บทที่ 6
สรุปและข้อเสนอแนะ

ในงานวิจัยทำการศึกษาการทำงานของระบบ ไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล และลักษณะการสื่อสารข้อมูลของเครื่องลูกข่าย โดยใช้เทคนิคในการแยกกลุ่มเครือข่ายในลักษณะ Classless Inter-Domain Routing (CIDR) และแบ่งประเภทของผู้ใช้งานเป็นผู้ใช้ที่ไม่ได้รับสิทธิ (Unauthorized User) และผู้ใช้ที่รับสิทธิ (Authorized User) ซึ่งมีรูปแบบลักษณะเครือข่ายแบบปกติและแบบปรับปรุงระบบความปลอดภัย เพื่อความยืดหยุ่นในการใช้งาน โดยแบ่งกลุ่มเครื่องลูกข่ายตามข้อมูล Mac Address ของเครื่องลูกข่าย

ซึ่งการออกแบบการทดลองการทำงานของการปรับปรุงระบบความปลอดภัยของ ไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลสำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ ได้แบ่งการทดลองออกเป็น 4 แบบ ตามลักษณะของกลุ่มผู้ใช้งานของเครื่องลูกข่ายในระบบเครือข่าย เพื่อวิเคราะห์การสื่อสารข้อมูลของเครื่องลูกข่าย โดยมีรายละเอียดของแต่ละการทดลองดังต่อไปนี้

การทดลองแบบที่ 1 เป็นการทดลองในรูปแบบเครือข่ายคอมพิวเตอร์สาธารณะแบบปกติ (Non-secured Public) ของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลลักษณะการทำงานแบบเดิม ซึ่งการทดสอบการสื่อสารข้อมูลของเครื่องลูกข่าย ในการใช้งานไดนามิกโฮสต์คอนฟิกกิวเรชัน โปรโตคอลเดิม เพื่อใช้ในการเปรียบเทียบกับการสื่อสารข้อมูลของเครื่องลูกข่ายการทำงานของการปรับปรุงระบบความปลอดภัยของ ไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลสำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ

การทดลองแบบที่ 2 เป็นการทดลองในรูปแบบเครือข่ายคอมพิวเตอร์สาธารณะแบบปรับปรุงระบบความปลอดภัย (Secured Public) ของการปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธาณะ รองรับผู้ใช้ที่ไม่ได้รับสิทธิ (Unauthorized User) โดยมีระบบความปลอดภัยในการจำกัดการสื่อสารข้อมูลระหว่างเครื่องลูกข่าย เพื่อให้สามารถเปรียบเทียบความแตกต่างระหว่าง การสื่อสารข้อมูลของเครื่องลูกข่ายและการทำงานของ ไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลเดิมกับการปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธาณะ

การทดลองแบบที่ 3 เป็นการทดลองในรูปแบบเครือข่ายคอมพิวเตอร์แบบส่วนตัวแบบป้องกันความปลอดภัย (Secured Private) ที่ทำงานร่วมกับ เครือข่ายคอมพิวเตอร์สาธารณะแบบปรับปรุงระบบความปลอดภัย (Secured Public) เพื่อรองรับผู้ใช้งานที่ได้รับสิทธิ (Authorized User) ซึ่งกลุ่มของเครื่องลูกข่ายแต่ละกลุ่ม สามารถกำหนดกฎของเครือข่าย (Network Policy) เป็นการทดสอบคุณสมบัติการแบ่งกลุ่มและการกำหนดกฎของเครือข่าย ซึ่งสามารถกำหนดกฎของเครือข่ายได้ทั้งในลักษณะการสื่อสารข้อมูลระหว่างเครื่องลูกข่ายภายในกลุ่มและระหว่างกลุ่มเครื่องลูกข่าย

การทดลองแบบที่ 4 เป็นการทดลองในรูปแบบเครือข่ายคอมพิวเตอร์แบบส่วนตัวแบบปกติ (Non-secured Private) ที่ทำงานร่วมกับ เครือข่ายคอมพิวเตอร์สาธารณะแบบปรับปรุงระบบความปลอดภัย (Secured Public) เพื่อรองรับผู้ใช้งานที่ได้รับสิทธิ (Authorized User) ที่ต้องการการเชื่อมต่อในลักษณะไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลเดิม ซึ่งกลุ่มของเครื่องลูกข่ายแต่ละกลุ่ม สามารถกำหนดกฎของเครือข่าย (Network Policy) เพื่อเป็นการทดสอบคุณสมบัติการแบ่งกลุ่มและการกำหนดกฎของเครือข่าย ซึ่งสามารถกำหนดกฎของเครือข่ายในลักษณะการสื่อสารข้อมูลระหว่างกลุ่มเครื่องลูกข่าย

