสบความสำเร็จมาแล้ว กำหนดหน้าที่การทำงานเฉพาะง่ายๆ เผื่อว่ามีการออกแบบหรือเปลี่ยนแปลงใหม่ อุปกรณ์ฮาร์ดแวร์ และซอฟต์แวร์จะได้ไม่ต้องเปลี่ยนแปลงตามมาตรฐานการกำหนดอินเตอร์เฟซ

เนื่องจาก OSI เกิดขึ้นมาหลังจากที่ TCP/IP (Transmission Control Protocol / Internet Protocol) ได้มีการใช้งานกันอย่างแพร่หลายไปแล้ว โดย TCP/IP ใช้ในเครือข่าย ARPANET เป็นเครือข่ายแรก ซึ่งต่อมาได้ขยายการเชื่อมต่อไปทั่วโลกเป็นเครือข่ายอินเตอร์เน็ต ทำให้มาตรฐานของ TCP/IP เป็นที่ยอมรับกันอย่างกว้างขวางและการที่ TCP/IP เป็นโปรโตคอลชนิดที่ไม่ต้องจ่ายค่าลิขสิทธิ์ ทำให้การใช้งาน TCP/IP ก็ยิ่งมีจำนวนผู้ใช้งานเพิ่มมากขึ้นจนถือเป็นมาตรฐานที่มีผู้ใช้งานรับส่งข้อมูลมากที่สุดในปัจจุบัน ถึงแม้ว่า TCP/IP จะไม่ได้มีการแบ่งชั้นการสื่อสารข้อมูลตรงตาม OSI 7-Layer Model แต่ OSI ก็ออกแบบมาให้เปิดกว้างและเข้ากันได้ดีกับ

TCP/IP โดย TCP จะเทียบได้กับประมาณชั้นที่ 4 คือ Transport Layer และ IP จะเทียบได้กับประมาณชั้นที่ 3 คือ Network Layer ของ OSI

ในการสื่อสารข้อมูลระหว่างชั้นซึ่งมีหน้าที่เกี่ยวข้องในการส่งผ่านข้อมูลจากสถานีต้นทางไปยังสถานีปลายทาง ข้อมูลจะถูกส่งผ่านจากโปรโตคอลระดับบนสุดจากสถานีต้นทางไปยังระดับล่างจนกระทั้งข้อมูลถูกแปลงให้อยู่ในรูปของ สัญญาณไฟฟ้าแล้วเดินทางผ่านเครือข่ายไปยังสถานีปลายทาง โปรโตคอลระดับล่างสุดที่สถานีปลายทางจะรับสัญญาณและส่งผ่านขึ้นไปยังโปรโตคอลระดับบนต่อไป เมื่อข้อมูลผ่านแต่ละระดับชั้น โปรโตคอลในชั้นนั้น ๆ จะผนวกข่าวสารกำกับการทำงานประจำโปรโตคอลซึ่งเรียกว่า โปรโตคอลเฮดเดอร์ (Protocol Header) เข้ากับข้อมูล โปรโตคอลเฮดเดอร์และข้อมูลจากระดับบนจะถูกส่งผ่านไปยังระดับล่าง โปรโตคอลระดับล่างจะมองโปรโตคอลเฮดเดอร์และตัวข้อมูลรวมเป็นเสมือนข้อมูล และเพิ่มโปรโตคอลเฮดเดอร์ประจำชั้นเข้าไป ข้อมูลเดิมจึงมีโปรโตคอลเฮดเดอร์หุ้มเป็นชั้น ๆ กระบวนการนี้เรียกว่า การเอ็นแคปซูเลต (Encapsulation) ดังรูปที่ 3.1 แสดงการเอ็นแคปซูเลตแพ็กเก็ต TCP/IP

เมื่อสถานีปลายทางได้รับแพ็กเก็ตก็จะดำเนินการส่งไปตามลำดับชั้น โปรโตคอลประจำชั้นจะถอดโปรโตคอลเฮดเดอร์ออกและส่งส่วนที่เหลือไปยังชั้นถัดไป โปรโตคอลเฮดเดอร์จะถูกถอดออกเหลือเฉพาะข้อมูลเมื่อถึงชั้นบนสุด กระบวนการนี้เรียกว่า การดีแคปซูเลต (Decapsulation)



