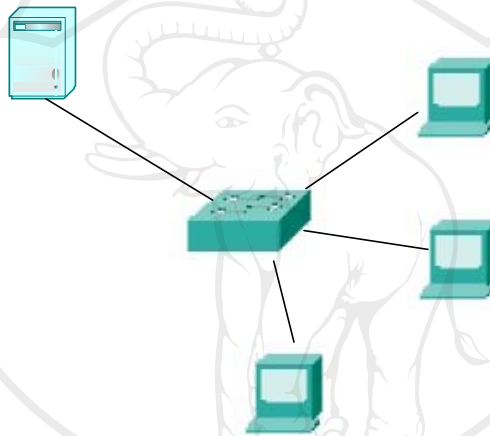


บทที่ 2

การวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์แบบสาธารณะ

2.1 การวิเคราะห์การทำงานไดนามิกโฮสต์คอนฟิกิวเรชันโปรโตคอลกับอุปกรณ์กระจายสัญญาณชนิดไม่มีการจัดการ (Unmanaged Switch) สำหรับเครือข่ายคอมพิวเตอร์แบบสาธารณะ

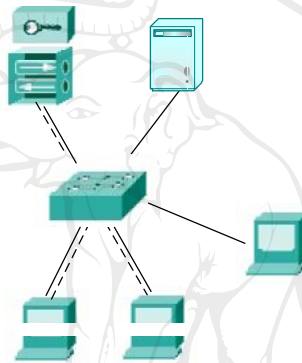


รูปที่ 2.1 การใช้งานเทคโนโลยี Single VLAN ในเครือข่ายคอมพิวเตอร์แบบสาธารณะ

กลุ่มที่มีการใช้งานระบบ DHCP นำมาใช้งานในเครือข่ายที่เป็น Public Area Network เรียกว่า DHCP (Single VLAN) ดังรูปที่ 2.1 คือ ลักษณะเครื่องลูกข่ายที่เชื่อมต่อกับ Switch Layer 1 (Unmanaged Switch) ใช้งานในระบบเครือข่ายโดยกำหนดค่าเครือข่ายและ IP address แบบ Static หรือ Dynamic ในการสื่อสารภายในเครือข่าย โดยการกำหนดค่าเครือข่ายและ IP address แบบ Dynamic ได้รับมาจาก DHCP Server ซึ่งอยู่ใน Server Zone และเครื่องลูกข่ายเป็นลักษณะของผู้ใช้งาน Unauthorized ซึ่ง อาจจะเป็นผู้ใช้งาน Unauthorized เพื่อใช้งานระบบจริง หรือเป็นผู้ไม่หวังดีก็ได้ ระบบอาจจะทำการตรวจสอบโดย DHCP ทำการเก็บข้อมูล MAC Address ในการอนุญาตการใช้งานระบบเครือข่าย ทำให้ยุ่งยากในการใช้งานของผู้ใช้งาน Unauthorized และผู้ดูแลระบบ แต่จริง ๆ ผู้ไม่หวังดี อาจจะทำการแทรกซึมเข้ามาในระบบเครือข่ายได้ง่าย โดยใช้วิธีการกำหนดค่าเครือข่ายและ IP address เป็นลักษณะ Static ที่อยู่ใน Subnet เดียวกับ Subnet ที่ใช้งาน ก็สามารถจะทำการใช้งานระบบได้ และยังสามารถ Access เครื่องลูกข่ายในระบบอื่น, เครื่องแม่ข่ายและอุปกรณ์เน็ตเวิร์กอื่นๆ ในระบบได้ถ้าเปิดช่องโหว่ไว้

ซึ่งแน่นอนเครื่องลูกข่ายที่อยู่ในระบบไม่ปลอดภัยแน่นอน และไม่สามารถควบคุมเครื่องลูกข่ายในลักษณะของผู้ใช้งานไม่ได้รับสิทธิ (Unauthorized User) ใน Public Area Network แต่ข้อดีของระบบในลักษณะนี้คือ ใช้งบประมาณค่อนข้างต่ำ, ไม่ต้องใช้ความรู้ของผู้ดูแลระบบมาก, เครื่องลูกข่ายไม่จำเป็นต้องติดตั้งโปรแกรมเพิ่มเติม, ใช้งานการกำหนดค่าเครื่องข่ายและ IP address ได้ทั้ง Static และ Dynamic