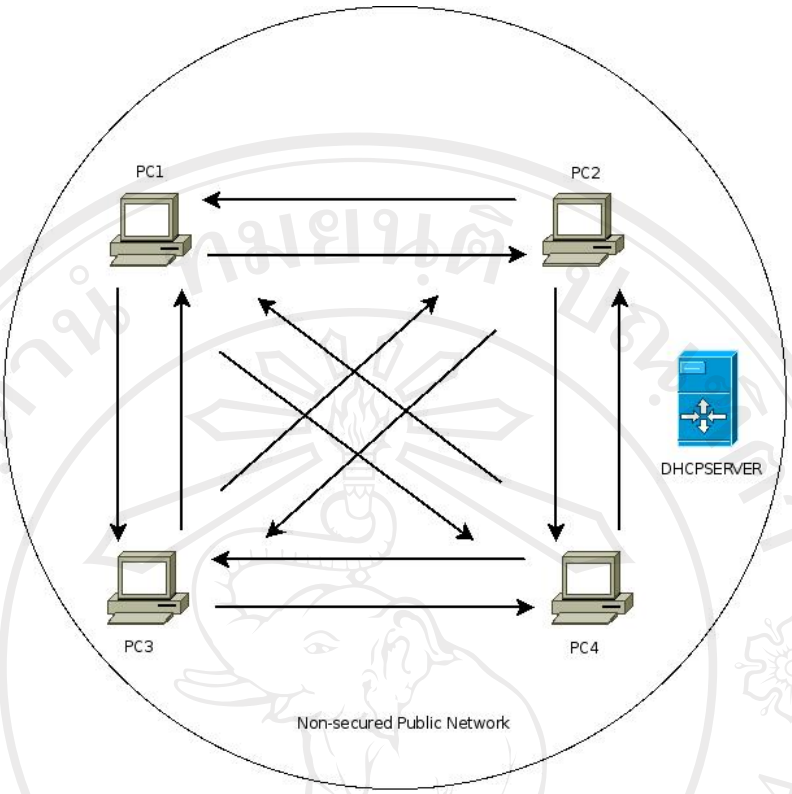
ซึ่งข้อมูลจากการทดลองแต่ละแบบ เพื่อนำมาวิเคราะห์และสรุปผลการทดลองการปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธาณะ

6.1 สรุปและวิเคราะห์การวิจัย

จากการทดลองใช้งาน การปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ เพื่อรองรับการใช้งานของผู้ใช้ที่ไม่ได้รับสิทธิ (Unauthorized User) และกลุ่มผู้ใช้งานที่ได้รับสิทธิ (Authorized User) โดยไม่มีการติดตั้งโปรแกรมเพิ่มบนเครื่องลูกข่าย รองรับการใช้งานของกลุ่มผู้ใช้งานแบบชั่วคราว (Guest User) ซึ่งเป็นประเภทหนึ่งของกลุ่มผู้ใช้ที่ไม่ได้รับสิทธิ (Unauthorized User) สามารถแบ่งกลุ่มลักษณะการใช้งานหลัก ๆ ออกเป็นสี่กลุ่มหลักคือ เครือข่ายคอมพิวเตอร์แบบสาธารณะชนิดปกติ (Non-secured Public Network), เครือข่ายคอมพิวเตอร์แบบสาธารณะป้องกันความปลอดภัย (Secured Public Network), เครือข่ายคอมพิวเตอร์แบบส่วนตัวป้องกันความปลอดภัย (Secured Private Network) และเครือข่ายคอมพิวเตอร์แบบส่วนตัวชนิดปกติ (Non-secured Private Network) ซึ่งมีรายละเอียดดังต่อไปนี้

6.1.1 เครือข่ายคอมพิวเตอร์แบบสาธารณะชนิดปกติ (Non-secured Public Network)