รูปที่ 3.1 ขั้นตอนการ Encapsulation และ Decapsulation

3.2 เทคนิคในการแยกการสื่อสารข้อมูลโดยใช้เทคนิคแยกกลุ่มเครือข่าย (Segment Network)

การอ้างอิงอุปกรณ์ในระบบเครือข่ายคอมพิวเตอร์ เพื่อให้สามารถสื่อสารข้อมูลระหว่างกัน จำเป็นต้องมีการกำหนดหรือระบุบเลขหมายของอุปกรณ์ทุกชนิดในเครือข่ายได้ เพื่อให้อ้างอิงได้ โดยไม่ซ้ำกัน เพราะถ้าซ้ำกันแล้วการรับส่งข้อมูลอาจจะไม่สามารถสื่อสารข้อมูลถึงผู้รับปลายทางได้อย่างถูกต้อง ซึ่งเลขหมายดังกล่าวจะเรียกว่า แอดเดรส (Address) หรือเลขหมายประจำตัวที่มีข้อกำหนดเป็นมาตรฐาน ในการใช้งานโปรโตคอล TCP/IP ในการเชื่อมต่อเครือข่ายอินเตอร์เน็ต เลขหมายที่ใช้อ้างอิงถึงกันจะใช้เป็นตัวเลขที่เรียกว่า หมายเลขไอพี (IP Address)

หมายเลข IP Address ถูกกำหนดขึ้นมาให้เป็นหมายเลขอ้างอิงประจำตัวของอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกันอยู่ในระบบเครือข่าย TCP/IP โดยการกำหนดหมายเลข IP Address แต่ละเครื่องหรือแต่ละอุปกรณ์นี้จะต้องไม่ซ้ำกัน ซึ่งหมายเลข IP Address นี้จะไม่ถูกผูกติดกับตัวฮาร์ดแวร์ จึงสามารถกำหนดใหม่หรือแก้ไขเปลี่ยนแปลงได้ ทั้งนี้เนื่องจากเป็นการกำหนดด้วยซอฟต์แวร์ แตกต่างกับหมายเลข MAC Address (Media Access Control Address) ซึ่งเป็นหมายเลขประจำตัวของอุปกรณ์ที่ต่ออยู่ในเครือข่าย ค่า MAC Address จะถูกกำหนดจากบริษัทผู้ผลิตอุปกรณ์ตั้งแต่เริ่มผลิต ซึ่งค่า MAC Address เป็นการระบุค่าอ้างอิงของอุปกรณ์ในระดับล่างสุด (Physical Layer) ของกลไกการสื่อสารข้อมูลภายในระบบเครือข่ายคอมพิวเตอร์

ค่าของ IP Address จะถูกกำหนดออกเป็น 2 ส่วนคือ ค่าของหมายเลขอุปกรณ์ในเครือข่าย (Host Address) และค่าของหมายเลขเครือข่าย (Network Address) ซึ่งในการใช้งานระบบเครือข่ายคอมพิวเตอร์ในองค์กรโดยชุด IP Address ที่องค์กรสามารถใช้งานได้ คือ ไพรเวตแอดเดรส (Private Address) ซึ่งเป็นชุด IP Address ที่จัดสรรให้สำหรับการใช้งานภายในองค์กร โดยแบ่งออกเป็นสามกลุ่มแยกตามแต่ละคลาส ดังตารางที่ 3.1

ตารางที่ 3.1 การแบ่งการใช้งานไพรเวตแอดเดรส (Private Address)

IANA Reserved Private Network Ranges	Class	Start of range	End of range
The 24-bit Block	A	10.0.0.0	10.255.255.255
The 20-bit Block	B	172.16.0.0	172.31.255.255
The 16-bit Block	C	192.168.0.0	192.168.255.255

