บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

ระบบแจก IP Address ให้กับเครื่องลูกข่ายในระบบเครือข่ายคอมพิวเตอร์ ได้ถูกพัฒนาอย่างต่อเนื่อง เพื่อช่วยอำนวยความสะดวกและจัดสรร IP Address ของระบบเครือข่าย ให้ถูกใช้งานอย่างเต็มที่และมีประสิทธิภาพ โดยปัจจุบันระบบแจก IP Address [1] ที่ใช้งานในองค์กรทั่วไป คือ ไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล (Dynamic Host Configuration Protocol) [2] ซึ่งออกแบบมาเพื่อใช้งานในเครือข่ายที่มีลักษณะเป็นแบบ Local Area Network คือลักษณะที่เครื่องลูกข่ายในระบบสามารถเชื่อมต่อกันได้โดยอิสระ ต่อมาได้มีการพัฒนาและปรับปรุงทั้งในส่วนของประสิทธิภาพการทำงาน [3] ความปลอดภัย [4,5] และความเร็วในการทำงาน [6] ของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล แต่การนำไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลไปใช้ในเครือข่ายที่เป็นเครือข่ายคอมพิวเตอร์แบบสาธารณะ (Public Area Network) [7] เช่น สนามบิน, สถานีรถไฟ, โรงแรม, ฯลฯ มีความไม่เหมาะสมอยู่หลายประการ ทำให้เกิดแนวความคิดพัฒนาปรับปรุงไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล ให้มีความเหมาะสมกับการใช้งานในเครือข่ายคอมพิวเตอร์แบบสาธารณะ (Public Area Network) [8] ซึ่งการพัฒนา ได้มีแนวคิดในการพัฒนาปรับปรุงในส่วนเครื่องแม่ข่าย (Server Site) โดยส่วนเครื่องลูกข่าย (Client Site) ไม่ต้องเปลี่ยนแปลง เนื่องจากต้องการให้ผู้ใช้งานง่ายต่อการใช้งาน ไม่จำเป็นต้องเปลี่ยนแปลงการกำหนดค่าต่างๆ และโปรแกรมที่ใช้งาน

ในการใช้งานระบบแจก IP Address ให้กับเครื่องลูกข่าย เนื่องจากระบบไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล ที่มีการใช้อยู่ในปัจจุบัน ถูกออกแบบมาสำหรับการใช้งานในลักษณะ Local Area Network ซึ่งเครื่องลูกข่ายในระบบสามารถเชื่อมต่อกันได้อย่างอิสระ จึงไม่เหมาะสมในการนำมาใช้งานในลักษณะเครือข่ายคอมพิวเตอร์แบบสาธารณะ (Public Area Network) ที่ลักษณะการใช้งานระบบของเครื่องลูกข่าย ไม่จำเป็นให้มีการเชื่อมต่อซึ่งกันและกันของเครื่องลูกข่าย เพราะอาจจะทำให้เกิดปัญหาต่าง ๆ เช่น การขโมยข้อมูลในระบบเครือข่าย, การโจมตีของไวรัส [9], การไม่ปลอดภัยของข้อมูล [10] ซึ่งมีหลาย ๆ วิธีที่ถูกนำมาใช้เพื่อให้การใช้งานในเครือข่ายคอมพิวเตอร์แบบสาธารณะ (Public Area Network) ทำได้เหมาะสมและง่ายต่อผู้ใช้งาน

2. วัตถุประสงค์การวิจัย

สามารถนำระบบ การปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ ที่ทำหน้าที่เครื่องแม่ข่ายในการกำหนดค่าเครือข่ายคอมพิวเตอร์สำหรับเครื่องลูกข่ายในระบบ เพื่อให้การทำงานระบบเครือข่ายของเครื่องลูกข่ายในระบบเครือข่าย ที่มีลักษณะแบบสาธารณะคือเครื่องลูกข่ายในระบบไม่มีความจำเป็นในการติดต่อไปยังเครื่องลูกข่ายอื่น ๆ แต่ยังคงต้องการสื่อสารไปยังเครื่องแม่ข่ายเพื่อร้องขอบริการต่าง ๆ ที่มีอยู่ในระบบเครือข่าย ดังนั้นการปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ สามารถเข้ามาจัดการ การใช้งานระบบเครือข่ายของเครื่องลูกข่าย ให้แยกการเชื่อมต่อของแต่ละเครื่องลูกข่าย เพื่อให้เหมาะสมกับการใช้งานลักษณะเครือข่ายที่เป็นแบบสาธารณะ

3. ขอบเขตการวิจัย

3.1 ออกแบบและพัฒนาบนไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล (ดีเอชซีพี)

3.2 ลักษณะเครือข่ายคอมพิวเตอร์ใช้มาตรฐาน TCP/IP และ IP Version 4

3.3 ลักษณะไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลใน รูปแบบเครื่องแม่ข่ายลักษณะเดี่ยว (Single Server)

3.4 สามารถแยกการเชื่อมต่อผู้ใช้งานที่ไม่ได้รับสิทธิ (Unauthorized User) ออกจากผู้ใช้งานอื่น ๆ

3.5 สามารถแบ่งกลุ่มของผู้ใช้งานและกำหนดสิทธิแต่ละกลุ่ม

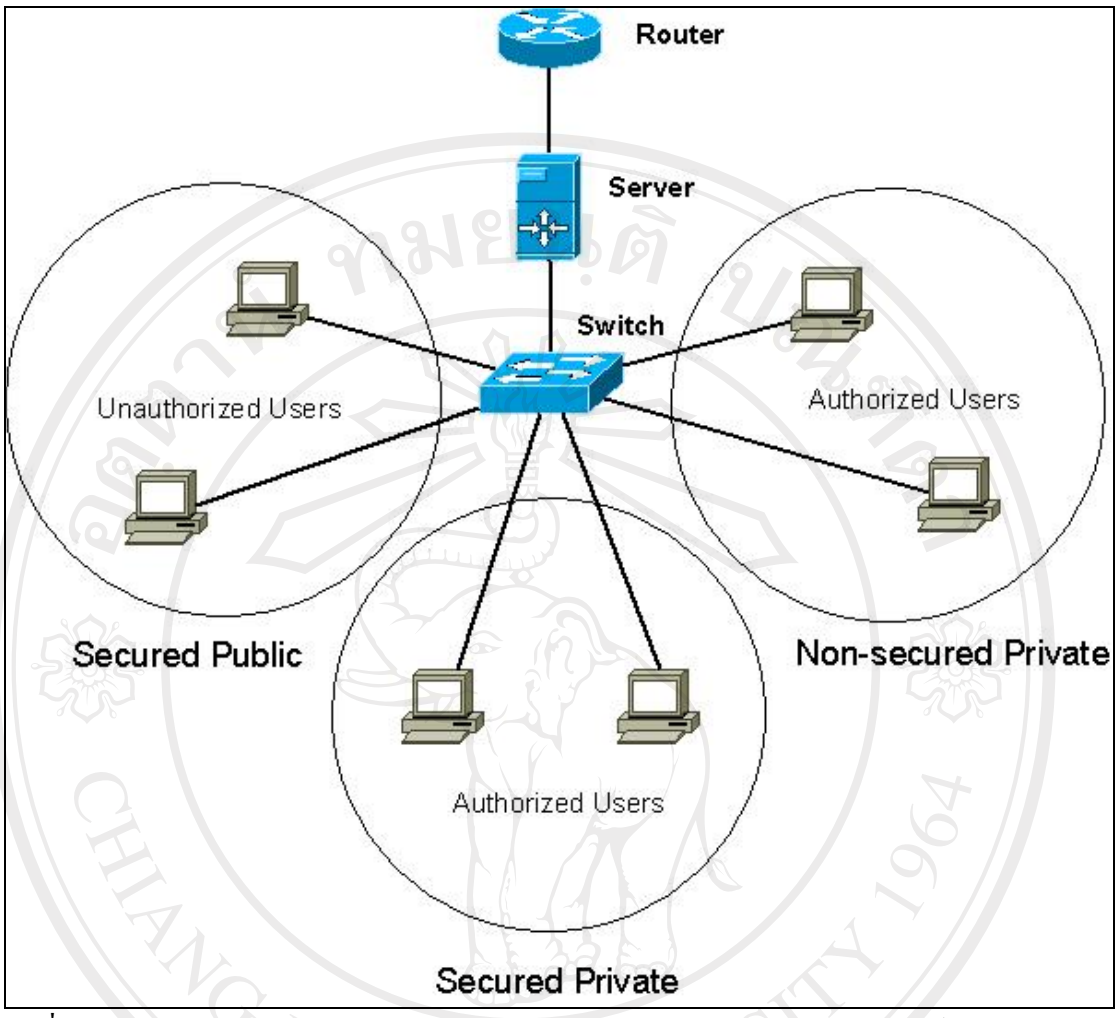
4. ทฤษฎีแนวความคิด

จากลักษณะปัญหาที่เกิดขึ้น จึงเกิดแนวความคิดเพื่อตอบสนองความต้องการในระบบเครือข่ายคอมพิวเตอร์แบบสาธารณะ (Public Area Network) ที่รองรับการใช้งานของเครื่องลูกข่ายที่มีลักษณะผู้ใช้งานที่ไม่ได้รับสิทธิ (Unauthorized User) คือเครื่องลูกข่ายในระบบไม่ต้องการสื่อสารกันภายในเครือข่ายแต่ต้องการเชื่อมต่อ ไปยังเครื่องแม่ข่ายที่ให้บริการในระบบเครือข่าย จึงทำให้เกิดแนวความคิดพัฒนาปรับปรุงระบบไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลให้รองรับการทำงานในลักษณะนี้ โดยใช้หลักการทำงาน การกำหนดค่าเครือข่ายและ IP Address สำหรับการเชื่อมต่อลักษณะ Virtual Multiple VLAN Network สำหรับการเข้ามาใช้งานระบบของเครื่องลูกข่าย และเพิ่มการทำงานของ Routing, Firewall บนเครื่องแม่ข่าย DHCP Server เพื่อให้รองรับการทำ Policy ทำให้ระบบมีความยืดหยุ่นและสามารถจัดการได้จากเครื่องแม่ข่ายเพียงเครื่องเดียว แทนที่จะอยู่หลายอุปกรณ์ และเพิ่มความสามารถของไดนามิกโฮสต์คอนฟิกกิวเรชัน

โปรโตคอล ให้สามารถรองรับการทำงานได้หลายกลุ่ม โดยไม่พึ่งอุปกรณ์ Switch Layer 3 (Managed Switch) ซึ่งมีราคาแพงกว่า Switch Layer 1 (Unmanaged Switch) อยู่มาก โดยแบ่งเครื่องลูกข่ายในระบบออกเป็นสองกลุ่มหลัก ๆ คือ กลุ่มผู้ไม่ได้รับสิทธิ (Unauthorized User) และกลุ่มผู้ได้รับสิทธิ (Authorized User) ซึ่งกลุ่มผู้ได้รับสิทธิ (Authorized User) ยังแบ่งออกได้เป็นกลุ่มส่วนตัวต้องการความปลอดภัย (Secured Private) กับรูปแบบที่ไม่ต้องการความปลอดภัย (Non-Secured Private) ซึ่งทั้งสองกลุ่มนี้สามารถแบ่งกลุ่มย่อยได้ โดยใช้ข้อมูล MAC Address ของเครื่องลูกข่าย ที่บันทึกข้อมูลอยู่ในไฟล์ที่กำหนดของแต่ละกลุ่ม โดยกลุ่มผู้ไม่ได้รับสิทธิ (Unauthorized User) คือกลุ่มที่ไม่ได้อยู่ในไฟล์ข้อมูล MAC Address ใดๆ เลย และได้ถูกกำหนดการเชื่อมต่อเป็นแบบ Virtual Multiple VLAN ทำให้ระบบมีปลอดภัยมากขึ้นและเครือข่ายสามารถกำหนดกฎของเครือข่าย (Network Policy) การสื่อสารข้อมูลของเครื่องลูกข่ายในกลุ่มหรือระหว่างกลุ่มเครื่องลูกข่ายขึ้นอยู่กับการกำหนดกฎของเครือข่าย (Network Policy) และถ้าต้องการความปลอดภัยในระบบสูงกว่านั้น สามารถเลือกการใช้งานแบบกลุ่มความปลอดภัย คือ Virtual Multiple VLAN เพียงอย่างเดียว เพื่อให้เครื่องลูกข่ายที่เข้ามาใช้งานระบบเครือข่ายไม่สามารถกำหนดค่าเครือข่ายแบบ Static ได้ เพราะต้องร้องขอการเชื่อมต่อกับระบบก่อนและสามารถตรวจสอบข้อมูล Black List ในกรณีเครื่องลูกข่ายที่ไม่ต้องการให้บริการ ซึ่งการทำงานลักษณะนี้ขึ้นอยู่กับเครื่องแม่ข่าย (DHCP Server) ทำให้ระบบมีความซับซ้อนน้อยลงและง่ายต่อการตรวจสอบและจัดการการทำงานของระบบสำหรับผู้ดูแลระบบ และใช้งบประมาณที่ต่ำกว่า ไม่ว่าจะเป็นเรื่องอุปกรณ์หรือค่าการดูแลระบบ

ระบบการปรับปรุงระบบความปลอดภัยของ ไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ เป็นการปรับปรุงการทำงานของระบบไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล โดยจากงานวิจัยจะได้เลือกปรับปรุงการทำงานของ Version 2 of the ISC DHCP Distribution ซึ่งเป็น Open Source โดยทำการปรับปรุงการทำงานในส่วนของเครื่องแม่ข่าย (Server Section) โดยอ้างอิงลักษณะการทำงานเดิมของ Initial Address Assignment Process ได้ทำการเพิ่มส่วนการทำงานเพื่อรองรับการทำงานใน Public Area Network โดยส่วนเพิ่มขยายแบ่งออกเป็นสามส่วนคือ ระบบเพิ่มขยายส่วนเพิ่มเติม Configuration, ระบบจัดสรรการเชื่อมต่อการสื่อสาร, ระบบเพิ่มขยายส่วนส่ง Packet Assign the Address to Client รายละเอียดในแต่ละส่วนเพิ่มขยายจากไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลเดิม มีหลักการทำงานดังนี้ ระบบเพิ่มขยายส่วนเพิ่มเติม Configuration จะประกอบด้วยสองส่วนคือ Configuration file (dhcp.conf) ในส่วนที่ทำหน้าที่ในการกำหนดกลุ่มของเครื่องลูกข่ายในระบบ โดยมีสามประเภทดังรูปที่ 1.1 คือ กลุ่มเครื่องลูกข่ายที่อยู่ในกลุ่มผู้

ไม่ได้รับสิทธิ (Unauthorized User) เรียกว่าแบบสาธารณะป้องกันความปลอดภัย (Secured Public), กลุ่มเครื่องลูกข่ายที่อยู่ในกลุ่มผู้ได้รับสิทธิ (Authorized User) ที่มีลักษณะความปลอดภัย เรียกว่า แบบส่วนตัวป้องกันความปลอดภัย (Secured Private), กลุ่มเครื่องลูกข่ายที่อยู่ในกลุ่มผู้ได้รับสิทธิ (Authorized User) เรียกว่า แบบส่วนตัวป้องกันความปลอดภัย (Secured Private) ซึ่งในแต่ละกลุ่มจะถูกกำหนดสมาชิกผู้ใช้งานอยู่ในไฟล์ข้อมูล Mac Address ของแต่ละกลุ่ม เมื่อระบบทำการอ่าน Configuration File ระบบจะทำหน้าที่เข้าสู่การทำงานของการรอการร้องขอบริการ DHCP จากเครื่องลูกข่าย, เมื่อมีการร้องขอบริการ DHCP จากเครื่องลูกข่าย ระบบจัดสรรการเชื่อมต่อ เป็นระบบที่ทำการตรวจสอบว่าเครื่องลูกข่ายที่ทำการร้องขอค่าเครือข่ายมายังเครื่องแม่ข่าย อยู่ในกลุ่มผู้ได้รับสิทธิ (Authorized User) หรืออยู่ในกลุ่มกลุ่มผู้ไม่ได้รับสิทธิ (Unauthorized User)หลังจากระบบทำการตรวจสอบเรียบร้อยแล้ว ระบบจะทำหน้าที่ในการส่งต่อข้อมูลไปยังส่วนระบบเพิ่มขยายส่วนส่ง Packet Assign the Address ซึ่งจะแตกต่างจากระบบไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลเดิม เพื่อเพิ่มขยายส่วนรับข้อมูลจากส่วนระบบจัดสรรค์การเชื่อมต่อ เพื่อทำการส่ง Packet Assign the Address ตามค่า Configruation ที่เรากำหนด กลับไปยังเครื่องลูกข่าย ทำการดำเนินการต่อไป โดยอ้างอิงรูปแบบ Packet Format เดิม เพื่อที่จะทำให้เครื่องลูกข่ายที่ใช้งาน DHCP ในระบบเดิมสามารถใช้งานระบบที่มีการปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะได้ทันที โดยระบบจะทำการแบ่งเครื่องลูกข่ายในลักษณะ Separated Host โดยรูปแบบ Virtual Multiple VLAN Network โดยใช้หลักการของการแบ่ง Classless Inter-Domain Routing บนเครือข่าย VLAN เดียวกัน



รูปที่ 1.1 การใช้งานเทคโนโลยีการปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิก
กิวเรชันโปรโตคอลสำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