เครือข่ายคอมพิวเตอร์แบบสาธารณะชนิดปกติ (Non-secured Public Network) เป็นการใช้งานไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลแบบเดิม ลักษณะผู้ใช้งานเป็นได้ทั้งผู้ใช้งานที่ได้รับสิทธิ (Authorized User) และผู้ใช้งานที่ไม่ได้รับสิทธิ (Unauthorized User) แม้ว่าไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลแบบเดิม สามารถกำหนดให้บริการเฉพาะกลุ่มผู้ใช้งานที่ได้รับสิทธิ (Authorized User) จากการกำหนดให้บริการเฉพาะเครื่องลูกข่ายที่มี Mac Address ในรายการเครื่องลูกข่ายให้บริการ (Access List) แต่ไม่ได้เป็นลักษณะการแบ่งกลุ่มการใช้งานของเครื่องลูกข่ายเป็นเพียงการกำหนดรายการให้บริการเฉพาะแก่เครื่องลูกข่าย ซึ่งการเข้าสู่ระบบเครือข่ายของผู้ใช้งานที่ไม่ได้รับสิทธิ (Unauthorized User) ก็สามารถทำได้โดยกำหนดค่าเครือข่ายแบบ Static คือการกำหนดค่าระบบเครือข่ายโดยไม่จำเป็นต้องได้รับค่าจากเครื่องแม่ข่ายที่ให้บริการ DHCP ในการสื่อสารข้อมูลระหว่างเครื่องลูกข่ายในระบบเครือข่าย เครื่องลูกข่ายสามารถสื่อสารข้อมูลกับเครื่องลูกข่ายอื่น ๆ ในระบบได้อย่างอิสระโดยเครื่องแม่ข่ายไม่สามารถควบคุมการสื่อสารข้อมูลใด ๆ ของเครื่องลูกข่ายได้ ดังรูปที่ 6.1 เรียกระบบเครือข่ายนี้ว่า เครือข่ายคอมพิวเตอร์แบบสาธารณะชนิดปกติ (Non-secured Public Network) เนื่องจากกลุ่มเครื่องลูกข่ายในระบบเครือข่ายนี้สามารถสื่อสารข้อมูลกับเครื่องลูกข่ายอื่นได้อย่างอิสระ เหมาะสำหรับระบบเครือข่ายที่ไม่ต้องการควบคุมการสื่อสารข้อมูลระหว่างเครื่องลูกข่ายภายในระบบเครือข่าย และต้องการความเร็วในการสื่อสารข้อมูลของเครื่องลูกข่าย เพราะเครื่องลูกข่ายไม่จำเป็นต้องส่งผ่านข้อมูลผ่านเครื่องแม่ข่าย

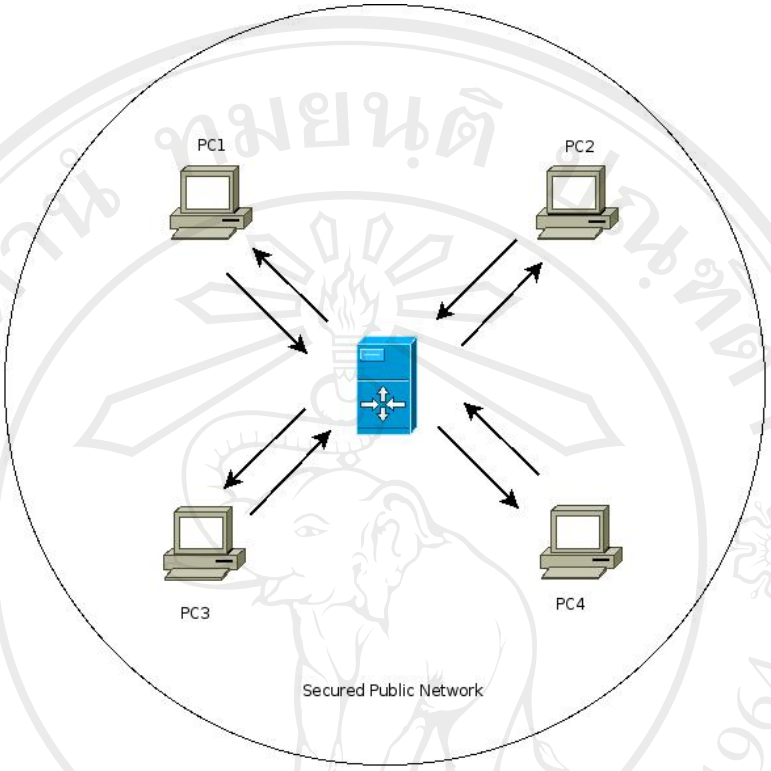


รูปที่ 6.1 แผนภาพสรุประบบเครือข่ายคอมพิวเตอร์แบบปกติ

6.1.2 เครือข่ายคอมพิวเตอร์แบบสาธารณะป้องกันความปลอดภัย (Secured Public Network)

เครือข่ายคอมพิวเตอร์แบบสาธารณะป้องกันความปลอดภัย (Secured Public Network) เป็นการใช้งานการปรับปรุงระบบความปลอดภัยของ ไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ เพื่อรองรับการใช้งานของผู้ใช้งานที่ไม่ได้รับสิทธิ (Unauthorized User) โดยกำหนดกฎพื้นฐานในการสื่อสารข้อมูลระหว่างเครื่องลูกข่ายในระบบเครือข่าย ให้ไม่สามารถสื่อสารข้อมูลซึ่งกันและกันได้ และเครื่องลูกข่ายไม่สามารถกำหนดค่าเครือข่ายแบบ Static ในการเข้าสู่ระบบเครือข่าย ทำให้สามารถควบคุมการสื่อสารข้อมูลของเครื่องลูกข่ายในระบบได้ คือเครื่องลูกข่ายในระบบไม่สามารถสื่อสารข้อมูลซึ่งกันและกันได้อย่างอิสระ ดังรูปที่ 6.2 จากการทดลองเครื่องลูกข่ายในเครือข่ายคอมพิวเตอร์แบบสาธารณะป้องกันความปลอดภัย (Secured Public Network) สรุปได้ว่าเครื่องลูกข่ายไม่สามารถเชื่อมต่อกันได้อย่างอิสระ เหมาะสำหรับระบบเครือข่ายที่เป็นลักษณะสาธารณะ ที่ต้องการควบคุมการสื่อสารข้อมูลเครื่องลูกข่ายของผู้ใช้งานที่ไม่ได้รับสิทธิ (Unauthorized User) ภายในระบบเครือข่าย โดยการส่งผ่านข้อมูลจะผ่านเครื่องแม่ข่ายที่ให้บริการ DHCP ถ้าอยู่ในกลุ่ม เครือข่าย

คอมพิวเตอร์แบบสาธารณะป้องกันความปลอดภัย (Secured Public Network) โดยกฎพื้นฐานเครื่องแม่ข่ายจะไม่อนุญาตให้มีการสื่อสารระหว่างเครื่องลูกข่ายในระบบ

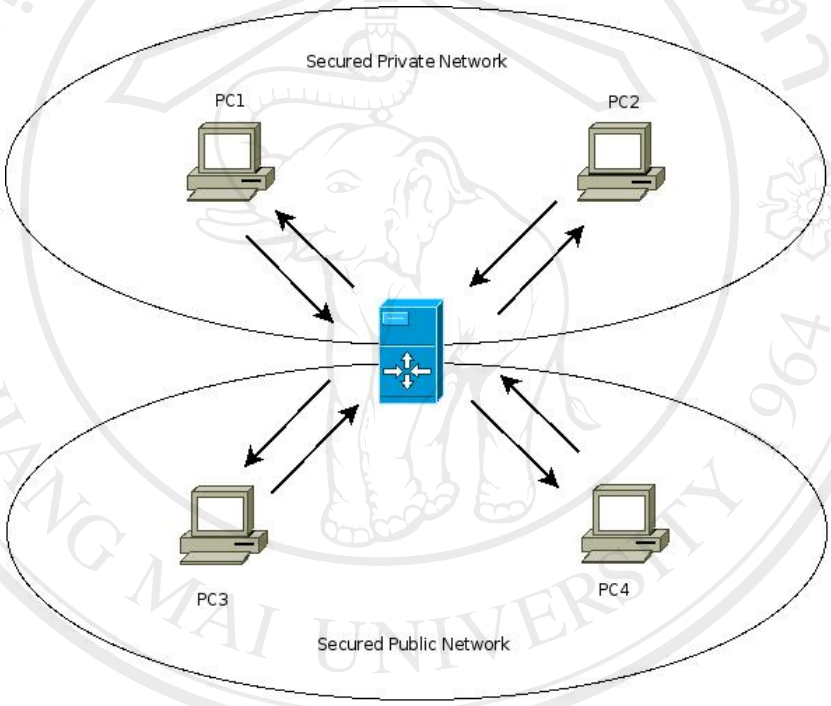


รูปที่ 6.2 แผนภาพสรุประบบเครือข่ายคอมพิวเตอร์แบบสาธารณะป้องกันความปลอดภัย (Secured Public Network)

6.1.3 เครือข่ายคอมพิวเตอร์แบบส่วนตัวป้องกันความปลอดภัย (Secured Private Network)

เครือข่ายคอมพิวเตอร์แบบส่วนตัวป้องกันความปลอดภัย (Secured Private Network) เป็นการใช้งานการปรับปรุงระบบความปลอดภัยของ ไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ เพื่อรองรับการใช้งานของผู้ใช้งานที่ได้รับสิทธิ (Authorized User) โดยกำหนดกฎพื้นฐานในการสื่อสารข้อมูลระหว่างเครื่องลูกข่ายในระบบเครือข่ายให้ สามารถสื่อสารข้อมูลกันได้กับเครื่องลูกข่ายในกลุ่มเครือข่ายคอมพิวเตอร์แบบส่วนตัวป้องกันความปลอดภัย (Secured Private Network) แต่ไม่สามารถสื่อสารข้อมูลกับเครื่องลูกข่ายกลุ่มอื่นได้ โดยเครื่องลูกข่ายไม่สามารถกำหนดค่าเครือข่ายแบบ Static คือกำหนดค่าเครือข่ายเองโดยไม่จำเป็นต้องได้รับค่าจากเครื่องแม่ข่ายที่ให้บริการ DHCP ได้ ซึ่งลักษณะการใช้งานเป็นการใช้งานบนระบบเครือข่าย สามารถควบคุมการสื่อสารข้อมูลของเครื่องลูกข่ายในระบบคือกลุ่มเครื่องลูกข่ายในเครือข่ายคอมพิวเตอร์แบบส่วนตัวป้องกันความปลอดภัย (Secured Private Network) สามารถสื่อสารข้อมูลซึ่งกันและกันได้โดยควบคุมการเชื่อมต่อส่งผ่านเครื่องแม่ข่ายที่ให้บริการ DHCP ดังรูปที่ 6.3 จากการทดลองเครื่องลูกข่ายใน เครือข่ายคอมพิวเตอร์แบบ

ส่วนตัวป้องกันความปลอดภัย (Secured Private Network) เหมาะสำหรับระบบเครือข่ายที่เป็นแบบส่วนตัวใช้งานรวมกับแบบสาธารณะ ที่ต้องการควบคุมการสื่อสารข้อมูลระหว่างเครื่องลูกข่ายภายในระบบเครือข่าย ให้สามารถสื่อสารข้อมูลกันได้ภายในกลุ่มเครื่องลูกข่ายเครือข่ายคอมพิวเตอร์แบบส่วนตัวป้องกันความปลอดภัย (Secured Private Network) แต่ไม่สามารถสื่อสารข้อมูลกับกลุ่มอื่นได้ โดยการส่งผ่านข้อมูลจะผ่านเครื่องแม่ข่ายที่ให้บริการ DHCP ถ้าอยู่ในเครือข่ายคอมพิวเตอร์แบบส่วนตัวป้องกันความปลอดภัย (Secured Private Network)โดยกฎพื้นฐานเครื่องแม่ข่ายที่ให้บริการ DHCP อนุญาตให้มีการสื่อสารระหว่างเครื่องลูกข่ายในระบบได้ แต่ไม่สามารถสื่อสารกับกลุ่มอื่นได้

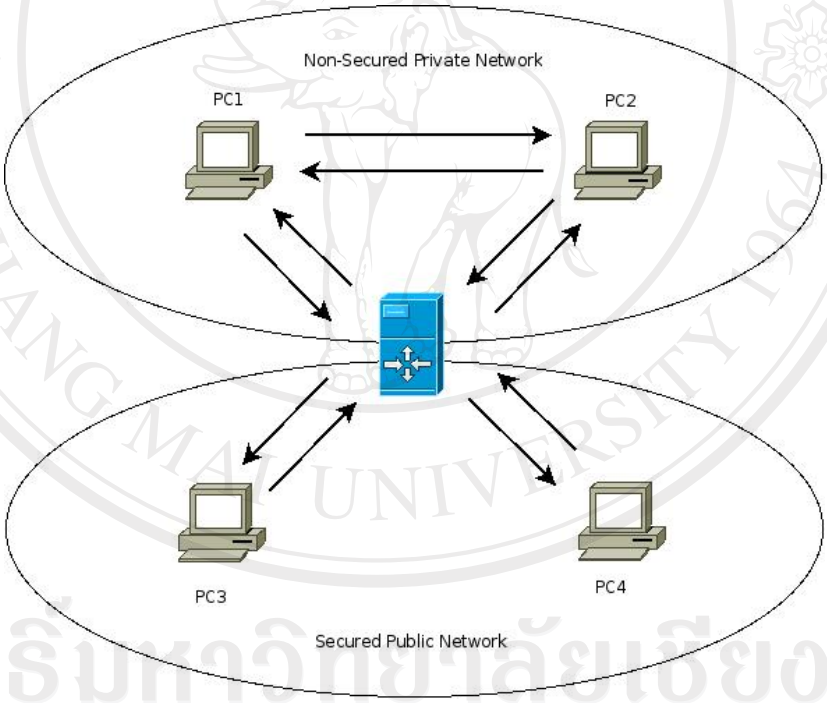


รูปที่ 6.3 แผนภาพสรุประบบเครือข่ายคอมพิวเตอร์แบบส่วนตัวป้องกันความปลอดภัย (Secured Private Network)

6.1.4 เครือข่ายคอมพิวเตอร์แบบส่วนตัวชนิดปกติ (Non-secured Private Network)

เครือข่ายคอมพิวเตอร์แบบส่วนตัวชนิดปกติ (Non-secured Private Network) เป็นการใช้งานการปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ เพื่อรองรับการใช้งานของผู้ใช้งานที่ได้รับสิทธิ (Authorized User) โดยกำหนดกฎพื้นฐานในการเชื่อมต่อระหว่างเครื่องลูกข่ายในระบบเครือข่ายให้สามารถสื่อสารข้อมูลกันได้กับเครื่องลูกข่ายในกลุ่มเครือข่ายคอมพิวเตอร์แบบส่วนตัวชนิดปกติ (Non-secured Private Network) แต่ไม่สามารถสื่อสารข้อมูลกับเครื่องลูกข่ายกลุ่มอื่นได้ โดยเครื่องลูกข่ายสามารถกำหนดค่าเครือข่ายแบบ Static ซึ่งลักษณะการใช้งานเป็นการใช้งานบน

ระบบเครือข่ายไม่สามารถควบคุม การสื่อสารข้อมูลของเครื่องลูกข่ายในกลุ่มเครือข่ายคอมพิวเตอร์แบบส่วนตัวชนิดปกติ (Non-secured Private Network) สามารถเชื่อมต่อซึ่งกันและกันได้โดยอิสระ โดยไม่ผ่านการควบคุมการสื่อสารข้อมูลส่งผ่านเครื่องแม่ข่าย ดังรูปที่ 6.4 จากการทดลองเครื่องลูกข่ายในเครือข่ายคอมพิวเตอร์แบบส่วนตัวชนิดปกติ (Non-secured Private Network) เหมาะสำหรับระบบเครือข่ายที่ไม่ต้องการควบคุมการเชื่อมต่อระหว่างเครื่องลูกข่ายของผู้ใช้งานที่ได้รับสิทธิ (Authorized User) ภายในกลุ่มระบบเครือข่าย และต้องการความเร็วในการเชื่อมต่อของเครื่องลูกข่ายของผู้ใช้งานที่ได้รับสิทธิ (Authorized User) เพราะไม่ต้องส่งผ่านข้อมูลผ่านเครื่องแม่ข่ายของเครือข่ายแบบส่วนตัว ทำให้ขาดความปลอดภัยและการแอบแฝงของเครื่องลูกข่ายของผู้ใช้งานที่ไม่ได้รับสิทธิ (Unauthorized User) เข้ามาใช้งานระบบและเข้าถึงเครื่องลูกข่ายอื่น ๆ ที่อยู่ในกลุ่มเครือข่ายคอมพิวเตอร์แบบส่วนตัวชนิดปกติ (Non-secured Private Network) ได้



รูปที่ 6.4 แผนภาพสรุประบบเครือข่ายคอมพิวเตอร์แบบส่วนตัวชนิดปกติ (Non-secured Private Network)

6.1.5 สรุปคุณสมบัติการปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ

จากผลลัพท์ที่ได้ข้างต้นสามารถนำมาสรุปเป็นตารางเปรียบเทียมคุณสมบัติต่าง ๆ ในแต่ละรูปแบบการใช้งานของระบบเครื่อข่าย โดยแยกคุณสมบัติออกเป็น ค่าใช้จ่าย, ความซับซ้อน, การ

ดูแลจัดการ, ความยืดหยุ่น, รอบรับผู้ใช้งาน Unauthorized User, การติดตั้งโปรแกรมเพิ่ม, การแบ่งกลุ่ม ดังรูปตารางที่ 6.1 ซึ่งคุณสมบัติหลักที่สามารถวัดผลได้คือ การรองรับผู้ใช้งานไม่ได้รับสิทธิ (Unauthorized User) โดยการปรับปรุงระบบความปลอดภัยของไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอลสำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ สามารถจำกัดการเชื่อมต่อของเครื่องลูกข่ายที่อยู่ในกลุ่มผู้ใช้งานไม่ได้รับสิทธิ, การติดตั้งโปรแกรมเพิ่มเครื่องลูกข่ายซึ่งระบบการปรับปรุงความปลอดภัยไม่จำเป็นต้องติดตั้งโปรแกรมเพิ่ม ทำให้เครื่องลูกข่ายสะดวกในการเข้ามาใช้งานระบบเครือข่าย, การแบ่งกลุ่ม ระบบการปรับปรุงความปลอดภัย สามารถรองรับกลุ่มผู้ใช้งานได้รับสิทธิ (Authorized User) เป็นสองกลุ่มหลัก ๆ คือ แบบส่วนตัวป้องกันความปลอดภัยและแบบส่วนตัวแบบปกติ จากคุณสมบัติหลักข้างต้นทำให้ระบบการปรับปรุงความปลอดภัย มีค่าใช้จ่ายต่ำ เพราะไม่ต้องใช้อุปกรณ์เครือข่ายที่มีราคาแพง, ลดความซับซ้อนของระบบและทำให้ง่ายต่อการดูแลจัดการระบบ เพราะใช้เทคโนโลยีพื้นฐานในการใช้งาน, ความยืดหยุ่นของระบบสูงขึ้นเนื่องจากสามารถแบ่งกลุ่มของผู้ใช้งานได้ ซึ่งเป็นคุณสมบัติรอง จากคุณสมบัติดังกล่าวเพื่อความเหมาะสมกับการใช้งานในระบบเครือข่ายแบบสาธารณะ

ตารางที่ 6.1 สรุปเปรียบเทียบคุณสมบัติของแต่ละวิธีในการใช้งานในระบบเครือข่ายแบบสาธารณะ

รายละเอียด	ปรับปรุง DHCP	Single VLAN	Client VPN	Multi VLAN
รองรับผู้ใช้งานไม่ได้รับสิทธิ	รองรับ	ไม่รองรับ	รองรับ	รองรับ
การติดตั้งโปรแกรมเพิ่ม	ไม่จำเป็น	ไม่จำเป็น	จำเป็น	ไม่จำเป็น
การแบ่งกลุ่ม	สามารถแบ่งกลุ่ม	ไม่สามารถ	สามารถแบ่งกลุ่ม	สามารถแบ่งกลุ่ม
ค่าใช้จ่าย	ต่ำ	ต่ำ	ปานกลาง	สูง
ความซับซ้อน	ต่ำ	ต่ำ	ปานกลาง	สูง
การดูแลจัดการ	ง่าย	ง่าย	ปานกลาง	ยาก
ความยืดหยุ่น	สูง	ต่ำ	ปานกลาง	สูง

6.2 ปัญหาที่พบและข้อเสนอแนะ

6.2.1 การปรับปรุงการทำงานไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ ทำงานแบบเครื่องแม่ข่ายลักษณะเดี่ยว (Single Server) เท่านั้น ซึ่งในการทำงานที่ต้องการความเสถียรภาพของระบบ ต้องสามารถทำงานแบบเครื่องแม่ข่ายลักษณะกลุ่ม (Multi Server)

6.2.2 การปรับปรุงการทำงานไดนามิกโฮสต์คอนฟิกกิวเรชันโปรโตคอล สำหรับสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ ทำงานบนเครือข่ายคอมพิวเตอร์ประเภทเครือข่าย IPv4 เท่านั้น ซึ่งในอนาคตเครือข่ายคอมพิวเตอร์ จะทำงานบนเครือข่ายคอมพิวเตอร์ประเภทเครือข่าย IPv6