การแบ่ง IP Address แบบไม่ลงตัว Class หรือเรียกว่า Classless Inter-Domain Routing (CIDR) คือการกำหนดหมายเลข IP Address ใน Class ในส่วนของหมายเลขเครือข่ายไม่ลงตัวตามค่า Class ซึ่งเป็นวิธีการในการแบ่งเครื่องลูกข่ายในระบบเครือข่ายให้เหมาะสมสำหรับองค์กร โดยทั้วไปจะใช้ในการแบ่งการสื่อสารข้อมูลในเครือข่ายที่ต้องการแยกการสื่อสารข้อมูลออกเป็นกลุ่มย่อย ๆ โดยใช้ Router เพื่อช่วยในการสื่อสารข้อมูลระหว่างกลุ่มเครือข่าย

3.3 หลักการในการทำงานของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล

DHCP ย่อมาจาก Dynamic Host Configuration Protocol คือโปรโตคอลที่ทำหน้าที่ในการจัดการเรื่องการกำหนดค่าของเครื่องลูกข่ายในระบบ TCP/IP จากส่วนกลาง DHCP จะทำหน้าที่ในการกำหนดค่า IP addresses และ ค่า TCP/IP Configuration parameters โดยอัตโนมัติ ซึ่ง DHCP จะถูกอธิบายรายละเอียดใน RFC 1541 ในการใช้งาน DHCP การกำหนดค่าของเครื่องลูกข่ายในระบบโดยอัตโนมัตินั้นจะใช้หลักในการสื่อสารระหว่าง DHCP Server และ DHCP Client ระหว่างกัน โดยในอดีตนั้นมีหลาย ๆ โปรโตคอลที่ทำหน้าที่ในการจัดการการกำหนดค่าเครื่องลูกข่ายในระบบโดยอัตโนมัติ เช่น RARP (Reverse Address Resolution Protocol) and BOOTP (Bootstrap Protocol) [13] ซึ่งสามารถทำหน้าที่ในการจัดการการกำหนดค่าบนเครื่องเครือข่ายได้เช่นเดียวกัน โดยใช้หลักการง่าย ๆ ในการทำงาน คือ เมื่อเครื่องลูกข่ายในระบบทำการร้องขอ เครื่องแม่ข่ายก็สามารถทำการตอบรับการร้องขอ RARP จะทำงานบนระบบ Ethernet และเปลี่ยน Ethernet address เป็น IP address ส่วน RARP จะใช้งานบนระบบ diskless workstations เป็นส่วนใหญ่ โดย RARP จะใช้ลักษณะ Ethernet frame directly BOOTP ในรูปแบบการรับส่งข้อมูลแบบ UDP (User Datagram Protocol) โดย BOOTP จะส่งค่า IP addresses และ Sub-net Mask ของ Network, Gateway และค่าอื่น ๆ ที่จำเป็น ทั้งระบบ RARP และ BOOTP ซึ่งมีข้อเสียคือไม่สามารถรองรับการทำงานในลักษณะ dynamic allocation ได้ คือเป็นการกำหนดค่าแบบ Static คือเครื่องลูกข่าย จะได้รับค่าต่าง ๆ เป็นค่าที่กำหนดไว้ตลอด และสามารถกำหนดค่าต่าง ๆ ได้เพียงบางค่าเท่านั้น

ซึ่งทำให้มีการพัฒนาระบบโปรโตคอลที่เป็นการพัฒนาจาก BOOTP เป็น DHCP โดย DHCP จะใช้ลักษณะการทำงานที่เป็น Client-Server Model และใช้ลักษณะการรับส่งข้อมูลแบบ UDP โดย DHCP จะมีเครื่องแม่ข่ายและเครื่องลูกข่ายในลักษณะเดียวกับ BOOTP ซึ่งเป็นการสื่อสารกันระหว่างเครื่องแม่ข่ายกับเครื่องลูกข่ายในระบบ DHCP เป็นการตอบโต้การทำงานกันระหว่างเครื่องแม่ข่ายกับเครื่องลูกข่าย โดย DHCP จะรองรับระบบการจัดการแบบ Dynamic allocation ในการจัดการเครื่องลูกข่ายในระบบ DHCP Server สามารถจัดสรรค์การใช้งาน IP address ในระบบเพื่อให้สามารถนำ IP address มาใช้งานได้อย่างมีประสิทธิภาพ โดยมีการนำ IP address กลับมาใช้ใหม่ซึ่งไม่ได้ถูกใช้งานมาเกินระยะเวลาที่กำหนด ผู้ดูแลระบบไม่จำเป็นต้องเป็นคนจัดการหรือกำหนดค่าใด ๆ ให้กับเครื่องลูกข่าย เพราะตัวระบบ DHCP จะทำหน้าที่ในการจัดการทั้งหมด