2.2 การวิเคราะห์การทำงานเครือข่ายเสมือนส่วนตัว(Virtual Private Network) สำหรับเครือข่ายคอมพิวเตอร์แบบสาธารณะ



รูปที่ 2.2 การใช้งานเทคโนโลยี VPN Client ในเครือข่ายคอมพิวเตอร์แบบสาธารณะ

รูปแบบการเชื่อมต่อลักษณะ Client VPN ดังรูปที่ 2.2 คือลักษณะที่เครื่องลูกข่ายเชื่อมต่อกับ Switch Layer 1 (Unmanaged Switch) หรือ Switch Layer 3 (Managed Switch) และทำการเชื่อมต่อไปยัง VPN Server เพื่อทำการร้องขอการเชื่อมต่อโดยใช้ลักษณะ Tunnel เพื่อใช้งานระบบเครือข่าย ทำให้เครื่องลูกข่ายในลักษณะนี้มีความปลอดภัยของข้อมูลและป้องกันการโจมตีจากผู้ไม่หวังดี ได้ระดับหนึ่ง การใช้งานในลักษณะนี้ เครื่องลูกข่ายต้องติดตั้ง VPN Client Software [11] เพื่อใช้งาน ซึ่งมีหลายค่าย และแต่ละค่ายก็ใช้ VPN Client Software ระบบเครือข่ายต่างกัน ซึ่งมีความยุ่งยากในการใช้งานและมีความไม่เหมาะสมของระบบเครือข่าย ซึ่งลักษณะของผู้ใช้งาน ต้องมีการติดตั้ง VPN Client Software ของทุก ๆ เครื่องในระบบเครือข่ายที่ต้องการใช้งานระบบเครือข่าย ทำให้มีผลกระทบในการใช้งบประมาณในการจัดการระบบเครือข่าย และผู้ดูแลระบบต้องมีการจัดการระบบ VPN ทำให้ก่อให้เกิดความยุ่งยาก และไม่เหมาะสมกับการใช้งานในลักษณะสภาพแวดล้อมเครือข่ายคอมพิวเตอร์แบบสาธารณะ ส่วนข้อดีคือความปลอดภัยของระบบเครือข่าย

**VPN
Server**

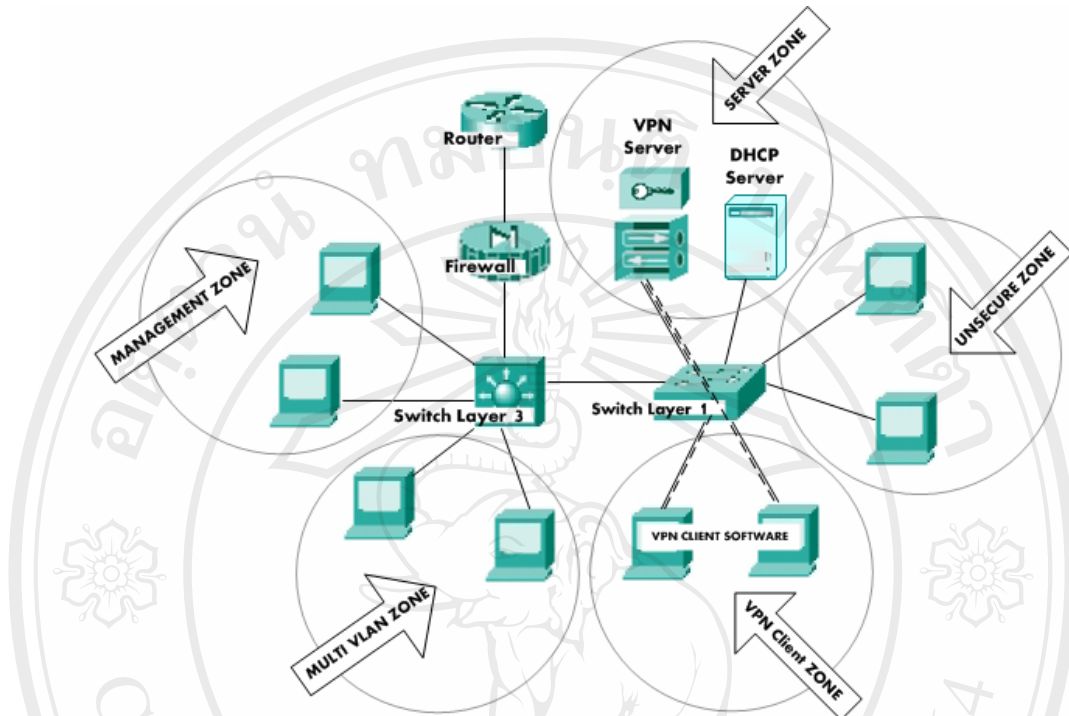
2.3 การวิเคราะห์การทำงานไดนามิกโสตต์คอนฟิกิเวอร์ชันโปรโตคอลกับอุปกรณ์กระจายสัญญาณชนิดมีการจัดการ (Managed Layer 3 Switch) สำหรับเครือข่ายคอมพิวเตอร์แบบสาธารณะ



**DHCP
Server**

Switch Layer 3

2.4 สรุปการวิเคราะห์ วิธีจัดการสำหรับเครือข่ายคอมพิวเตอร์แบบสาธารณะ



รูปที่ 2.4 การใช้งานเทคโนโลยีปัจจุบันในเครือข่ายคอมพิวเตอร์แบบสาธารณะ

จากวิธีการข้างต้นดังรูปที่ 2.4 แต่ละรูปแบบมีข้อดีและข้อเสียที่แตกต่างกัน เป็นวิธีการที่เหมาะสมสำหรับการใช้งานในเครือข่ายที่เป็นลักษณะ Public Area Network ที่มีการใช้งานของผู้ใช้งาน Unauthorized เพื่อตอบสนองการทำงานในเครือข่ายแบบ Public Area Network โดยมีลักษณะดังนี้

- งบประมาณต่ำ
- ระบบมีความซับซ้อนน้อย เวลาเกิดปัญหาสามารถตรวจสอบได้ง่าย
- ง่ายต่อการจัดการ จัดการระบบได้จากจุดเดียว ไม่ต้องจัดการแต่ละอุปกรณ์
- ยืดหยุ่นต่อการใช้งาน กำหนด Policy ได้
- ระบบมีความปลอดภัย รองรับการทำงานของผู้ใช้งานแบบ Unauthorized
- เครื่องลูกข่ายไม่ต้องยุ่งยากในการลง Software หรือกำหนดค่าเพิ่มเติม
- กำหนดได้หลาย ๆ กลุ่ม ตามความเหมาะสมของแต่ละกลุ่ม

ตาราง 2.1 เปรียบเทียบคุณสมบัติของแต่ละวิธีในการใช้งานในระบบเครือข่ายแบบสาธารณะ

รายละเอียด	Single VLAN	Client VPN	Multi VLAN
ค่าใช้จ่าย	ต่ำ	ปานกลาง	สูง
ความซับซ้อน	ต่ำ	ปานกลาง	สูง
การดูแลจัดการ	ง่าย	ปานกลาง	ยาก
ความยืดหยุ่น	ต่ำ	ปานกลาง	สูง
รองรับผู้ใช้งาน Unauthorized	ไม่รองรับ	รองรับ	รองรับ
การติดตั้งโปรแกรมเพิ่ม	ไม่จำเป็น	จำเป็น	ไม่จำเป็น
การแบ่งกลุ่ม	ไม่สามารถแบ่งกลุ่ม	สามารถแบ่งกลุ่ม	สามารถแบ่งกลุ่ม

จากวิธีการข้างต้น สามารถจำแนกคุณลักษณะต่าง ๆ ได้ตามหัวข้อดังต่อไปนี้ คือ ค่าใช้จ่ายของระบบเครือข่าย, ความซับซ้อนของระบบเครือข่าย, ความยุ่งยากในการจัดการระบบเครือข่ายของผู้ดูแลระบบ, ความยืดหยุ่นในการใช้งานของระบบเครือข่าย, การรองรับลักษณะของผู้ใช้งานแบบ Unauthorized, ความจำเป็นในการติดตั้งโปรแกรมเพิ่มเติม, การรองรับการแบ่งกลุ่มของเครื่องลูกข่ายในระบบเครือข่าย ซึ่งในแต่ละวิธีการ คือ Single VLAN, Client VPN, Multi VLAN มีรายละเอียดดังตารางที่ 2.1

จากคุณสมบัติข้างต้นสามารถแยกคุณสมบัติส่วนที่วัดผลได้ คือ รองรับผู้ใช้งานที่ไม่ได้รับสิทธิ (Unauthorized User), การติดตั้งโปรแกรมเพิ่มเครื่องลูกข่าย, การแบ่งกลุ่ม เพื่อสะดวกต่อการตรวจสอบและประเมินผลของการใช้งาน