รูปแบบในการสื่อสารข้อมูลของระบบ DHCP จะมีลักษณะ Packet Format ดังตารางที่ 2 เช่นเดียวกับ BOOTP ทำให้ DHCP Server สามารถตอบรับกับเครื่อง BOOTP Client ได้ โดยมีรายละเอียดดังตารางที่ 3.2 และรายละเอียดตัวแปรต่าง ๆ ดังตารางที่ 3.3

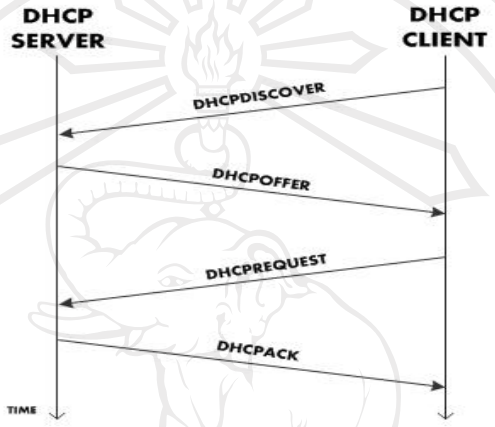
ตารางที่ 3.2 รูปแบบ DHCP Packet Format

op (1)	htype (1)	heln (1)	hops (1)
xid (4)			
secs (2)		flags (2)	
ciaddr (4)			
yiaddr (4)			
siaddr (4)			
giaddr (4)			
chaddr (16)			
sname (64)			
File (128)			
options (312)			

ตารางที่ 3.3 ข้อมูลรายละเอียดตัวแปรของ DHCP Packet Format

op	Packet op code / Message type.
Htype	Hardware address type.
Hlen	Hardware address length.
Hops	Client sets to zero,optionally used by gateways in cross-gateway booting.
Xid	Transaction ID, a random number, used to match this boot request with the responses it generates.
Secs	Filled in by client, seconds elapsed since client started trying to boot.
Flags	Flags.
Ciaddr	Client IP address; filled in if client can respond to ARP requests.
Yiaddr	‘your’ (client) IP address
siaddr	Server IP address;returned in bootreply by server.
Giaddr	Gateway IP address,used in optional cross-gateway booting
chaddr	Client hardware address,filled in by client.
Sname	Optional server host name.
file	boot file name.
options	optional parameters field.

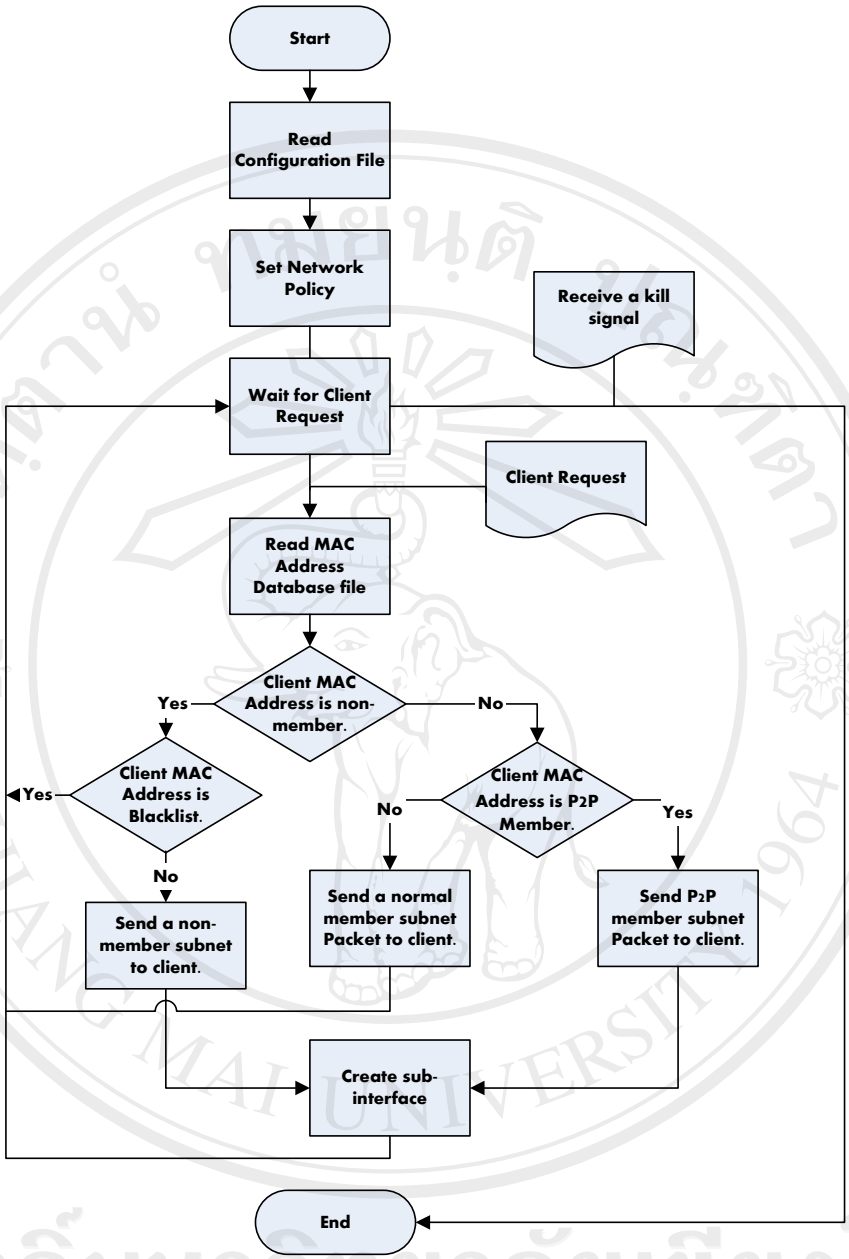
DHCP เป็นลักษณะการทำงานแบบ Client-Server โดยขั้นตอนการทำงาน [14] สามารถแบ่งออกได้เป็นสองส่วนคือ ส่วนแรกเครื่องลูกข่ายในระบบเครือข่ายจะทำการส่งข้อมูลร้องขอในระบบเรียกว่า DHCPDISCOVER เพื่อร้องขอไปยังเครื่องแม่ข่าย เมื่อเครื่องแม่ข่ายได้รับการร้องขอก็จะส่ง DHCPOFFER กลับไปยังเครื่องลูกข่าย เพื่อแจ้งว่าจะทำการตอบรับการร้องขอ หลังจากนั้นเครื่องลูกข่ายจะทำการส่ง DHCPREQUEST กลับไปยังเครื่องแม่ข่าย เพื่อให้เครื่องแม่ข่าย ทำการกำหนดค่าต่าง ๆ กลับมาให้เครื่องลูกข่าย โดย DHCPACK ดังรูปที่ 3.2



รูปที่ 3.2 การทำงานของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล (Initial Address Assignment)

3.4 เทคนิคในการปรับปรุงการทำงานของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล

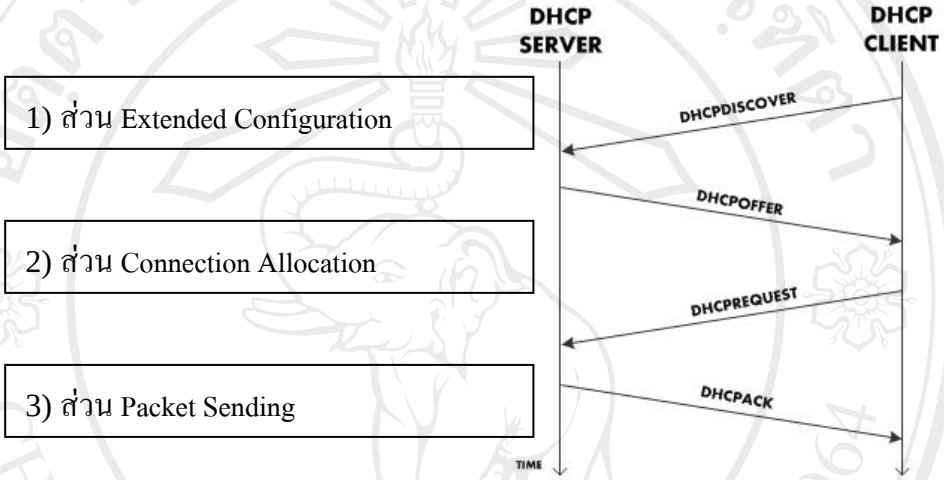
หลักการทำงานของระบบ การปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะทำการปรับปรุงพัฒนาไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลเดิม โดยเพิ่มส่วนของการทำงานของ การปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะขึ้น ดังรูปที่ 3.3 โดยเริ่มต้นในส่วนระบบทำการอ่าน (Configuration file) ซึ่งจะประกอบด้วย Parameter ต่าง ๆ โดยจะบอกรายละเอียดของแต่ละกลุ่ม หลังจากอ่าน Configuration File ระบบจะทำการ Set Policy ของระบบตามที่กำหนดไว้ตามที่ต้องการโดยทำงานรวมกับ Firewall เช่น iptables, ipchain เมื่อกำหนด Policy ของระบบเรียบร้อยแล้ว ระบบจะรอการร้องขอ จากเครื่อง Client เมื่อมีเครื่อง Client ทำการร้องขอมาระบบจะทำการอ่านฐานข้อมูล MAC Address ที่กำหนดไว้ เพื่อตรวจสอบว่า Client ที่ร้องขออยู่กลุ่มใด กรณีแรกคือ Client ที่ร้องขอไม่มีค่า MAC Address อยู่ในฐานข้อมูล



รูปที่ 3.3 ไดอะแกรมการทำงาน การปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ

ระบบจะทำการตรวจสอบอีกว่าเป็น MAC Address ที่อยู่ใน Black List หรือไม่ ถ้าไม่อยู่ ระบบจะทำการสร้าง Packet ค่า Parameter ต่าง ๆ ในลักษณะ Secure Connection กลับไปยัง Client เพื่อให้ Client ทำการ Configuration IP address และ Server จะทำการสร้าง Sub Interface เพื่อมารองรับการเชื่อมต่อ กรณีที่สองคือ เครื่องลูกข่ายที่ทำการร้องขอมีค่า MAC Address อยู่ในไฟล์ข้อมูลของกลุ่ม Member ระบบจะทำการตรวจสอบว่าอยู่ในกลุ่มใด และส่ง Packet Parameter ของกลุ่มนั้นกลับไปยังเครื่องลูกข่าย และถ้าอยู่ในกลุ่ม Secure Connection

ระบบจะทำการสร้าง Sub Interface เพื่อรองรับการเชื่อมต่อด้วยเช่นกัน โดยระบบจะกลับไปยังสถานะรอการร้องขอเช่นเดิมจนกว่าจะมีการ Kill Process เกิดขึ้น ส่วนในการทำงานอื่น ๆ ของ DSHCP ยังอ้างอิงการทำงานเดิมของ DHCP เช่นเดิม โดยการปรับปรุงข้างต้นจะทำการแก้ไขในส่วนของ DHCP Server ดังรูปที่ 3.4 โดยเพิ่มส่วนขยายเพื่อรองรับการทำงานโดยแบ่งออกเป็นสามส่วนหลัก ๆ คือ ส่วนของ Extended Configuration Part, ส่วนของ Connection Allocation Part และส่วนของ Packet sending part



รูปที่ 3.4 ส่วนในการปรับปรุงการทำงานไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล เทียบกับไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลเดิม