

ระบบค้นหาโครงสร้าง VLAN ในเครือข่าย

นพพล เฉยศิริ

งานนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ

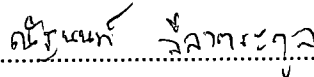
คณะวิทยาการสารสนเทศ มหาวิทยาลัยบูรพา

สิงหาคม 2558

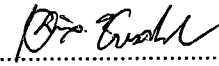
ลิขสิทธิ์เป็นของมหาวิทยาลัยบูรพา

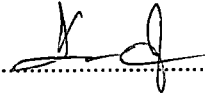
คณะกรรมการควบคุมงานนิพนธ์และคณะกรรมการการสอบงานนิพนธ์ได้พิจารณา
งานนิพนธ์ของ นพปฎล เฉยศิริ จบนี้แล้ว เห็นสมควรรับเป็นส่วนหนึ่งของการศึกษาตาม
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยบูรพาได้

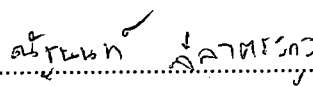
คณะกรรมการควบคุมงานนิพนธ์


..... อาจารย์ที่ปรึกษาหลัก
(ดร. ฉันทนันท์ สีลาตระกูล)

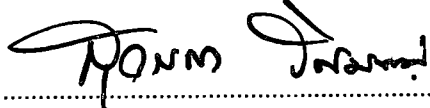
คณะกรรมการสอบงานนิพนธ์


..... ประธานกรรมการ
(ดร. เนติมพล ชาญศรีภิญโญ)


..... กรรมการ
(ดร. คณินิจ กุโบล่า)


..... กรรมการ
(ดร. ฉันทนันท์ สีลาตระกูล)

คณะวิทยาการสารสนเทศ อนุมัติให้รับงานนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตาม
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยบูรพา


..... คณบดีคณะวิทยาการสารสนเทศ

(ผู้ช่วยศาสตราจารย์ ดร. สุวรรณ รัศมีขวัญ)

วันที่ 17 เดือน สิงหาคม พ.ศ. 2558

กิตติกรรมประกาศ

งานนิพนธ์ฉบับนี้สำเร็จลงได้นั้น ต้องขอขอบพระคุณ ดร.ณัฐนนท์ ติลาตระกูล อาจารย์ที่ปรึกษางานนิพนธ์เป็นอย่างสูง ที่ให้คำปรึกษาและให้คำแนะนำในการดำเนินงาน และช่วยแก้ไขข้อบกพร่องต่าง ๆ จนสำเร็จ

ขอขอบพระคุณ ดร.เฉลิมพล ชาญศรีภิญโญ และ ดร.คณินิจ กุโธตา ที่กรุณาให้คำแนะนำ ทำให้งานนิพนธ์ฉบับนี้มีความสมบูรณ์ขึ้น

สุดท้ายนี้ขอกราบขอบพระคุณ คุณแม่อุไร คุณพ่อสุทัศน์ เฉยศิริ และพี่ ๆ ที่คอยสนับสนุนและให้กำลังใจในการศึกษาต่อครั้งนี้

นพปฎล เฉยศิริ

56920004: สาขาวิชา: เทคโนโลยีสารสนเทศ; วท.ม. (เทคโนโลยีสารสนเทศ)

คำสำคัญ: SNMP/ VLAN/ การค้นหา VLAN

นพปฎล เถยศิริ: ระบบค้นหาโครงสร้าง VLAN ในเครือข่าย (VLAN MONITORING NETWORK) อาจารย์ผู้ควบคุมงานนิพนธ์: ฉันทนันท ลีลาตระกูล, Ph.D. 124 หน้า. ปี พ.ศ. 2558.

งานนิพนธ์ฉบับนี้นำเสนอการออกแบบและพัฒนาระบบ สำหรับตรวจสอบการตั้งค่า VLAN และแสดงผังภาพการเชื่อมต่อ VLAN เพื่อแก้ปัญหาที่อาจเกิดจากความผิดพลาดของผู้ปฏิบัติงานที่ตั้งค่า VLAN ไม่เหมาะสม เช่น ปลั๊กอินที่มีสมาชิกผู้ใช้งานต่อ VLAN มากเกินไป การอนุญาตให้พอร์ตที่หนึ่ง มี VLAN อื่นที่ไม่สอดคล้องกับ VLAN ของสวิตช์ปลายทางปัญหาเหล่านี้ นอกจากทำให้การบริหารจัดการ VLAN ยากแล้วอาจนำไปสู่การเกิดบรอดคาสท์ และเสี่ยงต่อการถูกโจมตีแบบเลเยอร์ 2 ซึ่งทำให้กระทบต่อประสิทธิภาพการใช้งาน

ระบบค้นหาโครงสร้าง VLAN ใช้การรวบรวมข้อมูล VLAN ผ่านโพรโทคอล SNMP เนื่องจากข้อมูล VLAN ของผู้ผลิตสวิตช์เก็บข้อมูล MIB ไม่เหมือนกัน (เก็บไว้ใน Private MIB) ผู้พัฒนาจึงแสดงวิธีการหาค่า OID ที่เกี่ยวกับ VLAN จากสวิตช์ 3 ยี่ห้อคือ Cisco, Huawei และ ZTE เพื่อเป็นข้อมูลพื้นฐานสำหรับนำไปประยุกต์ใช้กับสวิตช์ยี่ห้ออื่นต่อไป

ผลจากการตรวจสอบ VLAN ที่ได้จากการทดลองในเครือข่ายของผู้ให้บริการอินเทอร์เน็ต ระบบสามารถแสดงให้เห็นถึงการตั้งค่า VLAN ที่ไม่เหมาะสมโดยสามารถรายงาน VLAN สูญหาย, VLAN ที่ไม่จำเป็น และ VLAN ที่ไม่สอดคล้องกับฐานข้อมูลสวิตช์ นอกจากนี้ระบบยังสามารถแสดงเส้นทางการเชื่อมต่อของแต่ละ VLAN ในรูปของแผนผังเครือข่าย

ผู้พัฒนาระบบมีความเห็นว่า การนำระบบตรวจสอบการตั้งค่า VLAN มาใช้ เพื่อรายงาน ปัญหาความผิดพลาดที่อาจเกิดขึ้นช่วยอำนวยความสะดวกและลดระยะเวลาในการทำงานและการแก้ปัญหาให้กับผู้ดูแลเครือข่ายและเพิ่มประสิทธิภาพในการทำงาน

56920004: MAJOR: INFORMATION TECHNOLOGY; M.Sc.
(INFORMATION TECHNOLOGY)

KEYWORDS: SNMP/ VLAN/ VLAN DISCOVERY

NOPPADOL CHOEISIRI: VLAN MONITORING NETWORK. ADVISOR:
NUTTHANON LEELATRAKUL, Ph.D. 124 P. 2015.

In this work, we present a VLAN monitoring system designed and developed for examining VLAN configurations, and demonstrating VLAN topologies. It helps troubleshooting VLAN configuration errors, such as the exceeding number of hosts (or MAC addresses) per VLAN, too many VLANs per switch, and VLAN inconsistency between the ones assigned for trunk ports and the one at destination switches. VLAN misconfiguration may lead to unnecessary broadcast messages, and is vulnerable to layer 2 attacks, which could devastatingly affect network performance.

The system use SNMP protocol to collect VLAN information. However, acquiring VLAN information based on private MIB data of different vendors requires dissimilar OIDs. In this work, we also present how to query VLAN MIB information via SNMP with 3 vendors- Cisco, Huawei and ZTE.

The experiments are conducted after deploying our system in the national service provider's network. The results show that our system can discover various VLAN misconfigurations (i.e., missing VLANs, unnecessary VLANs and inconsistent VLANs between switch ports and switch databases). In addition, the system provides VLAN topology visualization.

In conclusion, our VLAN monitoring system can report VLAN setting errors, reducing network administrators' time spent on solving VLAN problems, and increasing productivity.

สารบัญ

| | หน้า |
|--|------|
| บทคัดย่อภาษาไทย..... | ง |
| บทคัดย่อภาษาอังกฤษ..... | จ |
| สารบัญ..... | ฉ |
| สารบัญตาราง..... | ซ |
| สารบัญภาพ..... | ญ |
| บทที่ 1 บทนำ..... | 1 |
| ความเป็นมาและความสำคัญของปัญหา..... | 1 |
| วัตถุประสงค์ของงานนิพนธ์..... | 2 |
| ประโยชน์ที่คาดว่าจะได้รับจากงานนิพนธ์..... | 2 |
| ขอบเขตของระบบ..... | 3 |
| ทรัพยากรที่ใช้ในการดำเนินการ..... | 3 |
| บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง..... | 5 |
| ความรู้เบื้องต้นเกี่ยวกับ VLAN..... | 5 |
| ลักษณะการทำงานของ VLAN..... | 5 |
| ประเภทของ VLAN..... | 6 |
| ประเภทพอร์ตของสวิตช์..... | 7 |
| รูปแบบเฟรมของ VLAN..... | 8 |
| จำนวน VLAN..... | 11 |
| ประโยชน์ของ VLAN..... | 12 |
| โพรโทคอล SNMP..... | 13 |
| รุ่นของ SNMP..... | 13 |
| ตัวจัดการและตัวแทน (Manager and agent) | 14 |
| โครงสร้างข้อมูลเพื่อการจัดการ..... | 15 |
| การตั้งชื่อ OID..... | 16 |
| การอธิบาย OID..... | 17 |
| ตัวอย่างค่า OID..... | 22 |
| วิธีการค้นคืนค่า MIB..... | 23 |

สารบัญ (ต่อ)

| | หน้า |
|--|------|
| การส่งข้อมูลแบบ DSL..... | 26 |
| ขั้นตอนวิธีค้นหาตามแนวคิด..... | 27 |
| การสร้างกราฟ..... | 30 |
| การตั้งค่า VLAN ในสวิตช์เลเยอร์ 2 ที่ควรปฏิบัติ..... | 33 |
| งานวิจัยที่เกี่ยวข้อง..... | 41 |
| บทที่ 3 วิธีดำเนินงาน..... | 44 |
| การวิเคราะห์และออกแบบระบบ..... | 44 |
| คุณสมบัติของระบบ..... | 44 |
| การออกแบบ Use case diagram และ Use case description..... | 45 |
| การออกแบบส่วนติดต่อผู้ใช้งาน..... | 47 |
| การออกแบบฐานข้อมูล..... | 50 |
| การหาค่า OID..... | 58 |
| OID VLAN สวิตช์ Cisco..... | 58 |
| OID VLAN สวิตช์ Huawei..... | 61 |
| OID VLAN สวิตช์ ZTE..... | 64 |
| ส่วนของการพัฒนาโปรแกรม..... | 68 |
| บทที่ 4 ผลการดำเนินงาน..... | 72 |
| ผลการพัฒนาโปรแกรม..... | 72 |
| สรุปผลการนำโปรแกรมไปใช้ตรวจสอบการตั้งค่า VLAN..... | 112 |
| บทที่ 5 สรุปและแนวทางการพัฒนาต่อ..... | 121 |
| สรุปผล..... | 121 |
| ข้อเสนอแนะ..... | 121 |
| แนวทางการพัฒนาต่อ..... | 122 |
| บรรณานุกรม..... | 123 |

สารบัญตาราง

| ตารางที่ | หน้า |
|----------|--|
| 2-1 | รายชื่อฟิลด์และความหมาย..... 10 |
| 2-2 | อธิบายขอบเขตการใช้แต่ละช่วงของ VLAN..... 11 |
| 2-3 | ประเภทข้อมูลที่ประกาศใน SMIv1..... 17 |
| 2-4 | สิทธิ์ในการเข้าถึงข้อมูล (Access)..... 21 |
| 2-5 | ความหมายของสถานภาพ..... 21 |
| 2-6 | OID ในกลุ่มของ system..... 22 |
| 2-7 | OID ในกลุ่มของ interface..... 22 |
| 2-8 | option ที่ใช้บ่อยของคำสั่ง Net-snmp..... 24 |
| 2-9 | ค่าพารามิเตอร์ต่าง ๆ ที่ต้องกำหนดก่อนการเรียกใช้ Arbor..... 31 |
| 2-10 | โหมดของโพรโทคอล DTP ต่าง ๆ ที่สามารถเลือกได้..... 33 |
| 2-11 | ผลลัพธ์เมื่อเลือกการตั้งค่า DTP ในโหมดต่าง ๆ 34 |
| 2-12 | ขั้นตอนการใช้คำสั่งในการจำกัดที่อยู่ MAC..... 35 |
| 2-13 | การใช้คำสั่งเปิดการทำงานของ DHCP snooping..... 39 |
| 2-14 | คำสั่งที่ใช้ในการป้องกันการโจมตีด้วย ARP..... 41 |
| 3-1 | รายละเอียดของยูสเคสในระบบ..... 46 |
| 3-2 | ตาราง region..... 52 |
| 3-3 | ตาราง pop..... 52 |
| 3-4 | ตาราง vender..... 52 |
| 3-5 | ตาราง devices..... 52 |
| 3-6 | ตาราง host_snmp_cache..... 54 |
| 3-7 | ตาราง host_vlan_cache..... 54 |
| 3-8 | ตาราง host_uplink..... 54 |
| 3-9 | ตาราง log_polling..... 55 |
| 3-10 | ตาราง oui..... 55 |
| 3-11 | ตาราง rpt_dfs..... 55 |

สารบัญตาราง (ต่อ)

| ตารางที่ | หน้า |
|---|------|
| 3-12 ตาราง rpt_nomaclearn..... | 56 |
| 3-13 ตาราง rpt_vlancount..... | 56 |
| 3-14 ตาราง user..... | 56 |
| 3-15 ตาราง user_log..... | 57 |
| 3-16 ตาราง vlans..... | 57 |
| 3-17 ตาราง vlan_count..... | 57 |
| 3-18 สรุปค่า OID ที่เกี่ยวข้องกับ VLAN ของสวิตช์ยี่ห้อต่าง ๆ..... | 67 |
| 4-1 จำนวนสวิตช์และจำนวน VLAN ที่ใช้ในการทดสอบ..... | 113 |
| 4-2 จำนวน VLAN ที่สูญหายของแต่ละพื้นที่..... | 113 |
| 4-3 สวิตช์ที่พบ VLAN เพียงพอร์ตเดียวสูงสุด 5 อันดับ..... | 115 |
| 4-4 สวิตช์ที่ไม่มี VLAN ใช้งานและจำนวน VLAN ที่ไม่ได้เรียนรู้ที่อยู่ MAC..... | 116 |
| 4-5 เปรียบเทียบจำนวน VLAN ก่อนและหลังนำระบบเข้าไปตรวจสอบ..... | 118 |
| 4-6 ตัวอย่างปริมาณบรอดคาสท์..... | 119 |
| 4-7 ค่าประสิทธิภาพความถูกต้องของระบบ..... | 119 |
| 4-8 สรุปผลการทำงานของระบบ..... | 120 |

สารบัญภาพ

| ภาพที่ | หน้า |
|--|------|
| 2-1 การใช้งาน VLAN..... | 6 |
| 2-2 ตัวอย่างการใช้งานพอร์ตแอกเซส..... | 7 |
| 2-3 การต่อใช้งานพอร์ตแบบทริงค์..... | 8 |
| 2-4 เฟรม VLAN แบบ ISL..... | 9 |
| 2-5 ภาพแบบเฟรมของ IEEE 802.1Q..... | 10 |
| 2-6 ขนาดของฟิลด์ต่าง ๆ ในอีเทอร์เน็ตเฟรม..... | 10 |
| 2-7 การใช้ VLAN ช่วยให้ประหยัดอุปกรณ์..... | 13 |
| 2-8 ความสัมพันธ์ระหว่างตัวจัดการและตัวแทน..... | 15 |
| 2-9 โครงสร้างการทำงานของโปรโตคอล SNMPv1..... | 15 |
| 2-10 ตัวอย่างลำดับโครงสร้างต้นไม้ของ MIB..... | 17 |
| 2-11 องค์ประกอบการให้บริการอินเทอร์เน็ต..... | 26 |
| 2-12 ลำดับการเดินทางของการค้นหาตามแนวลิบบนโครงสร้างต้นไม้..... | 28 |
| 2-13 ตัวอย่างการท่องไปในกราฟแบบ DFS..... | 29 |
| 2-14 ตัวอย่างที่ได้จากโค้ด Arbor..... | 32 |
| 2-15 การโจมตีแบบ DHCP starvation..... | 37 |
| 2-16 การโจมตีแบบ rogue DHCP server..... | 38 |
| 2-17 การป้องกันการโจมตีด้วย DHCP โดยใช้ DHCP Snooping..... | 38 |
| 2-18 ตัวอย่างการโจมตีด้วย ARP..... | 40 |
| 3-1 Use case diagram ของระบบเฟื่อะวัง VLAN..... | 45 |
| 3-2 การจัดแบ่งพื้นที่หน้าเว็บ..... | 48 |
| 3-3 การวางตำแหน่งโดยรวม..... | 49 |
| 3-4 ตัวอย่างการแสดงผลเมนูย่อย..... | 49 |
| 3-5 หน้าจอการแสดงผลอุปกรณ์แบบ โครงสร้างลำดับชั้น..... | 50 |
| 3-6 หน้าจอแสดงผลแผนภาพเครือข่าย หลังเลือกกลุ่มและ VLAN ที่ต้องการ..... | 50 |
| 3-7 ตาราง ER diagram..... | 51 |
| 3-8 การหาหมายเลข VLAN และชื่อของสวิตช์ Cisco..... | 58 |

สารบัญภาพ (ต่อ)

| | หน้า |
|---|------|
| ภาพที่ | |
| 3-9 จำนวนพอร์ตสมาชิกของ VLAN 104 ในรูปดัชนี..... | 59 |
| 3-10 การแปลงหมายเลขดัชนีให้อยู่ในรูปแบบของชื่อ..... | 59 |
| 3-11 หมายเลข MAC address ตาม VLAN 104..... | 60 |
| 3-12 หมายเลข MAC address และหมายเลขพอร์ตที่เรียนรู้เข้ามา..... | 60 |
| 3-13 การสอบถามหมายเลข VLAN และชื่อ..... | 61 |
| 3-14 พอร์ตที่เป็นสมาชิกแต่ละ VLAN ที่อยู่ในรูปแบบเลขฐาน 16..... | 62 |
| 3-15 การใช้คำสั่งแบบ Command-line เพื่อเปรียบเทียบกับการใช้ SNMP..... | 63 |
| 3-16 การหาค่า mac-address และพอร์ตที่เรียนรู้..... | 63 |
| 3-17 การหาชื่อพอร์ต (ifDescr) จากหมายเลข ifIndex..... | 64 |
| 3-18 ผลจากการใช้คำสั่งแบบ command-line เพื่อแสดงที่อยู่ MAC..... | 64 |
| 3-19 การหาหมายเลข VLAN และชื่อของสวิตช์ ZTE..... | 65 |
| 3-20 การหาพอร์ตที่เป็นสมาชิกของแต่ละ VLAN..... | 65 |
| 3-21 ค่า MAC address ของ VLAN 34 และพอร์ต ifIndex..... | 66 |
| 3-22 การหาค่า ifName เพื่อเทียบกับค่า ifIndex ของสวิตช์ ZTE..... | 66 |
| 3-23 การใช้คำสั่งแบบ command-line แสดง MAC address VLAN 34..... | 67 |
| 3-24 การเชื่อมโยงส่วนประกอบของระบบ..... | 68 |
| 3-25 รหัสเทียมที่ใช้ในการหา VLAN ที่สูญหาย..... | 70 |
| 3-26 แนวคิดการออกแบบระบบเฟื่อะวัง VLAN..... | 71 |
| 4-1 หน้าจอตรวจสอบสิทธิ์เข้าใช้งาน..... | 72 |
| 4-2 เมนูหลักของระบบตรวจสอบการตั้งค่า VLAN..... | 73 |
| 4-3 เมนูย่อยของเมนู Vlan | 73 |
| 4-4 การเปลี่ยนรหัสผ่าน..... | 74 |
| 4-5 การเปลี่ยนข้อมูลผู้ใช้งานและรหัสผ่าน..... | 74 |
| 4-6 ส่วนหัวของตารางข้อมูล..... | 75 |
| 4-7 ส่วนควบคุมตารางส่วนท้าย..... | 75 |
| 4-8 ลักษณะของหน้าจอแสดงผลรวม..... | 76 |

สารบัญญภาพ (ต่อ)

| | หน้า |
|---|------|
| ภาพที่ | |
| 4-9 สรุปสถานะของสวิตช์ทั้งหมดในระบบ..... | 76 |
| 4-10 สวิตช์ที่มี MAC หนาแน่น 10 อันดับ..... | 77 |
| 4-11 พอร์ตของสวิตช์ที่มี VLAN ประกาศไว้สูงสุด 10 อันดับ..... | 77 |
| 4-12 รายชื่อสวิตช์ที่มีจำนวน VLAN (ที่ไม่เรียนรู้ที่อยู่ MAC ภายใน 30 วัน)..... | 78 |
| 4-13 รายชื่อสวิตช์ทั้งหมดที่มีในระบบ..... | 79 |
| 4-14 หน้าจอการเพิ่มสวิตช์เข้าสู่ระบบ..... | 80 |
| 4-15 การเตือนเมื่อป้อนหมายเลขไอพีที่มีอยู่แล้วในระบบ..... | 80 |
| 4-16 การเตือนเมื่อป้อนข้อมูลไม่ครบ..... | 81 |
| 4-17 การเข้าสู่หน้าจอจัดการข้อมูลสวิตช์..... | 81 |
| 4-18 หน้าจอการแก้ไขข้อมูลสวิตช์..... | 82 |
| 4-19 การแจ้งเตือนเมื่อผู้ใช้ไม่มีสิทธิ์ในการแก้ไขข้อมูล..... | 82 |
| 4-20 การลบข้อมูลสวิตช์ออกจากระบบ..... | 83 |
| 4-21 การแจ้งเตือนเมื่อผู้ใช้ไม่มีสิทธิ์ลบข้อมูล..... | 83 |
| 4-22 ข้อมูลการเชื่อมต่อสวิตช์ในระบบ..... | 84 |
| 4-23 การเพิ่มข้อมูลการเชื่อมต่อ..... | 85 |
| 4-24 การเลือกแถวที่ต้องการแก้ไขการเชื่อมต่อ..... | 85 |
| 4-25 หน้าจอการแก้ไขการเชื่อมต่อ..... | 86 |
| 4-26 การลบข้อมูลการเชื่อมต่อ..... | 86 |
| 4-27 การเลือกสรุปจำนวนการใช้งาน VLAN แยกตามพื้นที่..... | 87 |
| 4-28 สรุปจำนวน VLAN ที่ใช้งานของแต่ละสวิตช์..... | 87 |
| 4-29 การแจ้งเตือนเมื่อสวิตช์ที่มีการใช้งาน VLAN เกินร้อยละ 80..... | 88 |
| 4-30 การแบ่งหน้าจอแสดงผลออกเป็น 3 ส่วน..... | 89 |
| 4-31 ข้อมูล VLAN ของแต่ละสวิตช์เมื่อเลือกที่แท็บ VLAN..... | 89 |
| 4-32 แสดงข้อมูลที่อยู่ที่ MAC ในแต่ละ VLAN..... | 90 |
| 4-33 การเลือกพอร์ตเพื่อดูการตั้งค่า VLAN..... | 90 |
| 4-34 การแสดงข้อมูล VLAN ที่ตั้งค่าที่พอร์ต..... | 91 |

สารบัญญภาพ (ต่อ)

| | หน้า |
|--|------|
| ภาพที่ | |
| 4-35 การเลือกสวิตช์ที่ต้องการปรับปรุงข้อมูลของ VLAN..... | 91 |
| 4-36 ข้อมูล VLAN ที่ได้จากการปรับปรุง..... | 92 |
| 4-37 เมนูย่อยภายใต้เมนู Vlan..... | 92 |
| 4-38 การเลือกหมายเลข VLAN ที่ต้องการดูเส้นทาง..... | 93 |
| 4-39 แสดงแผนภาพเส้นทางของ VLAN ตามที่ผู้ใช้เลือก..... | 93 |
| 4-40 การแสดงพอร์ตที่เป็นสมาชิก VLAN | 94 |
| 4-41 การเลือกพอร์ตเพื่อเปรียบเทียบ VLAN..... | 95 |
| 4-42 ผลลัพธ์ที่ได้จากการเปรียบเทียบ VLAN..... | 96 |
| 4-43 การเลือกสวิตช์ต้นทางและปลายทางที่ต้องการหาเส้นทาง..... | 96 |
| 4-44 เครื่องมือการหาจำนวน hop ของสวิตช์..... | 97 |
| 4-45 การแสดงผังภาพเครือข่ายแยกตามพื้นที่..... | 97 |
| 4-46 เมนูรายงานแบ่งออกเป็น 4 กลุ่ม..... | 98 |
| 4-47 รายงาน VLAN ที่มีเส้นทางไม่ครบ..... | 99 |
| 4-48 ผังการเชื่อมต่อเมื่อผู้ใช้เลือกที่หมายเลข VLAN..... | 100 |
| 4-49 การเลือกแสดงจำนวนพอร์ตที่ขอมให้ตั้งค่า VLAN ซ้ำกันได้..... | 100 |
| 4-50 หมายเลข VLAN และจำนวนลิงค์ที่ซ้ำกัน..... | 101 |
| 4-51 แสดงข้อมูลที่อยู่ที่ MAC ในแต่ละ VLAN..... | 101 |
| 4-52 รายละเอียดแต่ละ VLAN ที่ไม่เรียนรู้ที่อยู่ MAC และพอร์ตที่เป็นสมาชิก..... | 102 |
| 4-53 รายงาน VLAN ที่มีสมาชิกเพียงพอร์ตเดียว..... | 102 |
| 4-54 การโหลดไฟล์คำสั่งในการลบ VLAN ที่ไม่ใช้งานออกจากสวิตช์..... | 103 |
| 4-55 ตัวอย่างไฟล์คำสั่งที่ใช้ลบ VLAN..... | 104 |
| 4-56 VLAN ที่ไม่สอดคล้องระหว่างพอร์ตกับฐานข้อมูล VLAN..... | 104 |
| 4-57 สวิตช์ที่มี MAC address ต่อ VLAN สูงสุด..... | 105 |
| 4-58 หน้าจอการค้นหา MAC address ในระบบ..... | 105 |
| 4-59 ผลที่ได้จากการค้นหา MAC address..... | 106 |
| 4-60 เมนูที่เกี่ยวข้องกับการตั้งค่าในระบบ..... | 106 |

สารบัญภาพ (ต่อ)

| | หน้า |
|--|------|
| ภาพที่ | |
| 4-61 การตั้งค่าตัวแปรที่เป็น default ในระบบ..... | 107 |
| 4-62 การตั้งค่าที่ Global จะส่งผลต่อหน้าจอการเพิ่มอุปกรณ์..... | 107 |
| 4-63 แสดงหน้าจอจัดการข้อมูล Region..... | 108 |
| 4-64 แสดงหน้าจอจัดการข้อมูล POP..... | 109 |
| 4-65 แสดงหน้าจอจัดการยี่ห้อสวิตช์..... | 109 |
| 4-66 การตั้งค่าแจ้งเตือนในระบบ..... | 110 |
| 4-67 ส่วนจัดการผู้ใช้งานในระบบ..... | 111 |
| 4-68 การเพิ่มผู้ใช้งานและกำหนดสิทธิ์เข้าใช้งานในระบบ..... | 111 |
| 4-69 การแจ้งข้อผิดพลาดเนื่องจากใส่ข้อมูลผู้ใช้ไม่ครบ ไม่ถูกต้อง..... | 112 |
| 4-70 หน้าจอหลังจากเพิ่มผู้ใช้งานสำเร็จ..... | 112 |
| 4-71 แผนภาพเวนน์-ออยเลอร์แสดงความสัมพันธ์ของ VLAN ที่ไม่จำเป็น..... | 114 |
| 4-72 ตัวอย่าง VLAN ที่มีสมาชิกเพียงพอร์ตเดียว..... | 115 |
| 4-73 การต่อเป็นวงแหวนของสวิตช์ lbg_m3k_02..... | 117 |

บทที่ 1

บทนำ

ความเป็นมาและความสำคัญของปัญหา

เครือข่ายท้องถิ่นเสมือน (Virtual local area network หรือ VLAN) เป็นเทคโนโลยีเครือข่ายที่ทำงานในระดับเลเยอร์ 2 (Layer 2) พบได้ในอุปกรณ์สวิตช์ (Switch) ซึ่งถูกนำมาเชื่อมต่อกันเป็นเครือข่ายท้องถิ่น (Local area network หรือ LAN) โดย VLAN มีความสามารถในการแบ่งกลุ่มผู้ใช้งานออกจากกันเสมือนอยู่ใน LAN ที่แตกต่างกันแม้จะเชื่อมต่อมาจากพอร์ตของสวิตช์ตัวเดียวกัน ผู้ใช้ที่อยู่ต่าง LAN หรือ VLAN ไม่สามารถติดต่อหากันได้โดยตรง ต้องอาศัยอุปกรณ์ระดับเลเยอร์ 3 เช่นเราเตอร์เป็นตัวกลางในการส่งข้อมูลข้อดีด้านหนึ่งที่เกิดจากการแบ่งกลุ่มผู้ใช้งานคือ VLAN ช่วยให้เขตการ broadcast (Broadcast domain) มีขนาดเล็กลดปัญหาการรบกวนที่เกิดจากข้อมูลประเภท broadcast กรณีมีผู้ใช้งานร่วมกันมากในเครือข่ายท้องถิ่น

ด้านผู้ให้บริการ (ISP) ได้นำเทคโนโลยี VLAN มาช่วยแยกประเภทบริการ (เช่น อินเทอร์เน็ตแบบ ADSL (Asymmetric digital subscriber line), บริการเชื่อมต่อเครือข่ายส่วนตัวเสมือน (Virtual private network: VPN), การสื่อสารด้วยระบบ Voice-over-IP (VoIP)) ซึ่งแต่ละบริการก็มีการใช้อุปกรณ์สวิตช์ร่วมกัน เชื่อมต่อเป็นเครือข่ายท้องถิ่นขนาดใหญ่เพื่อให้บริการได้ครอบคลุมทุกพื้นที่ ปัญหาที่พบในเครือข่ายเมื่อมีสวิตช์เชื่อมต่อกันเป็นจำนวนมาก คือ การตั้งค่า VLAN ที่สวิตช์ถูกเปลี่ยนแปลงในโอกาสต่าง ๆ และจำนวนผู้ใช้งานในแต่ละ VLAN อาจเพิ่มขึ้น บางครั้งพบว่าบาง VLAN มีจำนวนผู้ใช้งานต่อ VLAN มากเกินความเหมาะสม (ซึ่งสถานการณ์นี้อาจเกิดจากการจัดการ VLAN ผิดพลาด โดยเฉพาะ VLAN ที่ให้บริการอินเทอร์เน็ตแบบ ADSL ซึ่งมีการขยายตัวสูงขึ้นเรื่อย ๆ ในปัจจุบัน) เมื่อเกิด broadcast ข้นใน VLAN นั้น ทำให้ส่งผลกระทบต่อคุณภาพการให้บริการ

ตามพฤติกรรมการส่งข้อมูลลำดับชั้นเลเยอร์ 2 เมื่อสวิตช์ได้รับเฟรมชนิด broadcast (Broadcast frame) จะส่งเฟรมชนิดนี้กระจายไปยังทุก ๆ พอร์ตที่อยู่ในวง LAN หรือวง VLAN เดียวกันของสวิตช์ยกเว้นพอร์ตที่รับข้อมูลเข้ามา ทำให้เฟรมชนิด broadcast สามารถส่งต่อไปทุก ๆ โหนดใน LAN ซึ่งในขณะที่เฟรม broadcast เกิดขึ้น หน่วยประมวลผลของเครื่องผู้ใช้งานทั้งหมดในเครือข่ายจะหยุดประมวลผลเพื่อตรวจสอบว่าเฟรมข้อมูลที่ได้รับมาเป็นของตนหรือไม่ ถ้าใช่ก็จะตอบกลับไปหากไม่ใช่ก็ทิ้งเฟรมนั้นและกลับไปประมวลผลงานอื่น ๆ ต่อพฤติกรรม

เช่นนี้เป็นการจัดจ้งหะการประมวลผลของผู้ใช้งานในเครือข่าย และหากมีผู้ใช้งานมีจำนวนมากขึ้น จะทำให้เกิดเหตุการณ์แพร่กระจายข้อมูล (หรือเรียกอีกชื่อว่า เหตุการณ์บรอดคาสท์) มีขนาดใหญ่ ทำให้กระทบต่อผู้ใช้และอุปกรณ์ที่อยู่ในเครือข่าย

งานวิจัยของ Edvin skaljo, Nasuf hadziahmetovic, Cevdet akyel นำเสนอผลงานวิจัย เรื่อง Impact of broadcast, Multicast and unknown unicast at low speed dsl connections based at SHDSL แสดงให้เห็นถึงผลกระทบที่เกิดจากบรอดคาสท์และมัลติคาสท์ซึ่งมีผลกระทบต่อคุณภาพการให้บริการโดยทำการทดลองส่งข้อมูลชนิดบรอดคาสท์ จำนวน 100 แพ็กเก็ตต่อวินาที เข้าไปในกลุ่มผู้ใช้ 6 กลุ่มที่อยู่ใน VLAN เดียวกัน (ประมาณ 500 เครื่อง) ผลปรากฏว่าผู้ใช้งานอินเทอร์เน็ตได้ความเร็วที่ลดลงเมื่อเปรียบเทียบกับช่วงเวลาปกติ นอกจากนั้นยังได้เสนอวิธีการแก้ปัญหาโดยการแบ่ง VLAN เพื่อลดจำนวนกลุ่มผู้ใช้งานที่อยู่ใน VLAN เดียวกันลง เนื่องจากเป็นขั้นตอนที่ใช้เวลาน้อยที่สุด

การที่จะบำรุงรักษาและตรวจสอบการตั้งค่า VLAN ในเครือข่ายที่มีอุปกรณ์สวิตช์จำนวนมาก เป็นเรื่องท้าทายผู้ดูแลเครือข่ายอย่างมากเนื่องจากผู้ให้บริการ (บางแห่ง) ขาดระบบบริหารจัดการแบบรวมศูนย์ที่สามารถรวบรวมและตรวจสอบการตั้งค่าแต่ละ VLAN ที่ทุก ๆ พอร์ตของทุก ๆ สวิตช์ ทำให้การตรวจสอบความเหมาะสมของการตั้งค่าของแต่ละ VLAN ต้องใช้เวลานานมากงานนิพนธ์นี้จึงนำเสนอซอฟต์แวร์สำหรับรวบรวมการตั้งค่า VLAN และตรวจสอบการใช้งาน VLAN ในสวิตช์ที่ไม่เหมาะสม เพื่อเป็นเครื่องมือในการช่วยวิเคราะห์ปัญหาที่อาจเกิดขึ้นในเครือข่าย

วัตถุประสงค์ของงานนิพนธ์

เพื่อพัฒนาและออกแบบซอฟต์แวร์สำหรับรวบรวมและตรวจสอบการใช้งาน VLAN ในแต่ละพอร์ตของแต่ละอุปกรณ์สวิตช์ โดยนำข้อมูล VLAN ที่จัดเก็บมาวิเคราะห์และแสดงผล เพื่อช่วยให้แก่ผู้ดูแลระบบเห็นภาพรวมในการใช้งาน VLAN ในเครือข่ายเข้าใจได้ง่ายขึ้น

ประโยชน์ที่คาดว่าจะได้รับจากงานนิพนธ์

1. เพิ่มประสิทธิภาพของเครือข่าย ช่วยลดอัตราการเกิดบรอดคาสท์
2. ช่วยตรวจสอบจำนวนผู้ใช้งานต่อหนึ่ง VLAN ไม่ให้มีจำนวนมากเกินไป
3. แสดงให้เห็นภาพรวมในการใช้งาน VLAN ที่ถูกตั้งค่าในเครือข่ายได้ชัดเจน

เมื่อเกิดปัญหาสามารถดำเนินการตรวจสอบแก้ไขได้อย่างรวดเร็ว

4. ลดความเสี่ยงที่อาจเกิดจากการโจมตีจากผู้ใช้งาน

5. เป็นเครื่องมือเพื่อช่วยสนับสนุนการทำงานแก่ผู้ที่ดูแลระบบหรือพนักงานที่ไม่ได้เป็นผู้เชี่ยวชาญคำสั่งของอุปกรณ์สวิตช์

6. ได้ข้อสรุปวิธีปฏิบัติสำหรับการจัดการ VLAN ที่เหมาะสมและใช้งานได้จริง

ขอบเขตของระบบ

1. การตรวจสอบการใช้งานและค้นหา VLAN ในอุปกรณ์สวิตช์ โดยใช้โปรโตคอล Simple Network Management Protocol (SNMP) และ Telnet ในการเก็บข้อมูล ดังนั้นอุปกรณ์สวิตช์ที่มีอยู่ในเครือข่ายต้องสามารถรองรับโปรโตคอลดังกล่าว และให้สิทธิ์ในการจัดการกับอุปกรณ์ได้

2. การเก็บข้อมูลโดยใช้โปรโตคอล SNMP อุปกรณ์ต้องมี Management information base (MIB) ที่เป็นมาตรฐานและมีเผยแพร่ข้อมูลที่ชัดเจนเช่นอุปกรณ์ที่ผลิตจากบริษัทซิสโก้ (Cisco) มีการเปิดเผยข้อมูล MIB สำหรับบุคคลทั่วไป ส่วนในกรณีที่เป็นสวิตช์จากผู้ผลิตอื่นที่ไม่เปิดเผย อาจทำให้เก็บข้อมูลได้ไม่สมบูรณ์

3. สามารถแสดงความสอดคล้องในการตั้งค่า VLAN ในพอร์ตแบบทั้งที่เชื่อมต่อระหว่างสวิตช์

4. แสดงผลให้ผู้ใช้ผ่านทางเว็บแอปพลิเคชัน โดยใช้ภาษา PHP และใช้ระบบจัดการฐานข้อมูล MySQL ในการจัดเก็บข้อมูล

5. แสดงเส้นทางของ VLAN ผ่านระบบแผนภาพโครงข่าย (Visualization) ง่ายต่อการเข้าใจ

6. แสดงหรือแจ้งเตือนการจัดการหรือการตั้งค่า VLAN ที่ไม่เหมาะสม เพื่อเป็นข้อมูลสำหรับปรับปรุงการตั้งค่าสวิตช์

ทรัพยากรที่ใช้ในการดำเนินงาน

1. ด้านฮาร์ดแวร์ (Hardware)

1.1 หน่วยประมวลผล: Intel® Xeon® 8 Processor E5440 2.83 GHz

1.2 หน่วยความจำหลัก: (RAM) 4.00 GB DDR2

1.3 หน่วยความจำสำรอง: (Hard Disk) 146 GB

2. ด้านซอฟต์แวร์ (Software)

2.1 ระบบปฏิบัติการ CentOS รุ่น 6.5

2.2 Apache webserver รุ่น 2.2.15

2.3 PHP រ៉ឺង 5.3.3

2.4 Net-SNMP រ៉ឺង 5.5

2.5 MySQL រ៉ឺង 5.5.36

บทที่ 2

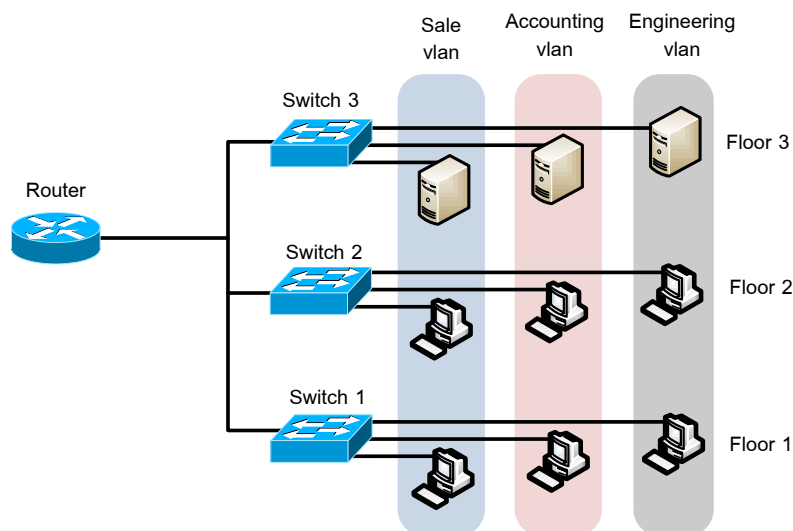
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในการพัฒนาระบบค้นหาโครงสร้าง VLAN ผู้จัดทำงานนิพนธ์ได้ศึกษาและประยุกต์ใช้ทฤษฎีที่เกี่ยวข้อง ดังนี้

ความรู้เบื้องต้นเกี่ยวกับ VLAN

1. ลักษณะการทำงานของ VLAN

เทคโนโลยี VLAN ได้ถูกกำหนดขึ้นภายใต้มาตรฐานของ IEEE และถูกเผยแพร่ตั้งแต่ปีค.ศ. 1998 ซึ่งมีชื่อว่า IEEE 802.1Q เป็นเทคโนโลยีที่ช่วยแก้ปัญหาการบริหารจัดการด้านเครือข่ายขนาดใหญ่ ซึ่งมักมีปัญหาเรื่องการรบกวนจากข้อมูลประเภทบรอดคาสต์และมัลติคาสต์การทำงานของ VLAN เสมือนเป็นการสร้างเขตการบรอดคาสต์ใหม่ขึ้นมา ทำให้เกิดการจัดแบ่งเครือข่ายออกเป็นเขตย่อย ๆ โดยเครื่องคอมพิวเตอร์จะสามารถสื่อสารกันได้เฉพาะเครื่องที่อยู่ใน VLAN เดียวกัน แต่หากต้องการสื่อสารข้าม VLAN ต้องอาศัยอุปกรณ์ระดับเลเยอร์ 3 เช่นเราท์เตอร์ เป็นตัวกลางในการส่งข้อมูล และเครื่องคอมพิวเตอร์จะอยู่ใน VLAN เดียวกันหรือไม่ไม่ได้ขึ้นอยู่กับลักษณะทางกายภาพใด ๆ กล่าวคือเครื่องคอมพิวเตอร์ไม่จำเป็นต้องต่ออยู่กับสวิตช์ตัวเดียวกัน อาจจะเป็นสวิตช์คนละตัวและอยู่คนละสถานที่แต่มีการกำหนดค่า VLAN ในตัวอุปกรณ์สวิตช์ให้อยู่เป็นกลุ่ม VLAN เดียวกันก็จะสามารถสื่อสารกันได้จะเห็นได้ว่าการใช้ VLAN ทำให้เกิดความยืดหยุ่นในการออกแบบและช่วยอำนวยความสะดวกให้แก่ผู้ดูแลระบบเครือข่าย ยกตัวอย่างดังภาพที่ 2-1 หากเราต้องการแบ่ง VLAN ออกตามหน่วยงาน (ต้องการให้พนักงานสังกัดต่างหน่วยงาน สื่อสารกันได้แต่ต้องผ่านเราท์เตอร์เท่านั้น) เช่น แต่ละชั้นมีสวิตช์ประจำชั้นและแต่ละชั้นมีพนักงานของทั้งฝ่ายขาย ฝ่ายบัญชี และฝ่ายวิศวกร เราสามารถตั้งค่าพอร์ตบนสวิตช์ที่อยู่แต่ละชั้นให้เครื่องของพนักงานที่อยู่ฝ่ายเดียวกันอยู่ใน VLAN เดียวกัน แต่เครื่องของพนักงานที่ต่างฝ่ายอยู่ใน VLAN ต่างกัน จะเห็นได้ว่าแม้เครื่องของพนักงานที่อยู่ชั้นเดียวกันไม่จำเป็นต้องอยู่ใน VLAN เดียวกัน ขึ้นอยู่กับนโยบายหรือความต้องการว่าจะให้อยู่ในเครือข่ายย่อยประเภทใด



ภาพที่ 2-1 การใช้งาน VLAN

2. ประเภทของ VLAN

หากเราแบ่ง VLAN ตามลักษณะการใช้งาน จะมีวิธีการกำหนดค่า VLAN ให้แก่อุปกรณ์ สวิตช์อยู่ 3 ประเภท คือ

2.1 การกำหนด VLAN โดยอิงพอร์ตของสวิตช์ (Port based VLAN)

สวิตช์พิจารณาเครื่องผู้ใช้งานว่าเป็นสมาชิก VLAN ใด โดยดูจากค่าที่ถูกตั้งไว้ที่พอร์ต ซึ่งผู้ดูแลระบบจะต้องพิจารณาและตั้งค่าให้แต่ละพอร์ตไว้ก่อน หากเครื่องของผู้ใช้งานสองเครื่อง เชื่อมต่อกับพอร์ต 2 พอร์ตที่ถูกตั้งค่าให้อยู่คนละ VLAN กัน เครื่องทั้ง 2 ก็จะไม่สามารถติดต่อ ถึงกันได้ (แม้ว่าทั้งสองพอร์ตจะอยู่บนสวิตช์ตัวเดียวกัน จะสามารถติดต่อถึงกันได้ต้องกระทำผ่าน อุปกรณ์เราท์เตอร์ในเลเยอร์ที่ 3 เท่านั้น) แต่หากพอร์ตทั้งสองอยู่ใน VLAN เดียวกัน เครื่องทั้งสอง จะอยู่ในเขตการ broadcast เดียวกัน

2.2 การกำหนด VLAN โดยอิงจาก MAC ของผู้ใช้งาน

การกำหนด VLAN ด้วยวิธีนี้เป็นการพิจารณาจากหมายเลข MAC ของเครื่อง ผู้ใช้งานเป็นหลัก เมื่อเครื่องคอมพิวเตอร์เชื่อมต่อกับพอร์ตของสวิตช์ สวิตช์จะตรวจสอบหมายเลข MAC กับฐานข้อมูลกลางที่อยู่บนเครื่องแม่ข่ายเพื่อดูว่าหมายเลข MAC ดังกล่าวควรเป็นสมาชิก ของ VLAN ใด โดยเครื่องแม่ข่ายที่ทำหน้าที่จับคู่หมายเลข MAC กับ VLAN มีชื่อว่า VLAN membership policy serve (VMPS) ผู้ดูแลเครือข่ายต้องทำการจับคู่ MAC กับ VLAN ให้ถูกต้อง ก่อน ซึ่งบางครั้งหากมีเครื่องคอมพิวเตอร์จำนวนมาก งานจับคู่นี้จะเพิ่มภาระให้กับผู้ดูแลเครือข่าย ค่อนข้างมาก

2.3 การกำหนด VLAN โดยอิงจากโพรโทคอล

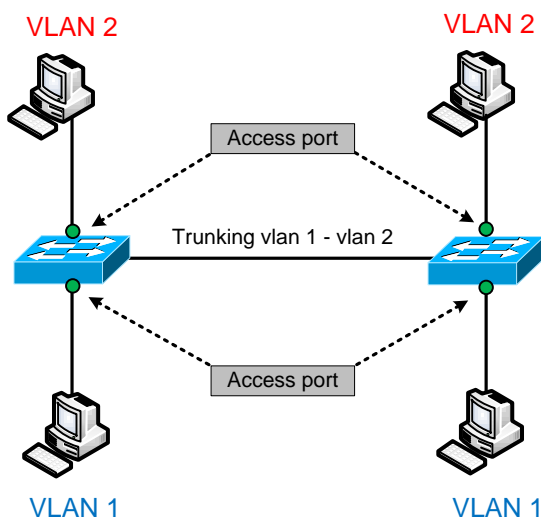
เป็นการแบ่ง VLAN ตามชนิดของโพรโทคอลที่ถูกระบุในส่วนหัวระดับเลเยอร์ที่ 2 ของแพ็กเก็ต วิธีนี้เหมาะกับเครือข่ายที่มีโพรโทคอลที่หลากหลายเช่น IP, IPX, AppleTalk ในทางตรงกันข้าม หากเครือข่ายที่ใช้ไอพีเป็นหลัก วิธีการนี้จะไม่ค่อยนิยมนำมาใช้มากนัก

3. ประเภทพอร์ตของสวิตช์

การกำหนดค่าการทำงานของพอร์ตสวิตช์ โดยทั่วไปจะมีอยู่ 2 ประเภทคือพอร์ตแอกเซส (Access port) และพอร์ตทริงค์ (Trunk port) ซึ่งมีหน้าที่การทำงานต่างกัน ขึ้นอยู่กับอุปกรณ์ที่นำมาเชื่อมต่อหรือวัตถุประสงค์ของผู้ใช้งาน

3.1 พอร์ตแอกเซส

การจะกำหนดให้เครื่องคอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ ที่ต่อกับสวิตช์ว่าจะให้เป็นสมาชิกของ VLAN ใด VLAN หนึ่ง เราจะต้องทำการกำหนดที่พอร์ตของสวิตช์นั้น ๆ ให้เป็นพอร์ตแอกเซส จึงอาจกล่าวได้ว่าข้อมูลที่ส่งผ่านเข้าออกพอร์ตประเภทนี้เป็นข้อมูลของ VLAN เพียง VLAN เดียวเท่านั้น



ภาพที่ 2-2 ตัวอย่างการใช้งานพอร์ตแอกเซส

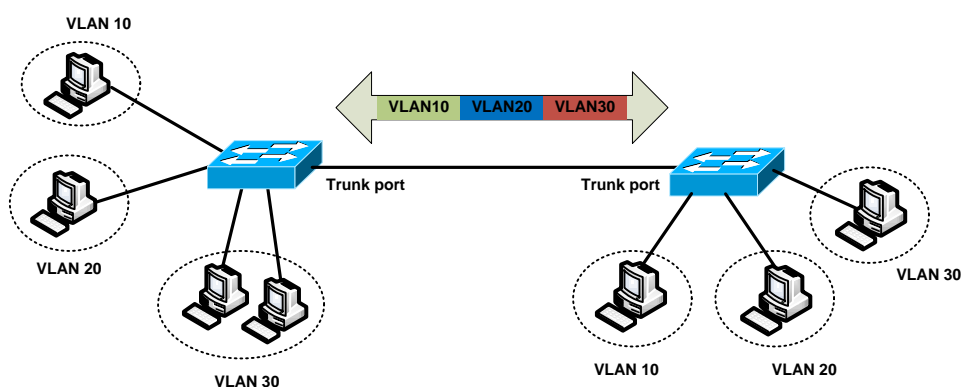
การทำงานและลักษณะของพอร์ตแอกเซสมีดังต่อไปนี้

- พอร์ตแอกเซสหนึ่งพอร์ตจะสัมพันธ์กับ VLAN ใดเพียง VLAN เดียวเท่านั้น
- เนื่องจากพอร์ตแอกเซสจะเป็นสมาชิกของ VLAN ใด VLAN หนึ่งซึ่งอยู่ในเขต

การ broadcast เดียวกัน ทำให้พอร์ตนั้น ๆ ยังได้รับข้อมูลที่เป็นทั้ง broadcast มัลติคาสต์ ซึ่งจะส่งออกไปยังทุก ๆ พอร์ตที่อยู่ใน VLAN เดียวกัน

3.2 พอร์ตทริงค์

เป็นพอร์ตที่มีสมาชิกของ VLAN ได้มากกว่าหนึ่ง VLAN หรือกล่าวอีกอย่างหนึ่งก็คือ การส่งข้อมูลหลาย ๆ VLAN สามารถทำผ่านพอร์ตทริงค์ได้ โดยมีโปรโตคอลทริงค์คอยควบคุมการทำงานและระบุว่า จะทำการติดป้าย (Tag) VLAN ใดออกไปบ้าง ตามการตั้งค่าของสวิตช์ จุดประสงค์ของการมีพอร์ตทริงค์ก็เพื่อรองรับความสามารถในการที่ VLAN หนึ่ง ๆ สามารถขยายออกไปบนพอร์ตสวิตช์หลาย ๆ ตัวได้



ภาพที่ 2-3 การต่อใช้งานพอร์ตแบบทริงค์

ตัวอย่างการต่อใช้งานพอร์ตทริงค์ที่พบได้จากอุปกรณ์เหล่านี้

- การต่อระหว่างสวิตช์
- การต่อระหว่างสวิตช์กับเราเตอร์ที่ทำหน้าที่เชื่อมต่อ VLAN เข้าหากัน
- สวิตช์กับพอร์ตของอุปกรณ์ที่มีความสามารถทำพอร์ตแบบทริงค์ได้ เช่น

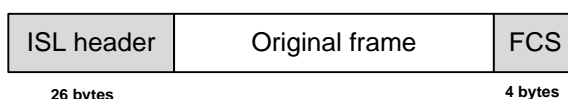
พอร์ตของการ์ดเชื่อมต่อเครือข่าย (Network interface card: NIC) ของเครื่องเครื่องแม่ข่าย

4. รูปแบบเฟรมของ VLAN

เนื่องจากเฟรมที่รับส่งผ่านพอร์ตทริงค์ อาจเป็นเฟรมของ VLAN ใดก็ได้ สวิตช์ จึงจำเป็นต้องใช้เทคนิคเพื่อจำแนก VLAN ของเฟรมที่สวิตช์รับเข้ามา ซึ่งเทคนิคที่ใช้กันมีอยู่ 2 เทคนิคคือ 1) เทคนิคการห่อหุ้ม (Encapsulation) เป็นการห่อหุ้มเฟรมด้วยส่วนหัวที่สร้างขึ้นมาโดยมีหมายเลข VLAN กำกับ และ 2) การแทรกแถบป้ายหมายเลข (Tag) เข้าไปในเฟรม โดยเพิ่มฟิลด์ (Field) ที่ระบุหมายเลข VLAN เข้าไป

4.1 ISL (Inter switch link)

เป็นโพรโทคอลเฉพาะ (Proprietary) ของบริษัทซิสโก้ (Cisco) ซึ่งเป็นการเพิ่มฟิลด์ขนาด 26 ไบต์ที่ประกอบด้วยหมายเลข VLAN ขนาด 15 บิตและฟิลด์ต่าง ๆ เพิ่มเข้าไปข้างหน้าเฟรมอีเทอร์เน็ต ต่อท้ายด้วยฟิลด์ตรวจสอบการผิดของเฟรม (Frame checksequence: FCS) ขนาด 4 ไบต์เข้าไปที่ท้ายเฟรม



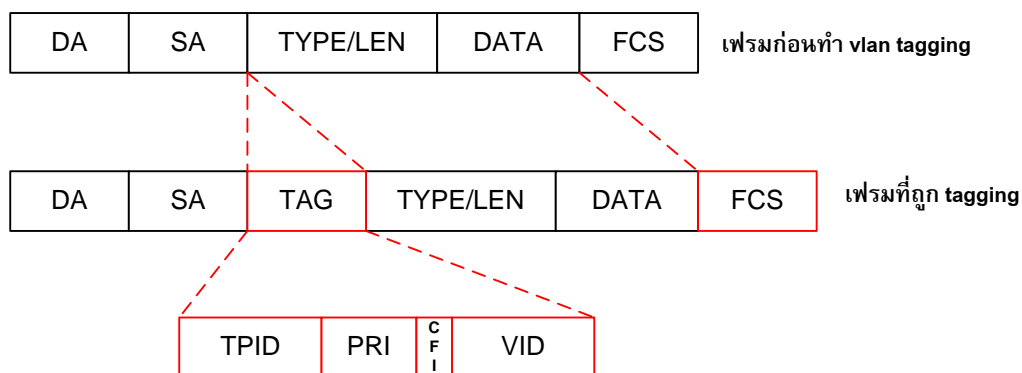
ภาพที่ 2-4 เฟรม VLAN แบบ ISL

เห็นได้ว่าการห่อหุ้มเฟรมข้อมูลเดิมด้วยส่วนหัวและส่วนท้าย ทำให้ได้เป็นเฟรมชุดใหม่ที่มีขนาดเพิ่มขึ้น 30 ไบต์ ส่งผลให้เฟรมอีเทอร์เน็ตมีขนาดตั้งแต่ 94 ไบต์ถึง 1548 ไบต์ (เฟรมอีเทอร์เน็ตปกติมีค่าตั้งแต่ 64 ถึง 1518 ไบต์) จึงอาจเกิดการแบ่งเฟรม (Fragmentation) ขึ้นในระบบ จึงควรพิจารณาขนาดของเฟรมที่เพิ่มขึ้นจะส่งผลถึงบางระบบหรือไม่ เช่น แอปพลิเคชันบางตัวอาจมีปัญหาเมื่อมีการแบ่งเฟรมเกิดขึ้น

เนื่องจาก ISL เป็นโพรโทคอลเฉพาะของบริษัทซิสโก้ทำให้ไม่สามารถใช้โพรโทคอลนี้ร่วมกับสวิตช์ของผู้ผลิตรายอื่นได้และรองรับ VLAN ได้เพียง 1000 VLAN แม้ภายหลังได้มีการปรับปรุงรุ่นใหม่ออกมา แต่ไม่ค่อยได้รับความนิยมมากนัก นอกจากนี้ยังมีคุณสมบัติการทำงานที่แตกต่างกัน เช่นรองรับโพรโทคอลในระดับเลเยอร์ 2 แบบอื่น นอกจากเครือข่ายแบบอีเทอร์เน็ต เช่นเครือข่ายแบบวงแหวนโทเค็น (Token ring), เครือข่ายแบบ ATM (Asynchronous transfer mode)

4.2 802.1Q

โพรโทคอลมาตรฐานที่กำหนดโดย IEEE ซึ่งใช้วิธีเพิ่มฟิลด์ขนาด 4 ไบต์ประกอบด้วยหมายเลข VLAN ขนาด 12 บิตและข้อมูลต่าง ๆ แทรกเข้าไปในเฟรมอีเทอร์เน็ตโดยจะแทรกหลังจากฟิลด์ SA (Source address) ดังแสดงในภาพที่ 2-5



ภาพที่ 2-5 ภาพแบบเฟรมของ IEEE 802.1Q

| | | | | | | | | | |
|--------------|----|----|------|----------|-----|-----|------|--------------|-----|
| # bits | 48 | 48 | 16 | 3 | 1 | 12 | 16 | 368 to 12000 | 32 |
| Frame fields | DA | SA | TPID | Priority | CFI | VID | TYPE | DATA | FCS |

ภาพที่ 2-6 ขนาดของฟิลด์ต่าง ๆ ในอีเทอร์เน็ตเฟรม

ตารางที่ 2-1 รายชื่อฟิลด์และความหมาย

| ชื่อฟิลด์ | รายละเอียด |
|--------------------------------|---|
| DA-Destination address | ที่อยู่ปลายทางของผู้รับ |
| SA-Source address | ที่อยู่ต้นทางของผู้ส่ง |
| TPID-Tag protocol identifier | ระบุโปรโตคอล มีขนาด 16 บิต ปกติมีค่าเป็น 0x8100 สำหรับเฟรม 802.1Q |
| Priority | ลำดับความสำคัญของเฟรม มี 8 ระดับ (0-7) |
| CFI-Canonical format indicator | ใช้สำหรับเครือข่ายแบบวงแหวนโทเค็น |
| VID-VLAN identifier | ขนาด 12 บิต สำหรับระบุหมายเลข VLAN มีค่าตั้งแต่ 0-4095 |
| TYPE | ระบุประเภทเฟรม |
| DATA | ข้อมูล มีขนาดตั้งแต่ 46 ไบต์ถึง 1500 ไบต์ |
| FCS-Frame check sequence | ตรวจสอบการผิดของเฟรม |

เนื่องจากเฟรมข้อมูลเดิมถูกเปลี่ยนแปลง จึงต้องมีกระบวนการคำนวณค่าตรวจสอบการผิดของเฟรมอีกครั้ง และปรับให้ถูกต้อง ทำให้ขนาดของเฟรมสูงสุดอยู่ที่ 1522 ไบต์ ข้อดีของ 802.1Q ที่เป็นโพรโทคอลมาตรฐานของ IEEE ก็คือมันช่วยให้อุปกรณ์สวิตช์ต่างยี่ห้อทำงานร่วมกันได้ นอกจากนี้ยังมีคุณสมบัติเพิ่มเติมดังนี้

- รองรับการทำงานของอีเทอร์เน็ตและเครือข่ายแบบวงแหวนโทเค็น
- รองรับ VLAN ได้สูงสุด 4096 VLAN
- รองรับการทำเฟรมอีเทอร์เน็ตที่ไม่ได้ถูกแท็กเข้ามา (Native VLAN)
- สามารถรองรับการควบคุมคุณภาพการให้บริการ (Quality of service, QoS)

5. จำนวน VLAN

จำนวนขนาดหรือหมายเลข VLAN ที่สามารถใช้งานได้ จะขึ้นอยู่กับการเลือกรูปแบบเฟรม เช่น หากตั้งค่าเป็นแบบ ISL หมายเลข VLAN ที่ใช้งานได้ตั้งแต่ 1 ถึง 1024 แต่หากใช้การตั้งค่าเฟรมแบบ IEEE 802.1Q จะมีช่วงตั้งแต่ 1 ถึง 4094 นอกจากนี้ยังอาจขึ้นอยู่กับความสามารถของสวิตช์ หรือตัวซอฟต์แวร์ที่ใช้ในการจัดการว่ารองรับหรือไม่

ตัวอย่างการกำหนดช่วง VLAN ของสวิตช์ซิสโก้ มีการแบ่ง VLAN ออกเป็น 2 ช่วง คือ ช่วงที่ใช้งานปกติ (Normal range) และช่วงส่วนขยาย (Extended range) ดังแสดงในตารางที่ 2-2

ตารางที่ 2-2 อธิบายขอบเขตการใช้แต่ละช่วงของ VLAN

| VLAN | ประเภท | อธิบายการใช้งาน |
|-----------|----------|--|
| 0, 4095 | สงวนไว้ | ใช้ในภายในสวิตช์เอง ไม่แสดงให้เห็น |
| 1 | ปกติ | เป็นค่าเริ่มต้นจากโรงงาน ใช้งานได้แต่ไม่สามารถแก้ไขหรือลบออกได้ |
| 2-1001 | ปกติ | สามารถสร้างสำหรับใช้งานและลบได้ |
| 1002-1005 | ปกติ | VLAN สำหรับโครงข่าย FDDI, Token Ring (เฉพาะสวิตช์ซิสโก้) ไม่สามารถลบได้ |
| 1006-4094 | ส่วนขยาย | ใช้งานได้ แต่ขึ้นอยู่กับแพลตฟอร์มของสวิตช์รุ่นนั้น ๆ หรือระบบจัดการของสวิตช์ว่ารองรับหรือไม่ |

6. ประโยชน์ของ VLAN

6.1 ควบคุมการเกิด broadcast

เมื่อจำนวนอุปกรณ์ในเครือข่ายเพิ่มมากขึ้น อัตราการเกิด broadcast ที่อยู่ในขอบเขตเดียวกันก็จะยิ่งเพิ่มขึ้นตามไปด้วย อัตราของ broadcast เป็นสิ่งที่มีนัยสำคัญต่อประสิทธิภาพการสื่อสารในเครือข่าย กล่าวคืออุปกรณ์ทุกตัวที่อยู่ในขอบเขตเดียวกันเมื่อได้รับ broadcast ที่เฟรมจะต้องหยุดการทำงานและฟังว่าเป็นข้อมูลที่ส่งมาเป็นของตนเองหรือไม่ หากมีอัตรา broadcast เกิดขึ้นสูงมาก ก็เท่ากับเป็นการขัดจังหวะการทำงานของอุปกรณ์ในเครือข่าย ทำให้ต้องใช้ CPU ในการประมวลผลข้อมูลที่สูงขึ้นและส่งผลกระทบต่อประสิทธิภาพการทำงานล่าช้าลง

6.2 เพิ่มความปลอดภัย

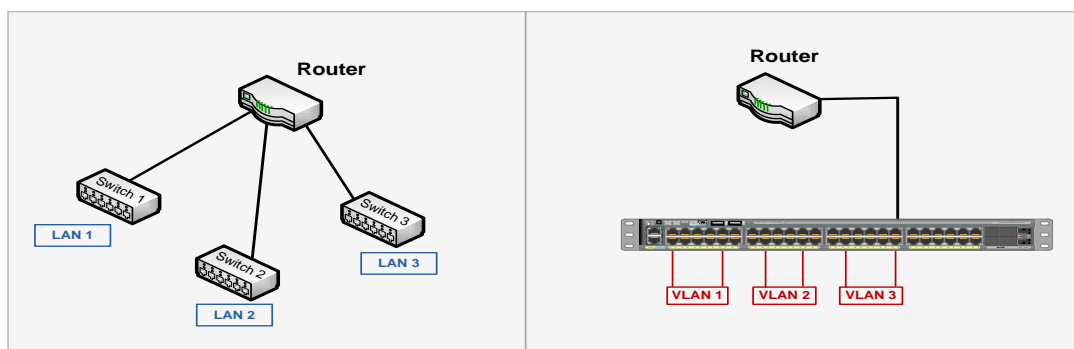
บ่อยครั้งที่หลาย ๆ องค์กรต้องการจำกัดการเข้าถึงทรัพยากรที่เชื่อมต่อกับเครือข่าย ผู้ดูแลเครือข่ายจึงจำเป็นต้องอาศัยการทำงานของ VLAN ที่สามารถแบ่งเครือข่ายออกเป็นกลุ่มย่อย ๆ เพื่ออนุญาตให้เครื่องคอมพิวเตอร์ในเครือข่ายท้องถิ่นเดียวกันเท่านั้นที่เข้าถึงทรัพยากรได้ แต่หากเครื่องคอมพิวเตอร์นอกเครือข่ายท้องถิ่นต้องการที่จะใช้ทรัพยากร จะต้องทำผ่านอุปกรณ์ระดับเลเยอร์ 3 เท่านั้น (ซึ่งจะมีมาตรการรักษาความปลอดภัยอย่างอื่นต่อไป)

6.3 ช่วยลดต้นทุนด้านอุปกรณ์

VLAN ช่วยประหยัดการใช้อุปกรณ์ในเครือข่ายและสะดวกต่อการบำรุงรักษา ตัวอย่างในภาพที่ 2-7 ระบบเครือข่ายท้องถิ่นแบบเดิม หากต้องการแบ่งวง LAN ออกเป็น 3 วง ต้องใช้สวิตช์ 3 ตัวแยกกัน ส่วนที่เราเตอร์ก็ต้องใช้พอร์ตถึง 3 พอร์ตเพื่อต่อไปยังสวิตช์แต่ละตัว หากเราเปลี่ยนมาใช้สวิตช์ที่รองรับ VLAN จะทำให้สามารถแบ่งวง LAN แยกตามพอร์ตของสวิตช์ แม้จะอยู่ในสวิตช์ตัวเดียวกันและที่เราเตอร์จะใช้เพียงพอร์ตเดียวในการเชื่อมต่อมาที่สวิตช์ ช่วยประหยัดอุปกรณ์และง่ายต่อการบำรุงรักษา เช่น ระบบไฟฟ้า การเดินสายเชื่อมต่อ

6.4 สะดวกต่อการบริหารเครือข่าย

VLAN ช่วยให้การจัดการโครงสร้างของระบบเครือข่ายสะดวก ยืดหยุ่น เช่น หากต้องการเพิ่มจำนวนผู้ใช้งานหรือเพิ่มกลุ่มผู้ใช้ เพียงเพิ่มสวิตช์ตัวใหม่ในเครือข่าย ด้วยคุณสมบัติของพอร์ตแบบที่รองรับ VLAN มากกว่าหนึ่ง VLAN จึงสามารถเลือกใช้ VLAN ตามความต้องการ ขึ้นอยู่กับการจัดสรรกลุ่มผู้ใช้งานตามนโยบายหรือการออกแบบที่วางไว้



ภาพที่ 2-7 การใช้ VLAN ช่วยให้ประหยัดอุปกรณ์

โพรโทคอล SNMP

โพรโทคอล Simple Network Management Protocol (SNMP) เป็นโพรโทคอลที่ใช้ในการบริหารจัดการเครือข่าย ทำงานง่ายไม่ซับซ้อนผู้ดูแลเครือข่ายสามารถเปลี่ยนค่าการทำงานของอุปกรณ์ที่รองรับ SNMP ตัวอย่างเช่นสามารถสั่งให้ SNMP เปิด-ปิดพอร์ตของเราเตอร์ หรือตรวจสอบความเร็วของพอร์ตที่กำลังทำงานอยู่ และสามารถติดตามการทำงานของอุปกรณ์เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น เช่น ที่ตัวอุปกรณ์มีอุณหภูมิที่สูงขึ้น

นอกจากผู้ดูแลเครือข่ายจะสามารถใช้ SNMP จัดการกับอุปกรณ์เครือข่าย เช่น เราเตอร์ หรือสวิตช์แล้วยังสามารถใช้งาน SNMP ได้กับระบบปฏิบัติการยูนิกซ์ ระบบปฏิบัติการวินโดวส์ เครื่องพิมพ์ หรืออุปกรณ์ต่าง ๆ ที่มีโพรโทคอล SNMP ทำงานอยู่และอนุญาตให้เข้าถึงข้อมูลได้

1. รุ่นของ SNMP

โพรโทคอล SNMP อยู่ในกลุ่มโพรโทคอลที่ได้รับการพัฒนาโดย IETF แบ่งออกเป็น 3 รุ่นดังนี้

1.1 SNMP รุ่นที่ 1 (SNMPv1) เป็นรุ่นแรกของโพรโทคอล SNMP ถูกกำหนดใน RFC 1157 และถูกเปลี่ยนสถานะเป็นมาตรฐานเก่า ซึ่ง SNMPv1 มีข้อเสียในเรื่องความปลอดภัยของชื่อกลุ่ม (Community string) เนื่องจากการสื่อสารระหว่างตัวจัดการและตัวแทนจะต้องอยู่ภายใต้ชื่อกลุ่มเดียวกัน และทั้งตัวจัดการและตัวแทนสามารถอยู่ในชื่อกลุ่มได้มากกว่าหนึ่งชื่อ โดยชื่อกลุ่มจะใช้ชุดของตัวอักษรเสมือนเป็นรหัสผ่านในการพิสูจน์ตัวตน แต่ในการสื่อสารไม่มีการเข้ารหัสข้อมูลให้เป็นความลับ ทำให้เกิดความเสี่ยงหากผู้ไม่หวังดีทราบชื่อกลุ่มก็สามารถเข้าถึงข้อมูลและจัดการกับตัวอุปกรณ์ได้ ซึ่งชื่อกลุ่มมีรูปแบบในการเข้าถึงข้อมูลอยู่ 3 แบบคือ อ่านอย่างเดียว (Read-only) อ่านและเขียน (Read-write) และแตรป (Trap) ถึงแม้ว่า SNMPv1 จะถูกให้เป็นมาตรฐานเก่าแล้วก็ตาม แต่ผู้ผลิตอุปกรณ์หลายรายก็ยังนำไปใช้เป็นตัวหลักเพื่อรองรับการทำงานของ SNMP

1.2 SNMP รุ่นที่ 2 (SNMPv2) เป็นรุ่นที่ยังใช้ชื่อกลุ่มเป็นหลักในการกำหนดสิทธิ์การเข้าถึงข้อมูล บางครั้งอาจเรียกรุ่นนี้ว่า SNMPv2c โดยมีคำสั่งเพิ่มขึ้นอีก 2 คำสั่งคือ getbulk สามารถดึงข้อมูลเป็นกลุ่มด้วยคำสั่งเพียงชุดเดียว ซึ่งต่างจากคำสั่ง get ที่ต้องส่งคำสั่งเพื่อดึงข้อมูลได้ทีละครั้งและคำสั่ง inform ใช้สำหรับติดต่อระหว่างตัวจัดการและตัวแทน มาตรฐานนี้ถูกกำหนดใน RFC 3416, RFC 3417 และ RFC 3418

1.3 SNMP รุ่นที่ 3 (SNMPv3) เป็นรุ่นล่าสุดมีจุดประสงค์หลักในเรื่องการรักษาความปลอดภัย เช่น มีการพิสูจน์ตัวตน (Authentication) การรักษาข้อมูล (Privacy) การเข้ารหัสข้อมูล (Encryption) และควบคุมการเข้าถึงข้อมูล (Access control) โดยเผยแพร่ออกมาในปี ค.ศ. 2002 ตาม RFC 3410 ถึง RFC 3418 และ RFC 2576 แต่เนื่องจากความยุ่งยากในการใช้งาน SNMPv3 จึงไม่ได้นำมาใช้ในงานทั่วไป ยกเว้นเครือข่ายที่ต้องการความปลอดภัยในระดับสูง

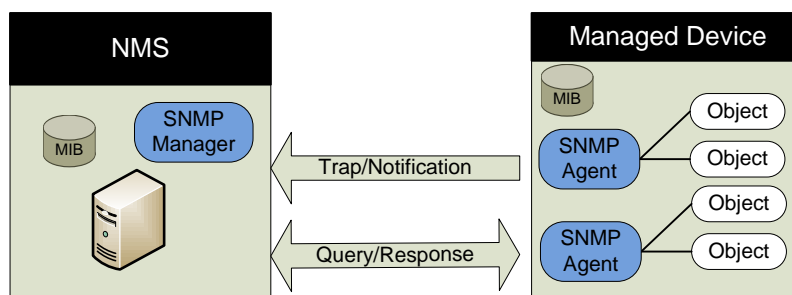
2. ตัวจัดการและตัวแทน (Manager and Agent)

โพรโทคอล SNMP ประกอบด้วยองค์ประกอบ 3 ส่วนคือ ตัวจัดการ (Manager), ตัวแทน (Agent), ข้อมูลเพื่อการจัดการหรือ MIB (Management information base) ดังแสดงในภาพที่ 2-8 และ 2-9

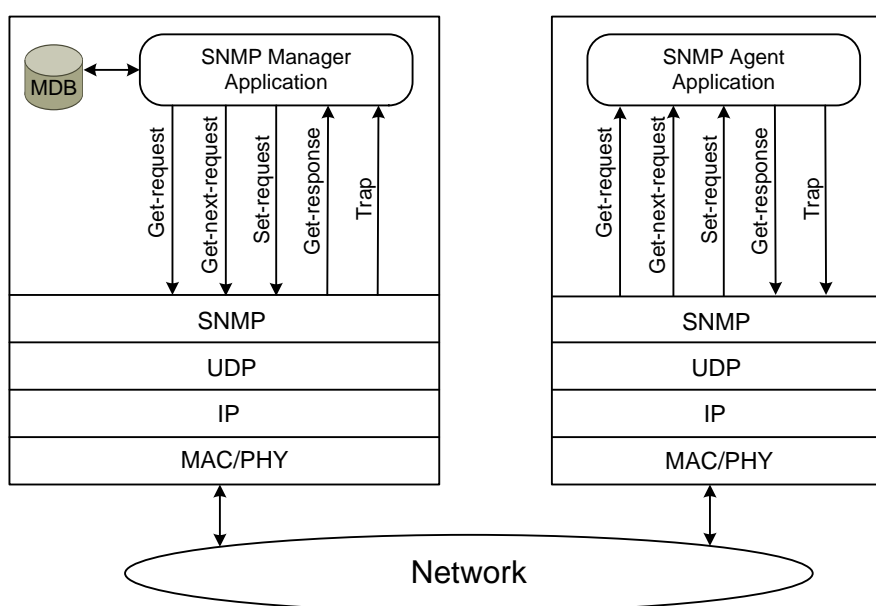
ตัวจัดการ โดยทั่วไปคือเครื่องแม่ข่ายที่ติดตั้งโปรแกรมประยุกต์สำหรับติดตามการทำงานของอุปกรณ์ บางครั้งอาจเรียกว่าระบบบริหารจัดการเครือข่าย (Network Management System: NMS) และมีฐานข้อมูล MDB (Management database) สำหรับจัดเก็บข้อมูลของ MIB ตัวจัดการมีหน้าที่ร้องขอ (Request) สืบรวจ (Polling) หรือรับข้อมูลประเภทเทรป (Trap) ที่ส่งจากตัวแทนโดยอัตโนมัติ

ตัวแทนคือ โปรแกรมขนาดเล็กที่ทำงานฝังตัวอยู่ในอุปกรณ์ ซึ่งอาจมีการทำงานแยกออกจากระบบหลักหรือทำงานร่วมกัน เช่น ในระบบปฏิบัติการเครือข่ายของซิสโก้ (Internetwork operating system: IOS) ตัวแทนจะส่งข้อมูลให้กับตัวจัดการ เมื่อมันถูกร้องขอหรือเมื่อพบเหตุผิดปกติ

การสืบรวจ คือการร้องขอข้อมูลจากตัวแทน (ทำงานในเร้าเตอร์หรือสวิตช์) ข้อมูลเหล่านี้สามารถใช้ประเมินสภาพการทำงานของตัวอุปกรณ์ ส่วนเทรปคือวิธีที่ตัวแทนใช้ส่งสัญญาณแจ้งเตือนมายังตัวจัดการว่ามีเหตุการณ์ผิดปกติเกิดขึ้น เทรปสามารถถูกส่งเมื่อใดก็ได้โดยไม่ต้องมีการร้องขอจากตัวจัดการและตัวจัดการอาจมีการตอบสนองต่อเทรปตามความสามารถของโปรแกรมประยุกต์ เช่น แสดงเป็นแถบสีต่าง ๆ บนหน้าจอ หรือส่งเสียงแจ้งเตือน



ภาพที่ 2-8 ความสัมพันธ์ระหว่างตัวจัดการและตัวแทน



ภาพที่ 2-9 โครงสร้างการทำงานของโปรโตคอล SNMPv1

3. โครงสร้างข้อมูลเพื่อการจัดการ (Structure of Management Information: SMI)

SMI เป็นการกำหนดโครงสร้างและรายละเอียดของอ็อบเจกต์ (Object) เช่น หลักของการตั้งชื่อ ประเภทของข้อมูล เพื่อเป็นวิธีการให้ตัวแทนและตัวจัดการเข้าถึงอ็อบเจกต์ได้อย่างถูกต้อง โดย SMIv1 ได้ระบุในเอกสาร RFC 1155 ต่อมา มีประเภทของข้อมูลเพิ่มมากขึ้นจึงมีมาตรฐาน SMIv2 ระบุใน RFC 2578

ในการกำหนดโครงสร้างของอ็อบเจกต์ มีองค์ประกอบหลักด้วยกัน 3 ส่วนคือ

- ชื่อ (Name) หรือตัวระบุอ็อบเจกต์ (Object identifier: OID) เป็นสิ่งที่ใช้ในการอ้างถึง แต่ละอ็อบเจกต์ในระบบต้องมีชื่อไม่ซ้ำกัน ชื่ออาจเป็นได้ทั้งตัวเลขหรือคำที่มีความหมาย ขึ้นอยู่กับ

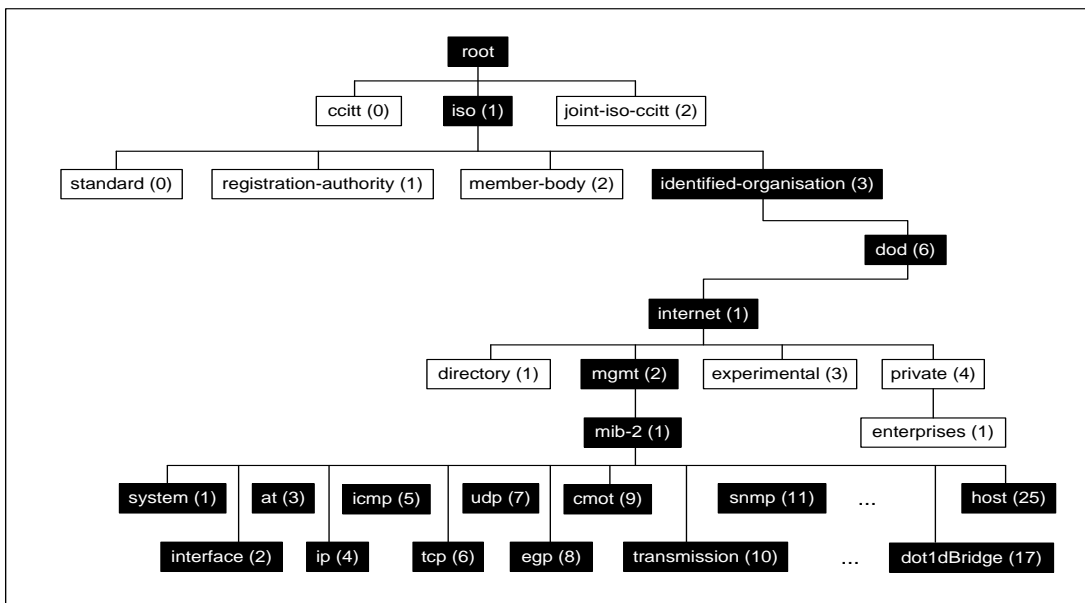
ความสะดวกของการใช้งานเช่น การแทนด้วยข้อความอาจยาวเกินไป หากต้องการอ้างถึงอ็อบเจกต์ *sysName* ด้วยตัวอักษรจะอยู่ในรูปแบบ iso.org.dod.internet.mgmt.mib-2.system.sysName แต่หากอ้างถึงแบบตัวเลขจะเขียนได้เป็น 1.3.6.1.2.1.1.5

- ประเภทและไวยากรณ์ (Type and Syntax) ใช้กำหนดประเภทข้อมูลในแต่ละออบเจกต์ เพื่อเป็นข้อตกลงในการรับ-ส่งข้อมูลระหว่างตัวจัดการและตัวแทน โดยใช้หลักการของภาษาลัทธิกษณ์ Abstract Syntax Notation One (ASN.1) ข้อดีของ ASN.1 คือเป็นมาตรฐานอิสระ ไม่ขึ้นอยู่กับภาษาของโปรแกรมหรือระบบปฏิบัติการที่กำลังทำงานอยู่ เช่น เครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการวินโดวส์ 2000 สามารถติดต่อกับเครื่องที่ใช้ระบบปฏิบัติการของซันได้โดยไม่ต้องห่วงเรื่องรูปแบบของคำสั่ง

- การเข้ารหัส (Encoding) เป็นวิธีการเข้ารหัสเพื่อเป็นการรับประกันความถูกต้องว่าชนิดข้อมูลที่ได้รับนั้นเป็นชนิดเดียวกัน จึงให้วิธีที่เรียกว่า Basic encoding rule (BER) เป็นการกำหนดถึงวิธีการเข้ารหัสและถอดรหัสเมื่อมีการส่งข้อมูลผ่านไปรษณีย์เช่น อีเทอร์เน็ต

4. การตั้งชื่อ OID

ชื่อใช้เป็นตัวระบุการเข้าถึงอ็อบเจกต์ มีโครงสร้างการจัดเก็บในลักษณะแบบต้นไม้ (Tree) โดยชื่ออ็อบเจกต์จะถูกกำกับด้วยตัวเลขและเรียงลำดับกัน ตั้งแต่รากของต้นไม้จนถึงโหนดที่ต้องการเข้าถึง โดยใช้จุดเป็นตัวคั่นระหว่างโหนด โดยสามารถเขียนให้อยู่ในรูปแบบที่มีเฉพาะตัวเลขหรือมีชื่อรวมอยู่ด้วยก็ได้ เช่น การอ้างถึงกลุ่มอ็อบเจกต์ในต้นไม้ย่อย internet สามารถเขียนได้ในแบบ iso(1).org(3).dod(6).internet(1) หรือ 1.3.6.1 การที่เขียนได้สองแบบก็เพื่ออำนวยความสะดวกสำหรับผู้ใช้งาน ส่วนใหญ่การอ้างถึงแบบตัวเลขจะใช้สื่อสารกันระหว่างตัวจัดการและตัวแทน คล้ายกับระบบชื่อโดเมนที่แปลงไอพีให้เป็นชื่อเพื่ออำนวยความสะดวก เห็นได้ว่าการจัดเก็บโครงสร้างของ MIB ที่อยู่ในรูปแบบต้นไม้โดยใช้เลขจำนวนเต็มบวกแทนโหนดต่าง ๆ ไม่มีข้อจำกัดในการในการเข้าถึงเมื่อข้อมูลมีขนาดใหญ่และมีระดับความลึกของต้นไม้หลายระดับแสดงให้เห็นว่าสามารถรองรับการตั้งชื่อได้อย่างไม่จำกัด ดังแสดงในภาพที่ 2-10



ภาพที่ 2-10 ตัวอย่างลำดับโครงสร้างต้นไม้ของ MIB

5. การอธิบาย OID

ประเภทข้อมูลของ OID แต่ละตัวถูกกำหนดตามหลักไวยากรณ์ของ ASN.1 ซึ่งระบุไว้ใน SMIV1 หากเราทราบประเภทข้อมูลของ OID ที่จัดเก็บก็จะทำให้สามารถจัดการกับข้อมูลเหล่านั้นได้อย่างถูกต้อง SMIV1 มีประเภทข้อมูลหลายชนิด ตามตารางที่ 2-3

ตารางที่ 2-3 ประเภทข้อมูลที่ประกาศใน SMIV1

| ประเภทข้อมูล | รายละเอียด |
|-------------------|--|
| INTEGER | ตัวเลขจำนวนเต็มขนาด 32 บิต แต่จะไม่ใช่ค่า 0 |
| OCTET STRING | ข้อความหรืออักขระ ตั้งแต่ 0 ไบต์ ส่วนใหญ่ใช้กับชุดตัวอักษรหรือแทนเลข MAC |
| Counter | ตัวเลขขนาด 32 บิตมีค่าตั้งแต่ 0 ถึง $2^{32}-1$ (4,294,967,295) เมื่อถึงค่าสูงสุดแล้วจะวนกลับมาเริ่มต้นที่ 0 ใหม่ |
| OBJECT IDENTIFIER | ชุดตัวเลขที่ค้นด้วยจุด ใช้ทำการอ้างอิงถึงวัตถุ เช่น 1.3.6.1.4.1.9 ใช้แทนค่า <i>OIDprivate enterprise</i> ของซิสโก้ |

ตารางที่ 2-3 (ต่อ)

| ประเภทข้อมูล | รายละเอียด |
|----------------|---|
| NULL | SNMP ยังไม่มีการนำมาใช้ |
| SEQUENCE | บอกว่ามีข้อมูลเป็นรายการหรือมีข้อมูลประเภทอื่นอีก |
| SEQUENCE OF | บอกว่าวัตถุชิ้นนั้นถูกสร้างขึ้นจาก <i>SEQUENCE</i> ของ ASN.1 |
| IpAddress | แทน ไอพีรุ่น 4 ขนาด 32 บิต |
| NetworkAddress | ที่อยู่ของชุด โพรโทคอล เช่นชุด โพรโทคอล TCP/IP ใช้เป็นแบบ หมายเลขไอพี |
| Gauge | เลขจำนวนเต็มขนาด 32 บิตตั้งแต่ 0 ถึง $2^{32}-1$ ต่างจาก <i>Counter</i> ก็คือ สามารถเพิ่มหรือลดค่าลงได้ เช่นความเร็วที่พอร์ตของเราเตอร์ |
| TimeTicks | เลขจำนวนเต็ม 32 บิตตั้งแต่ 0 ถึง $2^{32}-1$ ใช้วัดเวลาในหน่วยของ 1/100 วินาที เช่นค่าระยะเวลาที่อุปกรณ์ทำงานมาจนถึงปัจจุบัน |
| Opaque | ให้ข้อมูลชนิดอื่นของ ASN.1 เข้ารหัสเป็น OCTET STRING |

ตัวอย่างไวยากรณ์ที่อยู่ในไฟล์ MIB ซึ่งเขียนตามหลักของภาษาสัญลักษณ์ ASN.1 จะแสดงโครงสร้างและการนิยามอ็อบเจกต์ประเภทข้อมูล การอธิบายรายละเอียดอ็อบเจกต์นั้น ๆ ดังตัวอย่างไฟล์ RFC1213-MIB ที่แสดงบางส่วนของไฟล์ ให้เห็นถึงการนิยามโครงสร้างของ OID (เครื่องหมาย "--" แสดงถึงหมายเหตุไม่นำมาประมวลผล , เครื่องหมาย "::=" หมายถึงตัวดำเนินการนิยาม)

```
-- This mib was extracted from RFC 1213
-- The following changes have been applied:
-- The enumerations unknown(4) and dormant(5) have been added to
-- ifOperStatus to reflect a change to the ifTable introduced in
-- RFC 1573
--
-- The SYNTAX of ifType has been changed to IANAifType, to reflect
-- the change to the ifTable introduced in RFC1573.

RFC1213-MIB DEFINITIONS ::= BEGIN
IMPORTS
    mgmt, NetworkAddress, IpAddress, Counter, Gauge, TimeTicks
    FROM RFC1155-SMI
OBJECT-TYPE
    FROM RFC-1212
TEXTUAL-CONVENTION
    FROM SNMPv2-TC
IANAifType
    FROM IANAifType-MIB
```



```

-- This MIB module uses the extended OBJECT-TYPE macro as
-- defined in [14];
-- MIB-II (same prefix as MIB-I)
    mib-2 OBJECT IDENTIFIER ::= { mgmt 1 }
-- textual conventions
    DisplayString ::=
        OCTET STRING
-- This data type is used to model textual information taken
-- from the NVT ASCII character set.  By convention, objects
-- with this syntax are declared as having
--
--
-- SIZE (0..255)
    PhysAddress ::=
        OCTET STRING
-- This data type is used to model media addresses.  For many
-- types of media, this will be in a binary representation.
-- For example, an ethernet address would be represented as
-- a string of 6 octets.

-- groups in MIB-II

    system      OBJECT IDENTIFIER ::= { mib-2 1 }
    interfaces  OBJECT IDENTIFIER ::= { mib-2 2 }
    at          OBJECT IDENTIFIER ::= { mib-2 3 }
    ip          OBJECT IDENTIFIER ::= { mib-2 4 }
    icmp       OBJECT IDENTIFIER ::= { mib-2 5 }
    tcp        OBJECT IDENTIFIER ::= { mib-2 6 }
    udp        OBJECT IDENTIFIER ::= { mib-2 7 }
    egg        OBJECT IDENTIFIER ::= { mib-2 8 }
    -- historical (some say hysterical)
    cmot       OBJECT IDENTIFIER ::= { mib-2 9 }
    transmission OBJECT IDENTIFIER ::= { mib-2 10 }
    snmp       OBJECT IDENTIFIER ::= { mib-2 11 }

-- the System group
-- Implementation of the System group is mandatory for all
-- systems.  If an agent is not configured to have a value
-- for any of these variables, a string of length 0 is returned.

sysDescr OBJECT-TYPE
    SYNTAX  DisplayString (SIZE (0..255))
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "A textual description of the entity.This value
        should include the full name and version identification
        of the system's hardware type,software operating-system,
        and networking software.It is mandatory that this only
        contain printable ASCII characters."
    ::= { system 1 }

sysObjectID OBJECT-TYPE
    SYNTAX  OBJECT IDENTIFIER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "The vendor's authoritative identification of the network
        management subsystem contained in the entity.This value
        is allocated within the SMI enterprises subtree(1.3.6.1
        .4.1)and provides an easy and unambiguous means for
        determining `what kind of box' is being managed.For
        example,if vendor `Flintstones, Inc.' was assigned the
        subtree 1.3.6.1.4.1.4242, it could assign the identifier
        1.3.6.1.4.1.4242.1.1 to its `Fred Router'."

```

```

 ::= { system 2 }

sysUpTime OBJECT-TYPE
    SYNTAX TimeTicks
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        "The time (in hundredths of a second) since the network
        management portion of the system was last re-
        initialized."
 ::= { system 3 }

sysContact OBJECT-TYPE
    SYNTAX DisplayString (SIZE (0..255))
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "The textual identification of the contact person for
        this managed node, together with information on how to
        contact this person."
 ::= { system 4 }

sysName OBJECT-TYPE
    SYNTAX DisplayString (SIZE (0..255))
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "An administratively-assigned name for this managed node.
        By convention, this is the node's fully-qualified domain
        name."
 ::= { system 5 }

sysLocation OBJECT-TYPE
    SYNTAX DisplayString (SIZE (0..255))
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "The physical location of this node(e.g., `telephone
        closet, 3rd floor')."
 ::= { system 6 }

```

จากไฟล์ RFC1213-MIB ที่บรรทัดแรกเป็นการนิยามชื่อของ MIB ไฟล์นั้น ในส่วนของการนำเข้า (IMPORTS) เป็นการอ้างถึงไฟล์อื่นที่เกี่ยวข้องกับการเรียกใช้ประเภทข้อมูล ในตัวอย่างนี้คือ RFC1155-SMI ซึ่งถือเป็นตัวนิยามประเภทข้อมูล (SMIV1) เช่น mgmt, Counter, Gauge ดังคำอธิบายในตารางที่ 2-3 นอกจากนี้ยังมีการนำเข้า RFC อื่น เช่น RFC 1212

การที่ OID ที่อยู่ในไฟล์นี้อ้างถึงโหนดที่อยู่ก่อนหน้า (ด้วยการนำเข้า) ทำให้กลุ่มอ็อบเจกต์ ของ mib-2(1) ที่อยู่ภายใต้ mgmt (iso(1).org(3).dod(6).internet(1).mgmt(2)) สามารถอ้างถึงได้ด้วยชุดตัวเลข 1.3.6.1.2.1 ในทำนองเดียวกัน กลุ่มของ system ซึ่งอยู่ถัดจาก mib-2 จึงถูกนิยามเป็น { mib-2 1 } หรือ 1.3.6.1.2.1.1

จากไฟล์ตัวอย่างที่แสดงข้างต้น ทำให้เราทราบถึงรูปแบบของการนิยามวัตถุที่อยู่ภายในไฟล์ MIB ซึ่งมีรูปแบบดังนี้

<ชื่อ> OBJECT-TYPE

SYNTAX <ชนิดของข้อมูล>

ACCESS <สิทธิ์ในการเข้าถึง>

STATUS <สถานะของวัตถุ>

DESCRIPTION

“อธิบายรายละเอียดของวัตถุนั้น ๆ”

:= { <ค่าที่ไม่ซ้ำกันระบบที่นิยาม OID > }

นอกจากชนิดข้อมูลแล้ว ในรูปแบบการอธิบายโครงสร้างวัตถุยังมีส่วนของการกำหนดสิทธิ์และสถานภาพที่ต้องมีอ็อบเจกต์เหล่านั้น ซึ่งมีความหมายดังตารางที่ 2-4 และตารางที่ 2-5

ตารางที่ 2-4 สิทธิ์ในการเข้าถึงข้อมูล (Access)

| สิทธิ์การเข้าถึงข้อมูล | คำอธิบาย |
|------------------------|---|
| Read-only | อ็อบเจกต์สามารถอ่านได้แต่เขียนไม่ได้ |
| Read-write | อ็อบเจกต์สามารถอ่านและเขียนได้ |
| Write-only | อ็อบเจกต์สามารถเขียนได้แต่อ่านไม่ได้ |
| Not-accessible | อ็อบเจกต์ที่ไม่สามารถอ่านและเขียนได้เช่นข้อมูลที่เก็บในรูปแบบของตาราง |

จากตารางที่ 2-4 เป็นการอธิบายถึงสิทธิ์หรือระดับของความสามารถในการเข้าถึงข้อมูลของอ็อบเจกต์ เนื่องจากค่าการทำงานบางอย่างที่อยู่ภายในตัวอุปกรณ์ไม่สามารถเขียนค่าลงไปได้แต่สามารถอ่านค่าได้อย่างเดียว เช่นค่า *sysUpTime* ที่แสดงระยะเวลาตั้งแต่อุปกรณ์นั้นเริ่มต้นทำงาน

ตารางที่ 2-5 ความหมายของสถานภาพ

| สถานภาพ | คำอธิบาย |
|------------|---|
| Mandatory | อ็อบเจกต์นี้จำเป็นต้องมี |
| Optional | อ็อบเจกต์นี้จะมีหรือไม่มีก็ได้ |
| Obsolete | อ็อบเจกต์นี้จะถูกเลิกใช้ในอนาคต |
| Deprecated | อ็อบเจกต์นี้ควรมีแต่อาจถูกยกเลิกเมื่อมีเวอร์ชันใหม่ |

จากตารางที่ 2-5 อธิบายสถานภาพของอ็อบเจกต์ ซึ่งแสดงถึงความจำเป็นต้องบรรจุอ็อบเจกต์เหล่านั้น เมื่อมีการพัฒนาไฟล์ MIB ขึ้นมา หรือกล่าวได้ว่าเป็นค่าพื้นฐานที่ควรมีในอุปกรณ์ทุกตัวที่ทำงานรองรับกับ SNMP

6. ตัวอย่างค่า OID

ค่า OID ที่ใช้งานทั่วไป ซึ่งกำหนดไว้ใน MIB-II ที่เป็นไฟล์อ้างอิงหลักของ SNMP อุปกรณ์ทุกยี่ห้อจะต้องมีไฟล์นี้เป็นพื้นฐาน ในหัวข้อนี้จึงแสดงตัวอย่างกลุ่มของ OID ดังกล่าวที่เรียกใช้งานอยู่บ่อย ๆ ตามโครงสร้างของ MIB ดังต่อไปนี้

ตารางที่ 2-6 OID ในกลุ่มของ system

| Object Descriptor | OID | คำอธิบาย |
|-------------------|-----------------|---|
| sysDescr | 1.3.6.1.2.1.1.1 | รายละเอียดของอุปกรณ์ |
| sysObjectID | 1.3.6.1.2.1.1.2 | OID ของอุปกรณ์ |
| sysUpTime | 1.3.6.1.2.1.1.3 | ระยะเวลาของระบบตั้งแต่เริ่มทำงานจนถึงปัจจุบัน โดยมีหน่วยเป็น 1/100 วินาที |
| sysContact | 1.3.6.1.2.1.1.4 | รายละเอียดการติดต่อผู้ดูแลระบบ |
| sysName | 1.3.6.1.2.1.1.5 | ระบุชื่ออุปกรณ์ |
| sysLocation | 1.3.6.1.2.1.1.6 | สถานที่ตั้งอุปกรณ์ |

จากตารางที่ 2-6 เป็นรายชื่อ OID ภายใต้ system ซึ่งประกอบด้วยโหนดย่อยจำนวน 6 โหนด ตั้งแต่ 1 ถึง 6 ซึ่งแต่ละโหนดมีความหมายและหน้าที่ตามตาราง

ตารางที่ 2-7 OID ในกลุ่มของ interface

| Object Descriptor | OID | คำอธิบาย |
|-------------------|----------------------|---|
| ifNumber | 1.3.6.1.2.1.2.1 | จำนวนพอร์ตทั้งหมดในอุปกรณ์ |
| ifTable | 1.3.6.1.2.1.2.2 | ตารางแสดงรายละเอียดของพอร์ต |
| ifEntry | 1.3.6.1.2.1.2.2.1 | การเข้าถึงวัตถุในตาราง |
| ifIndex | 1.3.6.1.2.1.2.2.1.1 | หมายเลขที่ไม่ซ้ำกันของแต่ละพอร์ตสำหรับอ้างอิง |
| ifDescr | 1.3.6.1.2.1.2.2.1.2 | ชื่อหรือรายละเอียดของพอร์ต |
| ifType | 1.3.6.1.2.1.2.2.1.3 | ชนิดของพอร์ต |
| ifMtu | 1.3.6.1.2.1.2.2.1.4 | ขนาดของ MTU (Maximum Transfer Unit) |
| ifSpeed | 1.3.6.1.2.1.2.2.1.5 | ความเร็วของพอร์ต |
| ifPhysAddress | 1.3.6.1.2.1.2.2.1.6 | หมายเลข MAC ของพอร์ต |
| ifAdminStatus | 1.3.6.1.2.1.2.2.1.7 | สถานะของการเปิดใช้งานพอร์ต |
| ifOperStatus | 1.3.6.1.2.1.2.2.1.8 | สถานะของการทำงานปัจจุบันของพอร์ต |
| ifLastChange | 1.3.6.1.2.1.2.2.1.9 | เวลาที่สถานะของพอร์ตเปลี่ยนแปลงล่าสุด |
| ifInOctets | 1.3.6.1.2.1.2.2.1.10 | จำนวนข้อมูลเข้าทั้งหมด |
| ifInUcastPkts | 1.3.6.1.2.1.2.2.1.11 | จำนวนข้อมูลที่เข้ามาเป็นแบบ Unicast |
| ifInNUcastPkts | 1.3.6.1.2.1.2.2.1.12 | จำนวนข้อมูลที่เข้ามาไม่ใช่แบบ Unicast |
| ifInDiscards | 1.3.6.1.2.1.2.2.1.13 | จำนวนข้อมูลที่เข้ามาแต่ถูกทิ้งไป |
| ifInErrors | 1.3.6.1.2.1.2.2.1.14 | จำนวนข้อมูลที่เข้ามาแต่ผิดพลาด |
| ifInUnknownProtos | 1.3.6.1.2.1.2.2.1.15 | จำนวนข้อมูลที่เข้ามาแต่ไม่ทราบโปรโตคอล |
| ifOutOctets | 1.3.6.1.2.1.2.2.1.16 | จำนวนข้อมูลส่งออกทั้งหมด |
| ifOutUcastPkts | 1.3.6.1.2.1.2.2.1.17 | จำนวนข้อมูลที่ส่งออกเป็นแบบ Unicast |
| ifOutNUcastPkts | 1.3.6.1.2.1.2.2.1.18 | จำนวนข้อมูลที่ส่งออกไม่ใช่แบบ Unicast |
| ifOutDiscards | 1.3.6.1.2.1.2.2.1.19 | จำนวนข้อมูลที่ส่งออกแต่ถูกทิ้งไป |
| ifOutErrors | 1.3.6.1.2.1.2.2.1.20 | จำนวนข้อมูลที่ส่งออกแต่ผิดพลาด |

7. วิธีการค้นคืนค่า MIB

การเข้าถึงหรือโต้ตอบกับอุปกรณ์ที่สนับสนุนโพรโทคอล SNMP ต้องมีการติดตั้งซอฟต์แวร์จัดการเครือข่ายประเภท NMS (Network management station) ซึ่งมีทั้งซอฟต์แวร์เชิงพาณิชย์เช่น HP's OpenView, OiDViEW, iReasoning MIB Browser หรือซอฟต์แวร์ที่เปิดให้ใช้งานฟรี เช่น Net-SNMP ซึ่งในงานนิพนธ์นี้ขอยกตัวอย่างการใช้งานซอฟต์แวร์ตัวนี้ เนื่องจากเป็นตัวเดียวกับที่ถูกเรียกใช้งานจากภาษา PHP

7.1 การใช้เครื่องมือ Net-SNMP

Net-SNMP เป็นซอฟต์แวร์โอเพนซอร์สที่ถูกพัฒนาและถูกนำไปใช้งานร่วมกับซอฟต์แวร์ประเภท NMS เช่น Cacti, Nagios, OpenSNMP และเป็นส่วนขยาย (Extension) ให้ภาษาอื่น เช่น ภาษา PHP นอกจากนี้ซอฟต์แวร์ Net-SNMP สามารถทำงานได้ทั้งในระบบปฏิบัติการลินุกซ์และวินโดวส์ สามารถดาวน์โหลดได้จาก <http://www.net-snmp.org>

ตัวอย่างในระบบปฏิบัติการลินุกซ์ตระกูล CentOS สามารถติดตั้ง Net-SNMP ด้วยคำสั่ง `$yum install net-snmp net-snmp-utils` เมื่อติดตั้งเรียบร้อยแล้ว Net-SNMP จะทำงานในโปรเซสชื่อ `snmpd` ซึ่งจัดเก็บอยู่ในไฟล์คอนฟิก `/etc/snmp/snmpd.conf`

เกือบทุกคำสั่งของ Net-SNMP รูปแบบคำสั่งจะมีโครงสร้างที่เหมือนกัน มีการใช้ options ร่วมกันและมีไวยากรณ์ที่เหมือนกัน ตัวอย่างเช่น รูปแบบการใช้คำสั่ง `snmpget` มีดังนี้

```
snmpget options hostname objectID..
```

คำสั่งจะถูกตามด้วยลำดับของ options , hostname คือชื่อหรือหมายเลขไอพีของอุปกรณ์ที่ต้องการติดต่อ และตามด้วย objectID ที่อาจมีตั้งแต่หนึ่งค่าหรือมากกว่า คำสั่ง `snmpset` จะเป็นเพียงคำสั่งเดียวที่มีรูปแบบแตกต่าง เนื่องจากการเปลี่ยนค่าของวัตถุ และต้องระบุชนิดของข้อมูลที่ต้องการเปลี่ยน ซึ่งรูปแบบมีดังนี้

```
snmpset options hostname objectID type value..
```

ในตารางที่ 2-8 เป็นการสรุป option ที่ใช้งานทั่วไปกับคำสั่งของ Net-SNMP

ตารางที่ 2-8 option ที่ใช้บ่อยของคำสั่ง net-snmp

| Option | คำอธิบาย |
|--------|--|
| -On | แสดงค่า OID เป็นตัวเลข (เช่น .1.3.6.1.2.1.1.3.0) |
| -Of | แสดง OID ข้อความแบบเต็มรูป (เช่น .iso.org.dod...) |
| -Os | แสดง OID แบบสั้นตั้งแต่ชื่ออ็อบเจกต์ (เช่น ifName.10005 = STRING: Fa1/0/5) |

ตารางที่ 2-8 (ต่อ)

| Option | คำอธิบาย |
|--------|---|
| -OS | แสดงเฉพาะส่วนสุดท้ายของ OID (เช่น sysUpTime.0) |
| -v | ระบุรุ่นของ SNMP ที่ใช้มีค่าเป็น 1, 2 และ 2c |
| -h | แสดงข้อความช่วยเหลือ (help) |
| -c | ระบุค่า community string สำหรับ SNMPv1 หรือ SNMPv2c |

7.2 คำสั่ง snmpget

เป็นคำสั่งที่ใช้สอบถามด้วยตัวดำเนินการ get ของโพรโทคอล SNMP ผลลัพธ์ที่ได้มีเพียงค่าเดียวตาม objectID ที่ระบุในคำสั่ง ตัวอย่างการสอบถามสถานที่ติดตั้งของสวิตช์

```
$snmpget -v2c -c public10.236.0.230 .1.3.6.1.2.1.1.6.0
SNMPv2-MIB::sysLocation.0 = STRING: Chonburi,Telecom Fl.2
```

จากตัวอย่างเป็นการสอบถามค่า System location ซึ่งมีค่า OID .1.3.6.1.2.1.1.6.0 จากสวิตช์หมายเลขไอพี 10.236.0.230 ที่มีการตั้งค่า community string คือ public ผลลัพธ์ที่อุปกรณ์ตอบกลับมาจะอยู่ในรูปแบบสตริง เห็นได้ว่าเมื่อเราต้องการสอบถามข้อมูล ซึ่งรู้ค่า OID หรือชื่ออ็อบเจกต์ก็สามารถใช้ชื่อนั้นแทนการใช้ OID ผลลัพธ์ที่ได้ก็มีค่าเหมือนกันตัวอย่าง

```
$snmpget -v2c -c public10.236.0.230sysLocation.0
SNMPv2-MIB::sysLocation.0 = STRING: Chonburi,Telecom Fl.2
```

7.3 คำสั่ง snmpwalk

คำสั่ง snmpwalk เป็นการทำงานโดยใช้ตัวดำเนินการ getNext ของโพรโทคอล SNMP ซึ่งแตกต่างจากคำสั่ง get ตรงที่ค่าอ็อบเจกต์ที่สอบถามนั้นจะเป็นค่าของอ็อบเจกต์ย่อยตัวต่อไป จากอ็อบเจกต์ที่สอบถามไป เช่น ต้องการสอบถามอ็อบเจกต์ตัวถัดไปจาก sysDescr.0 นอกจากอุปกรณ์จะตอบกลับมาด้วยค่าของ sysDescr แล้ว ยังมีค่าในฟิลด์ OID เป็น sysObjectID ซึ่งคืออ็อบเจกต์ที่อยู่ถัดไป คำสั่งนี้จะมีประโยชน์มากเมื่อใช้กับอ็อบเจกต์ที่อยู่ในรูปของตาราง เนื่องจากเราไม่รู้จำนวนแถวที่แน่นอนของตารางตัวอย่างการใช้คำสั่ง snmpwalk เช่น

```

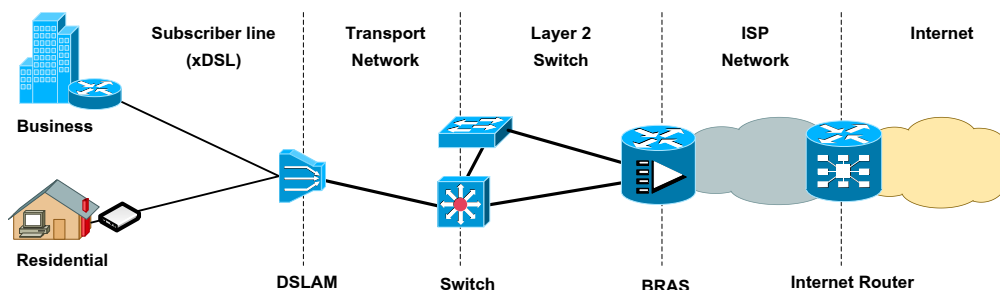
$snmpwalk -v2c -c public 10.236.0.230 .1.3.6.1.2.1.1
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software, C3560
Software (C3560-IPBASE-M), Version 12.2(35)SE5, RELEASE
SOFTWARE (fc1)Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 19-Jul-07 18:15 by nachen
SNMPv2-MIB::sysObjectID.0= OID:SNMPv2
SMI::enterprises.9.1.615
SNMPv2-MIB::sysUpTimeInstance = Timeticks:(2097823994)242
days, 19:17:19.94
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING:omc_noc_04
SNMPv2-MIB::sysLocation.0 = STRING:Chonburi,Telecom Fl.2
SNMPv2-MIB::sysServices.0 = INTEGER:6
SNMPv2-MIB::sysORLastChange.0 = Timeticks:(0)0:00:00.00

```

จากตัวอย่างเป็นการสอบถามข้อมูลทั้งหมดที่อยู่ภายใต้กลุ่มต้นไม้ย่อย system หากเขียนในแบบเต็มคือ iso(1).org(3).dod(6).internet(1).mgmt(2).mib2(1).system(1) ข้อมูลจะถูกถามต่อไปเรื่อย ๆ จนกระทั่งสิ้นสุดที่โหนดสุดท้ายในต้นไม้ย่อยนั้น

การส่งข้อมูลแบบ DSL (Digital subscriber line)

ในหัวข้อนี้เป็นการยกตัวอย่างการให้บริการอินเทอร์เน็ตแบบ DSL ของผู้ให้บริการอินเทอร์เน็ต ว่ามีองค์ประกอบและการทำงานอย่างไร VLAN เข้าามีบทบาทในส่วนใดบ้างของระบบ ซึ่งมีรายละเอียดในแต่ละส่วนดังต่อไปนี้



ภาพที่ 2-11 องค์ประกอบการให้บริการอินเทอร์เน็ต

1. Internet router

เป็นเราท์เตอร์ที่เชื่อมต่อระหว่างผู้ให้บริการอินเทอร์เน็ตด้วยกัน มักจะอยู่ที่ขอบของเครือข่ายผู้ให้บริการแต่ละราย

2. B-RAS (Broadband remote access server)

เป็นอุปกรณ์ทำหน้าที่รวบรวมการจราจรจากผู้ให้บริการและยกเลิกเซสชัน (Session termination) รวมไปถึงทำหน้าที่จัดการตรวจสอบสิทธิ์ผู้ใช้งาน รับรองความถูกต้องและบันทึกการเข้าใช้งานหรือ AAA (Authentication, Authorization, Accounting) นอกจากนี้ยังทำหน้าที่แจกจ่ายหมายเลขไอพีให้แก่ผู้ให้บริการเพื่อใช้ติดต่อในอินเทอร์เน็ต

ฝั่งผู้ให้บริการจะต้องสร้างการเชื่อมต่อจากเราท์เตอร์ของตนเอง ผ่าน DSLAM, Aggregate switch จนมาถึงตัว B-RAS ซึ่งเป็นการเชื่อมต่อบนเลเยอร์ 1 และ 2 ส่วนการทำงานในระดับเลเยอร์ 3 จะเกิดขึ้นได้ก็ต่อเมื่อมีการพิสูจน์สิทธิ์เป็นที่เรียบร้อยแล้ว ดังนั้น B-RAS จะต้องประมวลผล VLAN ที่ส่งมาจาก DSLAM ผ่านสวิตช์เลเยอร์ 2 ซึ่งมีการแบ่งกลุ่มลูกค้ำตาม VLAN

3. Aggregate switch

คือกลุ่มของสวิตช์เลเยอร์ 2 ทำหน้าที่กระจายโหนดให้ครอบคลุมพื้นที่ให้บริการมากที่สุดเพื่อรวบรวมทราฟฟิกจาก ให้บริการสื่อสารข้อมูลในรูปแบบของเฟรมอีเทอร์เน็ต โดยใช้ VLAN แยกประเภทหรือกลุ่มลูกค้ำ

4. DSLAM (Digital subscriber line access multiplexer)

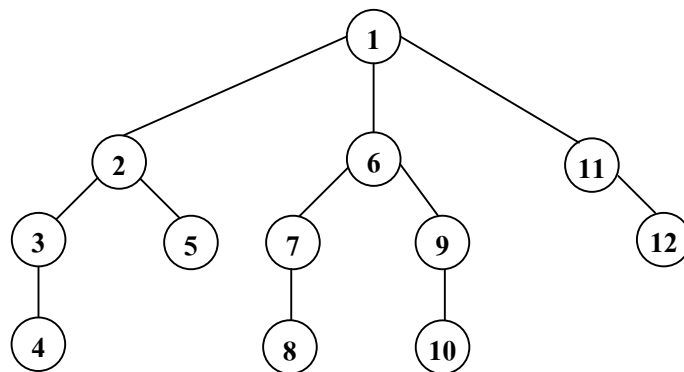
คืออุปกรณ์ที่ทำหน้าที่รวมสัญญาณ โทรศัพท์และอินเทอร์เน็ตผ่านไปในคู่สายโทรศัพท์ที่เป็นทองแดง เนื่องจากในอดีตเราไม่ได้ใช้ประโยชน์ของสายทองแดงได้อย่างเต็มที่ ซึ่งในความจริงแล้วสายทองแดงสามารถรองรับแถบความถี่หรือแบนด์วิดท์ได้หลายเมกะเฮิรตซ์ แต่ใช้ในการสื่อสารโทรศัพท์เพียงแค่ 4 กิโลเฮิรตซ์เท่านั้น เมื่อนำมาแบ่งช่องความถี่ให้มากขึ้น ทำให้ Dslam สามารถจัดส่งข้อมูลพร้อมด้วยสัญญาณเสียงหรือคุยโทรศัพท์ที่ได้พร้อม ๆ กัน

ใน DSLAM แต่ละตัวสามารถสร้าง VLAN ได้มากกว่าหนึ่ง VLAN ต่อหนึ่งพอร์ต DSL เพื่อให้ลูกค้ำใช้บริการที่หลากหลายได้เช่น ใช้ VLAN 10 สำหรับบริการอินเทอร์เน็ต, VLAN 20 สำหรับบริการ VoIP และใช้ VLAN 30 สำหรับดูเนื้อหาแบบ Streaming

ขั้นตอนวิธีค้นหาตามแนวลึก

การเชื่อมต่อในเครือข่ายที่มีลักษณะเป็นโครงสร้างต้นไม้โดยมีรูทบริดจ์เป็นโหนด เริ่มต้นหากเราต้องการตรวจสอบการเชื่อมต่อของ VLAN ว่ามีความสมบูรณ์หรือไม่ เราสามารถใช้ขั้นตอนวิธีค้นหาตามแนวลึก (Depth-first search algorithm หรือ DFS) ช่วยในการค้นหาคำตอบ

การค้นหาคตามแนวลึกคือการค้นหาโหนดจากรูปของโครงสร้างต้นไม้โดยพิจารณาในแนวลึกก่อน ขั้นตอนวิธีค้นหาคตามแนวลึกอาจใช้ตัวบ่งทักสถานะของโหนดแสดงถึงการเยี่ยมโหนด (Node-visit status) ที่ได้ท่องผ่านมาแล้ว โดยเริ่มต้นจากโหนดราก (Root node) ที่อยู่บนสุดแล้วท่องผ่านลงมาให้ลึกที่สุดจนไม่สามารถไปต่อ จากนั้นให้ย้อนขึ้นมาที่จุดสูงสุดของกิ่งเดียวกันที่มีกิ่งแยกและยังไม่ได้ท่องผ่าน ให้เริ่มท่องผ่านลงมาจนถึงโหนดลึกสุดอีก ทำเช่นนี้สลับไปเรื่อยจนพบโหนดที่ต้องการหาหรือสำรวจครบทุกโหนดแล้วตามภาพที่ 2-12 การค้นหาคตามแนวลึกจะมีลำดับการเดินตามโหนดดังตัวเลขที่กำกับไว้ในแต่ละโหนดเช่น เริ่มต้นที่โหนด 1 ลงไปโหนด 2 จากโหนด 2 จะมีโหนด 3 และ 5 ให้เก็บโหนด 5 ไว้และท่องผ่านโหนด 3 และ 4 ก่อนจากนั้นจึงย้อนขึ้นมาที่โหนด 5



ภาพที่ 2-12 ลำดับการเดินทางของการค้นหาคตามแนวลึกบนโครงสร้างต้นไม้

การทำงานของขั้นตอนวิธีค้นหาคตามแนวลึก

การท่องเข้าไปในกราฟแบบDFS จะใช้กองซ้อน (Stack) มาช่วยในการจัดการเริ่มจากโหนดเริ่มต้น ให้นำโหนดที่อยู่ติดกับโหนดที่กำลังสำรวจอยู่ (ที่ยังไม่ได้ท่องผ่าน) มาเก็บไว้ในกองซ้อนเมื่อสำรวจโหนดนั้นแล้วให้ดึงตัวบนสุดของโหนดออกมาสำรวจ ให้นำโหนดข้างเคียงทั้งหมดที่ยังไม่ได้สำรวจมาต่อท้ายกองซ้อนแล้วดึงตัวบนสุดออกมาสำรวจ ทำเช่นนี้เรื่อย ๆ จนกระทั่งพบโหนดที่ต้องการหาหรือสำรวจครบทุกโหนด สามารถเขียนเป็นรหัสเทียมได้ดังนี้

DFS(G, v) (v is vertex where the search starts)

Stack $S := \{\}$; (start with an empty stack)

for each vertex u , set $visited[u] := false$;

push S, v ;

while (S is not empty) **do**

$u := pop S$;

if (not $visited[u]$) **then**

$visited[u] := true$;

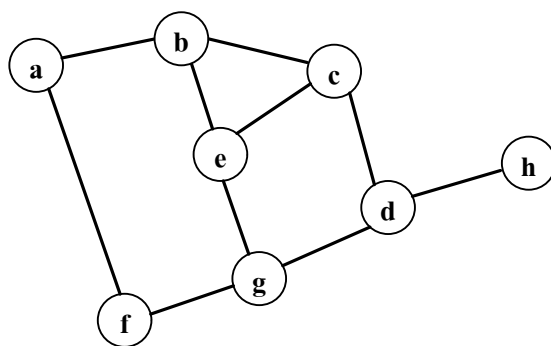
for each unvisited neighbour w of u

 push S, w ;

end for each

end if

end while



(a) กราฟไม่มีทิศทาง

| โหนดที่ท่อง | Stack |
|-------------|-------------|
| a | a |
| b | a b |
| c | a b c |
| d | a b c d |
| g | a b c d g |
| e | a b c d g e |
| (นำออก) | a b c d g |
| f | a b c d g f |
| (นำออก) | a b c d g |
| (นำออก) | a b c d |
| h | a b c d h |
| (นำออก) | a b c d |
| (นำออก) | a b c |
| (นำออก) | a b |
| (นำออก) | a |
| (นำออก) | ว่าง |

(b) การท่องผ่านโหนดตามแนวลึก

ภาพที่ 2-13 ตัวอย่างการท่องไปในกราฟแบบ DFS

จากโค้ดรหัสเทียมที่แสดงหากนำไปท่องในกราฟตามภาพที่ 2-13 (a) ตัวอย่างกราฟไม่มีทิศทาง สามารถแสดงลำดับการทำงานการเก็บข้อมูลลงในกองซ้อนตามขั้นตอนดังภาพที่ 2-13 (b) ลำดับที่ได้จากการท่องเข้าไปในกราฟคือ a b c d g e f และ h

การสร้างกราฟ

การแสดงผลหรือผลลัพธ์ต่าง ๆ โดยเฉพาะข้อมูลที่มีความซับซ้อน ข้อมูลมีปริมาณสูง ให้อยู่ในรูปแบบของภาพ จะช่วยให้แก่ผู้เข้าใจได้รวดเร็วและมีส่วนช่วยสำหรับนำไปใช้ในการสนับสนุนการตัดสินใจอย่างมีประสิทธิภาพ ดังเช่นการใช้ทฤษฎีกราฟมาอธิบายการเชื่อมต่อของอุปกรณ์ในเครือข่าย สามารถสะท้อนให้เห็นถึงปัญหาได้อย่างรวดเร็ว

ในโครงการนี้เราใช้กราฟแสดงการเชื่อมต่อของอุปกรณ์ในเครือข่ายของบริษัทไอทีในพื้นที่จังหวัดชลบุรีและใช้ขั้นตอนวิธีประมวลผลกราฟเครือข่ายเพื่อบริหารจัดการ VLAN

Arbor เป็นไลบรารีซึ่งพัฒนาด้วยจาวาสคริปต์และทำงานร่วมกับเจคิววี (jQuery) ใช้สำหรับสร้างกราฟและแสดงรูปภาพ เหมาะกับระบบที่พัฒนาด้วยเทคโนโลยีเว็บ สามารถศึกษาข้อมูลและดาวน์โหลดที่ <http://arborjs.org>

การติดตั้งและนำมาใช้งานให้นำไฟล์ arbor.js วางไว้ในไฟล์ที่ต้องการเรียกใช้ภายใต้แท็กของจาวาสคริปต์ พร้อมกับมีการเรียกใช้ jquery ด้วย เช่น

```
<script src="path/to/jquery.min.js"></script>
```

```
<script src="path/to/arbor.js"></script>
```

การเรียกใช้งาน Arbor จะต้องมีการกำหนดค่าเริ่มต้น โดยการเรียกคอนสตรักเตอร์ (Constructor) ชื่อ ParticleSystem() พร้อมด้วยค่าพารามิเตอร์ดังคำสั่งต่อไปนี้

```
arbor.ParticleSystem(repulsion, stiffness, friction, gravity, fps, dt, precision)
```

ตารางที่ 2-9 ค่าพารามิเตอร์ต่าง ๆ ที่ต้องกำหนดก่อนการเรียกใช้ arbor

| พารามิเตอร์ | ค่าโดยปริยาย | อธิบาย |
|-------------|--------------|---|
| repulsion | 1000 | แรงผลักกันหรือแรงดึงดูดในแต่ละโหนด |
| stiffness | 600 | ความคงตัวไม่ยืดหยุ่นของ edage |
| friction | 0.5 | การเสียดสีกันระหว่างโหนด |
| gravity | false | แรงดึงดูดเข้าหาจุดกำเนิด |
| fps | 55 | แสดงผลเฟรมต่อวินาที |
| dt | 0.02 | ระดับของช่วงเวลาทีน้อย ๆ เพิ่มขึ้น |
| precision | 0.6 | ความแม่นยำเทียบกับความเร็วในการคำนวณ (ถ้าค่าเป็น 0 จะแสดงผลเร็วแต่ภาพจะกระตุก หากเท่ากับ 1 จะแสดงผลนุ่มนวลแต่ใช้หน่วยประมวลผลสูง) |

หากไม่มีการใส่อาร์กิวเมนต์ไว้ พารามิเตอร์จะถูกแทนค่าโดยปริยาย ดังตารางที่ 2-9 อธิบายความหมายของพารามิเตอร์แต่ละตัว และค่าโดยปริยาย เราสามารถเรียกใช้ ParticleSystem ได้หลายรูปแบบ ซึ่งจะให้ผลเหมือนกัน เช่น

```
arbor.ParticleSystem()
arbor.ParticleSystem(600)
arbor.ParticleSystem(600,1000, .5,55, .02,false)
arbor.ParticleSystem({friction:.5,stiffness:600,repulsion:1000})
```

เมื่อ ParticleSystem ถูกเรียกใช้ไปแล้ว หากต้องการเปลี่ยนแปลงพารามิเตอร์บ้างตัว เราสามารถส่งค่าอ็อบเจกต์เหล่านั้นผ่านทางเมธอด parameters ได้ เช่น

```
var sys = arbor.ParticleSystem()
sys.parameters({gravity:true,dt:0.005})
```

1. คำสั่งที่ใช้สร้างกราฟ

กราฟเป็น โครงสร้างที่ประกอบด้วยจุดยอด (Vertex) และเส้นเชื่อม (Edge) ซึ่งเชื่อมต่อกัน จุดยอดเหล่านั้น เมธอดที่ใช้ในการสร้างกราฟของ arbor มี 2 เมธอดคือ

1. addNode (name, data) เมื่อ

name คือชื่อตัวแปรที่ใช้อ้างอิงในโปรแกรม

data คือข้อมูลรายละเอียดหรือชื่อของโหนด

2. addEdge (source, target, data) เมื่อ

source และ target คือตัวแปรที่ถูกอ้างอิงถึงการสร้างโหนด

data คือข้อมูลที่ให้รายละเอียดของเส้นเชื่อมนั้น

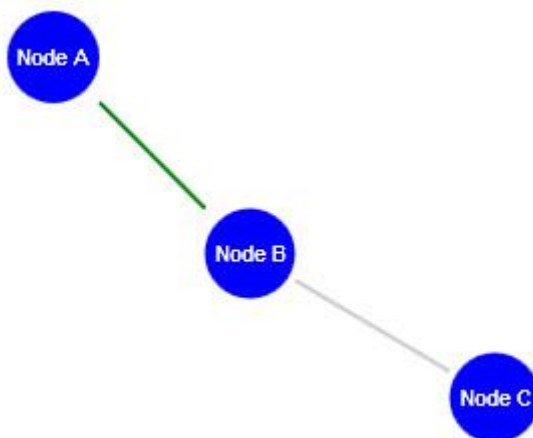
```

1: <body>
2: <canvas id="view" width="400" height="300"></canvas>
3: </body>
4: <script type="text/javascript">
5:   var sys = arbor.ParticleSystem();
6:   sys.renderer = Renderer("#view");
7:   sys.addNode('node1',{
8:     'color':'blue','shape':'dot','label':'Node A'
9:   });
10:  sys.addNode('node2',{
11:    'color':'blue','shape':'dot','label':'Node B'
12:  });
13: sys.addNode('node3',{
14:   'color':'blue','shape':'dot','label':'Node C'
15:  });
16:  sys.addEdge('node1','node2',{
17:    'length':1.25,'weight':2,'color':'green'
18:  });
19: sys.addEdge('node2','node3',{ 'weight':2});
20: </script>

```

ตัวอย่างการสร้างกราฟด้วย arbor เมื่อใช้ร่วมกับภาษา HTML จากตัวอย่างโค้ดในบรรทัดที่ 2 แท็ก canvas กำหนดให้กราฟแสดงผลภายในพื้นที่นี้ ตามความกว้าง ความสูงที่กำหนด บรรทัดที่ 5 arbor ถูกเรียกใช้โดยสร้างตัวแปรอ็อบเจกต์ sys และสร้างโหนดด้วยเมธอด addNode ขึ้นมา 3 โหนด ภายใต้ชื่อตัวแปร node1, node2 และ node3 โดยเราสามารถกำหนดรูปร่าง สี และใส่ชื่อของโหนด ได้ภายใต้เครื่องหมาย {} ในบรรทัดที่ 16 และ 19 เป็นการสร้างเส้นเชื่อมระหว่างโหนดด้วยเมธอด addEdge () ซึ่งรายละเอียดในการสร้างเส้นเชื่อม เราสามารถระบุค่าของน้ำหนักของเส้น ความยาว และสี ได้เช่นกัน

ตัวอย่างจากโค้ดด้านบน เมื่อเรียกด้วยเว็บเบราว์เซอร์แล้วจะได้ผลดังภาพที่ 2-14



ภาพที่ 2-14 ตัวอย่างที่ได้จากโค้ด Arbor

การตั้งค่า VLAN ในสวิตช์เลเยอร์ 2 ที่ควรปฏิบัติ

การนำอุปกรณ์เครือข่ายเช่น สวิตช์หรือเราเตอร์มาใช้งาน นอกจากการตั้งค่าอุปกรณ์ให้สามารถใช้งานได้ตามต้องการแล้ว ควรคำนึงถึงวิธีการตั้งค่าอุปกรณ์ให้มีความปลอดภัยที่สูงขึ้น เนื่องจากค่าความปลอดภัยที่ตั้งมาจากผู้ผลิต จะมีความปลอดภัยในระดับต่ำ หากผู้ปฏิบัติงานหรือผู้ดูแลระบบเครือข่ายขาดความรู้ในการป้องกันการตั้งค่าอุปกรณ์อาจเป็นสาเหตุให้เครือข่ายอยู่ในความเสี่ยงที่จะถูกโจมตีหรือถูกรบกวนจากผู้ใช้งานและส่งผลให้เครือข่ายมีประสิทธิภาพการทำงานที่ลดลงมีข้อแนะนำหรือข้อควรควรปฏิบัติในการตั้งค่าสวิตช์เลเยอร์ 2 ดังต่อไปนี้

1. ควรหลีกเลี่ยงการใช้ VLAN 1

เนื่องจาก VLAN 1 เป็นค่าปริยาย (Default) มาจากโรงงาน หากเรายังไม่ได้ตั้งค่าใด ๆ ในสวิตช์ ผู้ใช้ที่เชื่อมต่อเข้ามาจะถือว่าอยู่ใน VLAN ID 1 ทั้งหมด เป็นความเสี่ยงจากบุคคลภายนอกองค์กรที่พยายามเชื่อมต่อเข้ามาในระบบ เนื่องจากสามารถคาดเดาได้ง่าย และยังไม่ป้องกันอุปกรณ์แปลกปลอมอื่น ๆ ที่อาจเข้ามาในระบบของเราได้อีกด้วย

2. ปิดการใช้ DTP (Dynamic trunking protocol)

DTP เป็น โพรโทคอลที่มีคุณสมบัติเฉพาะของบริษัทซิสโก้ ถูกพัฒนาโดยมีจุดประสงค์ต้องการให้มีการเจรจาระหว่างสวิตช์ทั้งสองฝั่ง สามารถสถาปนาการเชื่อมต่อให้เป็นพอร์ตทริงค์ได้โดยอัตโนมัติ ซึ่งปกติแล้วเฟรมของ DTP จะส่งออกจากพอร์ตของสวิตช์อยู่ตลอดเวลา เพื่อตรวจสอบปลายทางว่าต้องการเจรจาด้วยหรือไม่ โดยคำสั่งที่ใช้สำหรับตรวจสอบการทำงาน DTP คือคำสั่ง `show dtp interface` จะแสดงการตั้งค่าและจำนวน DTP แพ็กเกจที่ส่ง-รับเข้ามาพอร์ตของสวิตช์ทำงานได้ 2 แบบคือแอกเซสและทริงค์ แต่การระบุโหมดการตั้งค่าในอุปกรณ์มีโหมดให้เลือกได้หลายแบบ ตามตารางที่ 2-10

ตารางที่ 2-10 โหมดของโพรโทคอล DTP ต่าง ๆ ที่สามารถเลือกได้

| โหมด | หน้าที่ |
|-------------------|--|
| Trunk | ทำหน้าที่เป็นทริงค์โดยไม่คำนึงว่าอีกฝั่งจะมีสถานะเป็นอะไร |
| Access | ทำหน้าที่เป็นพอร์ตแอกเซส โดยไม่สนต่อการเจรจาของฝั่งตรงข้าม |
| Dynamic Auto | สร้างทริงค์โดยดูจาก DTP ที่ร้องขอจากฝั่งตรงข้ามว่าต้องการเป็นแบบใด |
| Dynamic Desirable | พยายามจะเป็นทริงค์หากฝั่งตรงข้ามสามารถเป็นทริงค์ได้เช่นกัน |
| Nonegotiate | ป้องกันพอร์ตส่ง DTP ออกไปใช้เฉพาะพอร์ตที่เป็นแอกเซสหรือทริงค์ |

ตารางที่ 2-11 ผลลัพธ์เมื่อเลือกการตั้งค่า DTP ในโหมดต่าง ๆ

| Mode | Dynamic auto | Dynamic desirable | Trunk | Access |
|-------------------|--------------|-------------------|----------|----------|
| Dynamic auto | Access | Trunk | Trunk | Access |
| Dynamic desirable | Trunk | Trunk | Trunk | Access |
| Trunk | Trunk | Trunk | Trunk | ไม่แนะนำ |
| Access | Access | Access | ไม่แนะนำ | Access |

จากตารางที่ 2-11 แสดงให้เห็นถึงผลที่ได้จากการตั้งค่าระหว่างพอร์ตทั้ง 2 ฟังก์ชันแสดงโหมดของฝั่งที่ 1 หลักแสดงโหมดของฝั่งที่ 2 ตัวอย่างเช่นหากทั้งสองฝั่งตั้งค่าเป็น โหมด Dynamic auto ทั้งคู่ ลิงก์ที่ได้จะทำงานในโหมดแบบแอกเซส หรือหากด้านหนึ่งตั้งเป็นแบบทริงค์ อีกฝั่งหนึ่งเป็นแบบ Dynamic auto ผลที่ได้จะเป็นแบบทริงค์

แม้ว่าโปรโตคอล DTP จะช่วยอำนวยความสะดวก แต่ข้อเสียของพอร์ตสวิตช์ที่สามารถเปลี่ยนโหมดการทำงานได้ หากเลือกโหมดการทำงานไม่เหมาะสมแล้ว อาจเป็นช่องโหว่จากการถูกโจมตีจากผู้ไม่หวังดีได้

ดังนั้น หากพอร์ตใดไม่มีความจำเป็นต้องเปลี่ยนแปลงการทำงานบ่อย ๆ ควรตั้งค่าพอร์ตสวิตช์ไม่ให้อัตโนมัติ (ด้วยคำสั่ง `nonegotiate`) เช่นในกรณีที่ต้องกับโฮสต์เพื่อป้องกันการโจมตีแบบ VLAN hopping ที่เกิดจากผู้โจมตีพยายามเปลี่ยนให้พอร์ตกลายเป็นทริงค์เพื่อส่งเฟรมที่มี VLAN 2 ชั้น (double encapsulated) เข้ามาในเครือข่ายทำให้เสมือนกลายเป็นส่วนหนึ่งของ VLAN ทุกแห่งที่เชื่อมต่อกับสวิตช์และสามารถส่งข้อมูลเข้ายังเครือข่ายภายในได้

ตัวอย่างคำสั่งที่ใช้ในการป้องกันการเป็นพอร์ตทริงค์

```
Switch(config-if)#switchport mode {access | trunk}
Switch(config-if)#switchport nonegotiate
```

จากตัวอย่างคำสั่งในบรรทัดแรกเป็นการบอกให้พอร์ตนี้ทำงานในแบบแอกเซส ถัดมาในบรรทัดที่สอง เป็นการบอกว่าพอร์ตนี้ไม่ต้องทำหน้าที่เจรจากับอุปกรณ์ที่อยู่เพื่อป้องกันการเปลี่ยนสถานะไปเป็นทริงค์

3. จำกัดค่าการเรียนรู้ MAC

การทำให้พอร์ตของสวิตช์ปลอดภัยมากขึ้น จะมีคำสั่งที่เกี่ยวกับด้านความปลอดภัย (Port security) ซึ่งใช้ในการป้องกันพอร์ตจากผู้ที่ไม่ได้รับสิทธิ์การใช้งาน หรือผู้โจมตีที่มุ่งหวังจะเข้ามาติดต่อกับพอร์ตของสวิตช์นั้น ๆ โดยมีการตรวจสอบจาก MAC ที่เราได้ตั้งค่าไว้ หรือตามจำนวน MAC ที่ได้จำกัดการเรียนรู้ไว้ในแต่ละพอร์ต

สำหรับพอร์ตแอกเซส หากทราบจำนวนผู้ใช้งานที่แน่นอน หรือผู้ใช้งานมีลักษณะการใช้งานประจำที่มีเครื่องคอมพิวเตอร์เครื่องเดิมและมีหมายเลข MAC เพียงเลขเดียวต่อเครื่องเท่านั้น ผู้ดูแลเครือข่ายควรจำกัดการเรียนรู้ MAC ที่พอร์ตของสวิตช์เพื่อป้องกันการโจมตีที่อาจเกิดขึ้น โดยใช้โปรแกรมสร้างหมายเลข MAC ปลอมขึ้นมาซึ่งอาจส่งผลให้สวิตช์มีการเรียนรู้และเก็บข้อมูลจนเต็มและไม่สามารถรับส่งหรือเรียนรู้หมายเลข MAC ใหม่ ๆ ที่จะเข้ามาได้ ดังตัวอย่างคำสั่งด้านล่าง

ตารางที่ 2-12 ขั้นตอนการใช้คำสั่งในการจำกัดหมายเลข MAC

| ขั้นที่ | คำสั่ง | จุดประสงค์ |
|---------|--|---|
| 1 | Switch(config)# interface interface_id | เข้าสู่โหมดการตั้งค่าในพอร์ตของสวิตช์ เช่น gigabitethernet 0/1 |
| 2 | Switch(config-if)# switchport mode access | ให้พอร์ตทำงานในโหมดแอกเซส |
| 3 | Switch(config-if)# switchport port-security | ให้พอร์ตทำงานแบบป้องกันและปลอดภัย |
| 4 | Switch(config-if)# switchport port-security maximum value | (ตัวเลือก) ระบุจำนวนหมายเลข MAC สูงสุดที่พอร์ตจะรับได้ หากไม่ระบุปกติมีค่าเป็น 1 |
| 5 | Switch(config-if)# switchport port-security violation {protect restrict shutdown} | - restrict พอร์ตยังทำงานแต่จะทิ้งเฟรมที่ไม่ใช่จาก MAC ที่กำหนดและแจ้งเตือนผ่านทาง SNMP แทรป - shutdown พอร์ตไม่ทำงานและอยู่ในสถานะ <i>error-disabled</i> ต้องใช้คำสั่ง <code>no shutdown</code> ให้ทำงานอีกครั้ง และมีการส่งการแจ้งเตือน |

ตารางที่ 2-12 (ต่อ)

| ขั้นที่ | คำสั่ง | จุดประสงค์ |
|---------|--|--|
| 6 | Switch(config-if)# end | ออกจากโหมดการตั้งค่า |
| 7 | Switch# show port-security address interfaceinterface_id Switch# show port-security address | ตรวจสอบการตั้งค่าความปลอดภัย ตามพอร์ตที่กำหนด |

ตามขั้นตอนการตั้งค่าพอร์ตของสวิตช์ เมื่อนำไปใช้อุปกรณ์สวิตช์ยี่ห้อซิสโก้ ดังตัวอย่างที่แสดง เป็นการจำกัดหมายเลข MAC ให้มีได้สูงสุดเพียง 3 ค่า หากมีหมายเลข MAC ของเครื่องที่ 4 เข้ามา พอร์ตจะไม่สนใจและทิ้งเฟรมข้อมูลนั้นไปส่วนเครื่องที่เริ่มส่งข้อมูลก่อน 3 เครื่องแรก ยังคงใช้งานได้ปกติ และไม่มีการบันทึกการละเมิดของการเข้าถึงนี้

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 3
Switch(config-if)#switchport port-security violation protect
```

4. ควรระบุ VLAN ในพอร์ตตามที่มีการใช้งานจริง

ในพอร์ตแบบทริงก์ ซึ่งส่วนใหญ่ใช้เชื่อมต่อระหว่างสวิตช์กับสวิตช์ หรืออุปกรณ์ที่มีความต้องการใช้งานมากกว่าหนึ่ง VLAN สมควรที่จะระบุเฉพาะ VLAN ที่ใช้งานอยู่จริงเท่านั้น เนื่องจากพบว่า การตั้งค่าที่ไม่เหมาะสม เช่น การปล่อยให้ทุก VLAN ผ่านเข้าออกพอร์ตได้ทั้งหมด (1-4094) ไม่มีการควบคุม VLAN ทำให้เป็นช่องโหว่ที่อาจถูกโจมตี หรือมีการส่งข้อมูลที่ไม่เป็นประโยชน์เช่น บรอดคาสต์เข้ามารบกวนโดยไม่จำเป็น จึงควรมีการระบุให้ชัดเจนว่ามี VLAN ไດบ้างต้องการใช้งาน ณ ปลายทางของสวิตช์ที่อยู่ด้วยเป็นการลดความเสี่ยงที่อาจถูกโจมตี และช่วยลดปริมาณข้อมูลที่ไม่เกี่ยวข้อง หรือข้อมูลที่ไม่พึงประสงค์

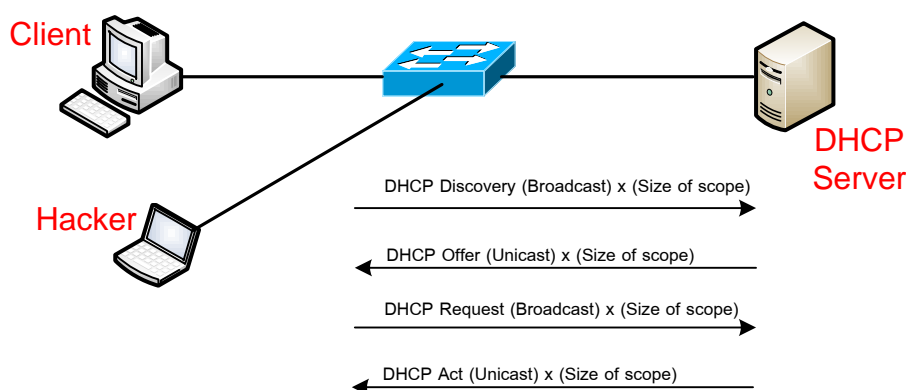
```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 40,45,50-56
Switch(config-if)#switchport nonegotiate
```

ตัวอย่างคำสั่งในการคุม VLAN ของพอร์ตแบบทริงค์ ในบรรทัดที่สองเป็นการระบุว่า จะให้ VLAN ใดผ่านเข้าออกพอร์ตนี้ได้บ้าง สามารถระบุเป็นช่วงของ VLAN ก็ได้ ตามตัวอย่าง เป็นการยอมให้ VLAN 40, 45 และ 50 ถึง 56 สามารถผ่านไปได้ ส่วนคำสั่ง `nonegotiate` เป็นการ บอกว่าไม่มีการเจรจาแลกเปลี่ยนการเป็นโฮมคอต โนมติกับพอร์ตฝั่งตรงข้าม

5. ป้องกันการโจมตีจาก DHCP

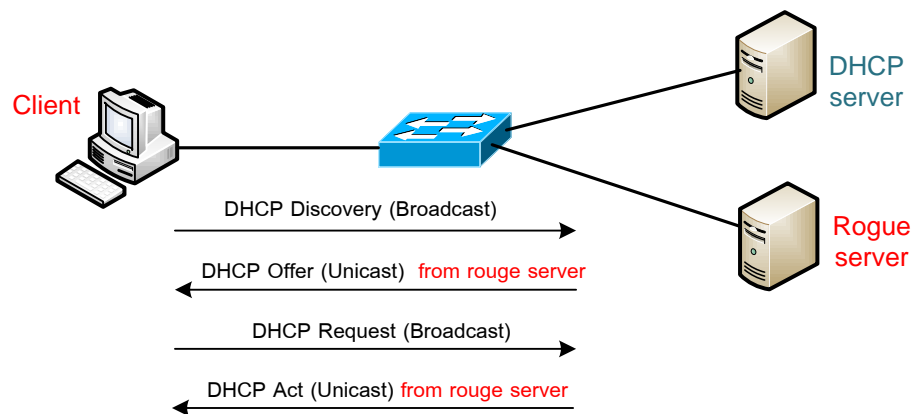
โพรโทคอล DHCP ใช้สำหรับจัดสรรหมายเลขไอพีให้แก่เครื่องลูกข่าย ช่วยลดภาระงาน ให้แก่ผู้ดูแลระบบ โดยมีเครื่องแม่ข่าย DHCP ทำหน้าที่ควบคุมการแจกไอพีตามที่มีการร้องขอ โดย เครื่องลูกข่ายจะได้รับค่าที่จำเป็นสำหรับใช้สื่อสาร เช่น หมายเลขไอพี, หมายเลขซับเน็ต, หมายเลขเกตเวย์, หมายเลข DNS หรือระยะเวลาที่ถือครองไอพีหมายเลขนั้น ๆ (Lease time)

การโจมตีด้วย DHCP อาจมีจุดประสงค์เพื่อรบกวนผู้ใช้งานในเครือข่าย เช่น การร้องขอ หมายเลขไอพีจำนวนมาก เกินขอบเขตที่เครื่องแม่ข่ายกำหนดไว้ เป็นการทำให้หมายเลขไอพีชุดนั้นหมดไป (DHCP starvation attack) ทำให้ผู้ใช้งานรายอื่นไม่สามารถใช้งานตามที่ร้องขอได้ ดังแสดง ตัวอย่างในภาพที่ 2-15 ผู้โจมตีส่งการร้องขอชนิดบรอดคาสต์จำนวนมากเพื่อค้นหาเครื่องแม่ข่าย ที่ให้บริการ DHCP โดยแต่ละครั้งที่ส่งจะทำการปลอมที่อยู่ของผู้โจมตี ทำให้เสมือนกับว่ามีเครื่อง ลูกข่ายขอใช้บริการจำนวนมาก และทำให้หมายเลขไอพีที่จัดสรรไว้ไม่เพียงพอต่อจำนวนผู้ใช้งาน



ภาพที่ 2-15 การโจมตีแบบ DHCP starvation

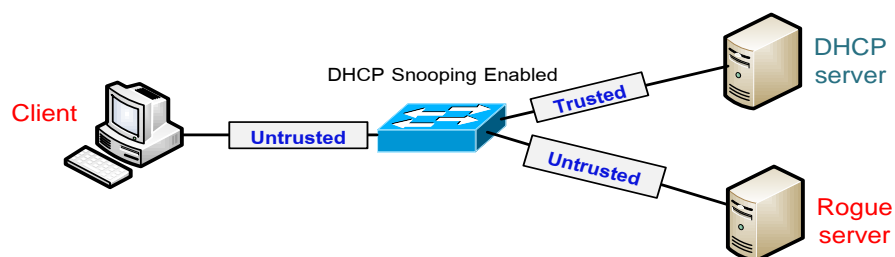
Rogue DHCP เป็นอีกหนึ่งของการโจมตีด้วย DHCP เพื่อดักจับข้อมูลผู้ใช้งาน โดยทำการ แจกหมายเลขเกตเวย์ของเครื่องที่ดักจับข้อมูลให้กับเครื่องผู้ใช้งานแทนเกตเวย์ที่มีอยู่ในระบบจริง ทำให้ผู้ไม่หวังดีมาคั่นแทรกกลางระหว่างการสื่อสาร ก่อนส่งออกไปเกตเวย์จริงในระบบ



ภาพที่ 2-16 การโจมตีแบบ rogue DHCP server

ผลกระทบของ Rogue DHCP ที่อาจเกิดขึ้นกับผู้ใช้งานมีหลายลักษณะ เช่น ได้รับเกตเวย์ที่ผิด การได้ค่า DNS server ที่ผิด หรือการได้หมายเลขไอพีที่ผิดเพื่อไม่ให้สามารถใช้งานได้ ทั้งนี้การเกิดปัญหาลักษณะนี้อาจเกิดได้จากความไม่ตั้งใจของผู้ใช้งานหรือรู้เท่าไม่ถึงการณ์ เช่น การนำอุปกรณ์ชนิดอื่นที่สามารถแจก DHCP ได้ ต่อเข้ามาในระบบ (เช่น Access point) โดยไม่ปิดการทำงานของ DHCPserver ก่อน

วิธีการป้องกันการเกิดเหตุการณ์ในลักษณะนี้สามารถทำได้ 2 วิธีคือ 1) การใช้โปรแกรมตรวจสอบการทำงานของ DHCP โดยติดตั้งที่เครื่องผู้ใช้งาน เช่น โปรแกรม DHCPloc, DHCP_prob 2) การตั้งค่าที่อุปกรณ์สวิตช์ เรียกการทำงานนี้ว่า DHCP snooping



ภาพที่ 2-17 การป้องกันการโจมตีด้วย DHCP โดยใช้ DHCP Snooping

การทำงานของ DHCP snooping เป็นการกำหนดที่พอร์ตของสวิตช์ว่าจะเชื่อถือพอร์ตที่ต่อกับเครื่องแม่ข่าย DHCP เท่านั้น ส่วนพอร์ตอื่น ๆ ที่ต่อกับเครื่องลูกข่ายจะกำหนดให้เป็นพอร์ตที่ไม่น่าเชื่อถือ และสวิตช์จะสร้างตารางการจับคู่ระหว่างหมายเลขไอพีกับหมายเลข MAC ซึ่งจะดู

จากเฟรมของ DHCP offer ว่ามาจากพอร์ตที่กำหนดว่าน่าเชื่อถือหรือไม่ ถ้ามาจากพอร์ตที่น่าเชื่อถือ ก็จะส่งเฟรมนั้นต่อไปและเพิ่มในตาราง DHCP snooping แต่หากไม่ใช่ก็จะทำการทิ้งเฟรมข้อมูลนั้นไป ตัวอย่างคำสั่งการตั้งค่าการทำงานของ DHCP snooping แสดงในตารางที่ 2-13

ตารางที่ 2-13 การใช้คำสั่งเปิดการทำงานของ DHCP snooping

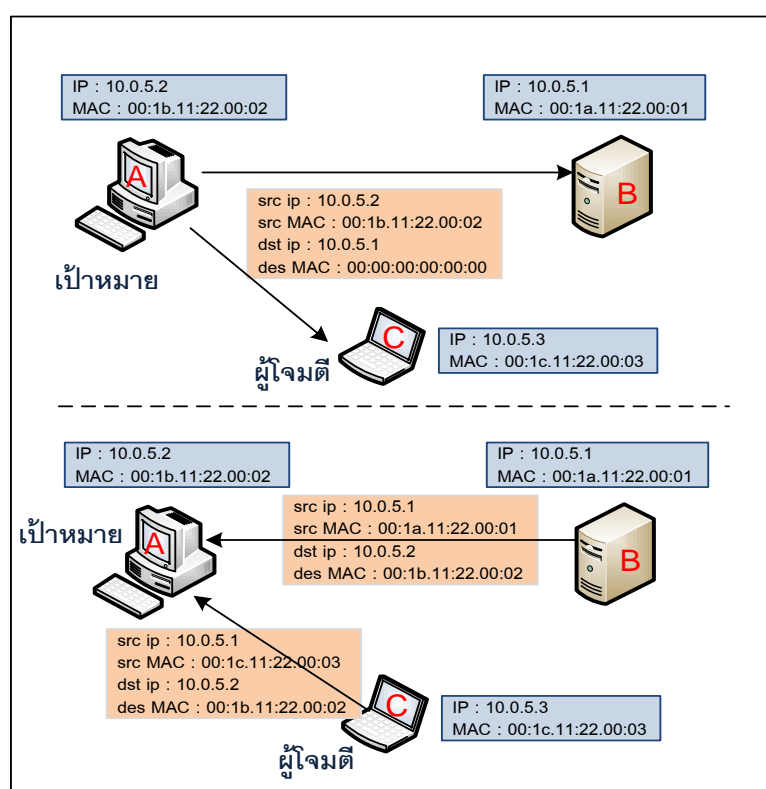
| ขั้นที่ | คำสั่ง | คำอธิบาย |
|---------|--|---|
| 1 | Switch(config)# ip dhcp snooping vlan {{vlan_ID [vlan_ID]} {vlan_range}} | ระบุ vlan ที่ต้องการตรวจสอบสามารถ ระบุได้หลาย vlan หรือเป็นช่วงก็ได้ |
| 2 | Switch(config)# ip dhcp snooping | เปิดฟังก์ชัน dhcp snooping ให้ทำงาน |
| 3 | Switch(config-if)# ip dhcp snooping trust | ระบุในพอร์ตสามารถ forward แพ็กเก็ต DHCP ได้ |
| 4 | Switch(config-if)# no ip dhcp snooping trust | ระบุให้พอร์ตเลิก forward แพ็กเก็ต DHCP |
| 5 | Switch(config-if)# ip dhcp snooping limit rate rate | จำกัดอัตราการร้องขอแพ็กเก็ต DHCP |

6. ป้องกันการโจมตีด้วยโปรโตคอล ARP

การโจมตีแบบ ARP poisoning หรือการปลอม (ARP spoofing) เป็นการอาศัยช่องโหว่ของโปรโตคอล ARP ซึ่งไม่ได้ถูกออกแบบมาให้มีการตรวจสอบความถูกต้องของผู้รับและผู้ส่งตั้งแต่แรก โดยจุดประสงค์ของการปลอม ARP มี 2 ลักษณะคือ 1) ต้องการเป็นตัวเป็นคนกลางเพื่อดักรับข้อมูล (Man in the middle) 2) ต้องการรบกวนการใช้งาน โดยส่งเกตเวย์ปลอมกลับไปยังผู้ใช้ทำให้ไม่สามารถติดต่อกับเครือข่ายอื่น ๆ ได้ เนื่องจากการทำงานของ ARP หากมีเครื่องที่อยู่ในเครือข่ายท้องถิ่นเดียวกันต้องการติดต่อกับเครื่องอื่น โดยทราบเพียงหมายเลขไอพีแต่ไม่ทราบหมายเลข MAC เครื่องที่ต้องการติดต่อกับจะส่งข้อมูลชนิดบรอดคาสท์ที่เรียกว่า ARP request เพื่อสอบถามเครื่องที่มีไอพีดังกล่าวว่ามีหมายเลข MAC เป็นอะไร หากเครื่องที่มีไอพีตรงกับ ARP request ได้รับก็จะตอบกลับไปด้วย ARP reply พร้อมด้วยข้อมูลหมายเลข MAC ของตนเอง

เห็นได้ว่าการทำงานของ ARP มีการส่ง ARP Request ออกไป แล้วรอให้มี ARP Reply ตอบกลับมา ระหว่างที่กำลังรอคำตอบอยู่นั้นหากมีผู้ไม่หวังดีตอบ ARP Reply ปลอมให้แทน ผู้รับไม่สามารถทราบได้ว่า ARP Reply นั้นไม่ได้มาจากผู้ส่งตัวจริง จึงบันทึกข้อมูลหมายเลข MAC ที่ไม่ถูกต้องไว้ในตาราง ARP ของตนเอง

ดังแสดงในภาพที่ 2-18 เครื่อง A ต้องการติดต่อกับเครื่อง B ที่มีหมายเลขไอพี 10.0.5.1 แต่ไม่รู้หมายเลข MAC จึงส่งข้อมูลชนิดบรอดคาสต์ถามทุกเครื่องที่อยู่ในเครือข่าย ว่าผู้ที่มีหมายเลขไอพีดังกล่าวมี MAC เป็นอะไร หากเครื่อง C เป็นของผู้โจมตี ตอบ ARP reply ได้เร็วกว่าเครื่อง B โดยมี MAC เป็นของเครื่องตนเอง ทำให้เครื่อง A ได้รับข้อมูลแบบผิด ๆ ว่า หากต้องการส่งข้อมูลไปหาไอพี 10.0.5.1 ให้ใช้หมายเลข MAC เป็น 00:1c:11:22:00:03 ซึ่งเป็นของเครื่อง C แทนที่ความจริงแล้วต้องเป็นหมายเลข MAC ของเครื่อง B ตัวอย่างโปรแกรมที่ทำการปลอม ARP เช่น ARPSpoof, Dsniff, Ettercap, Netcut, Cain & Abel



ภาพที่ 2-18 ตัวอย่างการโจมตีด้วย ARP

การป้องกันทำได้โดยการใช้ความสามารถของสวิตช์ที่เรียกว่า Dynamic ARP inspection (DAI) เป็นการตรวจสอบการทำงานของ ARP ว่าผิดปกติหรือไม่ โดยจะสร้างตารางจับคู่ระหว่างหมายเลข MAC กับหมายเลข IP (ชื่อตาราง DHCP snooping) ไว้เป็นฐานข้อมูล เมื่อมีแพ็กเก็ต ARP เข้ามาก็จะเทียบค่า MAC กับหมายเลข IP ที่มีในตารางว่าตรงกันหรือไม่ หากไม่ตรงกันก็จะทิ้งแพ็กเก็ต ARP นั้นไป ดังภาพที่ 2-19 ตัวอย่างการจับคู่ MAC และหมายเลข IP ในตาราง DHCP snooping ซึ่งจะบอกหมายเลข VLAN และพอร์ตที่เรียนรู้แพ็กเก็ต ARP เข้ามา

| sra_noc_m3k_01#show MacAddress | ip dhcp snooping IpAddress | binding Lease(sec) | Type | VLAN | Interface |
|-----------------------------------|-------------------------------|-----------------------|---------------|------|----------------------|
| 00:23:7D:53:2A:61 | 10.5.5.81 | 27180 | dhcp-snooping | 8 | FastEthernet1/0/20 |
| 00:23:AE:18:1A:C2 | 10.5.5.51 | 20403 | dhcp-snooping | 8 | GigabitEthernet1/1/1 |
| 00:21:5D:C6:27:08 | 10.5.5.162 | 27520 | dhcp-snooping | 8 | FastEthernet1/0/20 |
| 00:1F:29:D8:3B:7E | 10.5.5.60 | 24159 | dhcp-snooping | 8 | FastEthernet1/0/19 |

ภาพที่ 2-19 ตาราง DHCP snooping จากสวิตช์ที่ป้องกันการโจมตีแบบ ARP

คำสั่งที่ใช้ในการป้องกันการโจมตีจากการปลอม ARP แสดงในตารางที่ 2-14

ตารางที่ 2-14 คำสั่งที่ใช้ในการป้องกันการโจมตีด้วย ARP

| ขั้นที่ | คำสั่ง | คำอธิบาย |
|---------|--|---|
| 1 | Switch(config)# ip arp inspection vlan {vlan_ID vlan_range} | ให้ DAI ทำงานตาม Vlan ที่กำหนด |
| 2 | Switch(config)# ip arp inspection log-buffer entriesnumber | ระบุขนาดในการเก็บ log มีค่าตั้งแต่ 0 – 1024 โดยปกติจะมีค่าเป็น 32 |
| 3 | Switch(config)# interface {interface name} | ระบุพอร์ตที่ต้องการตรวจสอบ |
| 4 | Switch(config-if)# ip arp inspection trust | |
| 5 | Switch(config-if)# ip arp inspection limit {ratepps [burst intervalseconds] none} | |

งานวิจัยที่เกี่ยวข้อง

ในการพัฒนาระบบค้นหาโครงสร้าง VLAN ทางผู้จัดทำได้ศึกษางานวิจัยต่าง ๆ ที่เกี่ยวข้องกับการออกแบบและใช้งาน VLAN ในเครือข่าย ผลกระทบที่อาจเกิดขึ้นหากขาดการออกแบบที่ดีโดยมีงานวิจัยที่เกี่ยวข้องดังต่อไปนี้

1. ลักษณะการออกแบบ VLAN ที่ควรปฏิบัติ

บทความเรื่อง Survey of virtual LAN usage in campus network ซึ่งตีพิมพ์ในวารสาร IEEE ปี 2011 โดย Minlan Yu, Jennifer Rexford, Xin Sun, Sanjay Rao และ NickFeamster ได้สำรวจการนำ VLAN มาใช้งานในเครือข่ายของมหาวิทยาลัย 3 แห่ง และปัญหาที่เกิดขึ้นจาก

การออกแบบหรือตั้งค่า VLAN ไม่ถูกต้องเมื่อใช้ในเครือข่ายขนาดใหญ่ โดยสรุปจุดประสงค์ของการนำ VLAN มาใช้ได้ 4 ด้านคือ ใช้ควบคุมการเกิด broadcast กำหนดนโยบายในการเข้าใช้เครือข่าย ใช้กระจายงานด้านบริหารจัดการเครือข่าย และรองรับผู้ใช้งานที่มีการเคลื่อนที่ เช่น เครือข่ายไร้สาย ซึ่งจากจุดประสงค์การใช้งานที่แตกต่างกัน ทำให้พบปัญหา เช่น ข้อจำกัดของจำนวน VLAN ต่อหนึ่งสวิตช์ที่มีได้เพียง 4096 VLAN หรือหน่วยความจำของสวิตช์ที่เพิ่มสูงขึ้น หากมีการใช้ VLAN จำนวนมาก และจำนวนผู้ใช้งานต่อหนึ่ง VLAN ที่ไม่เหมาะสม นอกจากนี้ยังมีปัญหาเรื่องความซับซ้อนในการตั้งค่าภายในเครือข่าย

งานวิจัยเรื่อง Finding efficient VLAN topology for better broadcast containment โดย Abdul Hameed และ Adnan Noor Mian (2012) ได้หาประสิทธิภาพการใช้งาน VLAN ในเครือข่ายเพื่อควบคุมปริมาณ broadcast ที่ดี เนื่องจากผู้ดูแลระบบมักออกแบบ VLAN โดยไม่คำนึงถึงจำนวนผู้ใช้งานหรือปริมาณข้อมูลที่ใช้งานอยู่ ส่งผลกระทบต่อประสิทธิภาพการใช้งาน จึงเสนออัลกอริทึมชื่อว่า Simple set-base (SS) โดยพิจารณาจากกลุ่มข้อมูลที่จัดเก็บด้วยวิธีการวัดปริมาณข้อมูลแบบเมทริกซ์ (Traffic matrix) (ปริมาณการส่งข้อมูลระหว่างอุปกรณ์ที่เชื่อมต่อกันที่มีทั้งหมดในเครือข่ายนำมาสร้างเป็นตารางแบบเมทริกซ์) จากนั้นจึงใช้อัลกอริทึมที่พัฒนาขึ้นไปทดสอบกับเครือข่ายจำลองที่สร้างขึ้น ผลที่ได้คือ โครงสร้าง VLAN ที่มีประสิทธิภาพช่วยลดการ broadcast ในเครือข่าย

งานวิจัยเรื่อง Characterizing VLAN usage in an Operational Network โดย Yu-Wei Sung, Nan Zhang, Sanjay Rao และ Prashant Garimella (2007) แสดงให้เห็นถึงการใช้งาน VLAN ในเครือข่ายขนาดใหญ่ ผลกระทบที่เกิดขึ้นจากการออกแบบหรือตั้งค่าในสวิตช์ที่ไม่ถูกต้อง เช่น การมี VLAN ที่ไม่ได้ใช้งานจริง กระจายไปยังพอร์ตแบบทริงก์นำไปสู่สาเหตุที่ทำให้เกิด broadcast แพร่กระจาย ส่งผลให้ระบบขาดประสิทธิภาพในการสื่อสาร ควรมีการควบคุม VLAN ให้เหมาะสมและไม่ทำให้เกิด VLAN สูญหาย

งานวิจัยเรื่อง Systematic Approach for Evolving VLAN Designs ของ Xin Sun, Yu-Wei E.Sung, Sunil D.Krothapalli , และ Sanjay G.Rao (2010) ได้เสนอการออกแบบ VLAN ที่พิจารณาถึงการออกแบบ VLAN และการตั้งค่า VLAN โดยคำนึงถึงอัตราการเกิด broadcast ไม่ให้มีค่าเกินกำหนดในแต่ละสมาชิกของ VLAN หากมีค่าเกิน จะทำการแบ่ง VLAN ใหม่ และย้ายสมาชิกของ VLAN นั้น ๆ ออกเป็นกลุ่มใหม่ เป็นการลดจำนวนการเกิด broadcast อีกทั้งยังเสนอการตั้งค่าในอุปกรณ์สวิตช์โดยอัตโนมัติ เพื่อลดความผิดพลาดที่อาจเกิดขึ้น การผู้ดูแลระบบในการตั้งค่า VLAN ในอุปกรณ์สวิตช์ที่มีจำนวนหลาย ๆ ตัว

2. การหาแผนผังของเครือข่าย (Network discovery)

งานวิจัยเรื่อง A toolkit for automating and visualizing VLAN configuration ของ Sunil D. Krothapalli, Xin Sun, Yu-Wei E. Sung, Suan Aik Yeo และ Sanjay G. Rao (2009) แสดงให้เห็นถึงความท้าทายในการตั้งค่า VLAN ในเครือข่ายขนาดใหญ่ ผลกระทบด้านประสิทธิภาพและความปลอดภัยที่เกิดจากปัญหาการตั้งค่า VLAN ที่ผิดพลาด ซึ่งอาจเกิดจากผู้ปฏิบัติงาน จึงมีการพัฒนาเครื่องมือสำหรับตรวจสอบการใช้งาน VLAN และสามารถตั้งค่า VLAN ได้อย่างอัตโนมัติโดยแสดงผลผ่านทางเว็บ เพื่อใช้ในการแก้ปัญหาดังกล่าว

งานวิจัยเรื่อง Topology discovery for virtual local area networks โดย Hassan Gobjuka (2010) ได้นำเสนอวิธีแก้ปัญหาการแสดงรูปแบบการเชื่อมต่อเครือข่ายที่ประกอบด้วย VLAN จำนวนมากและมีอุปกรณ์ต่างผู้ผลิตอยู่ในเครือข่ายเดียวกัน จึงเป็นอุปสรรคในการรวบรวมข้อมูลการเชื่อมต่อของสวิตช์ เนื่องจากอุปกรณ์บางรายไม่สามารถเข้าถึงจาก SNMP ได้ (มีค่า OID เฉพาะของตนเอง) โดยเสนออัลกอริทึมในการค้นหาการเชื่อมต่อของสวิตช์ 2 รูปแบบคือ 1) แบบ Dense-AFT (Address forwarding table: AFT) สำหรับเครือข่ายที่มีค่า MAC จำนวนมาก และ 2) แบบ VLANs-Connections สำหรับกรณีเครือข่ายมีค่า MAC น้อยหรือเก็บข้อมูลจากสวิตช์ได้ไม่สมบูรณ์ เหมาะกับเครือข่ายขนาดเล็ก สุดท้ายเป็นการนำอัลกอริทึมทั้งสองมาใช้งานร่วมกันเพื่อสามารถนำไปใช้งานกับเครือข่ายที่มีขนาดใหญ่ได้

งานวิจัยเรื่อง Network topologic discovery base on SNMP โดย Kuangyu Qin และ Chunquan Li (2010) แสดงถึงวิธีการค้นหารูปแบบการเชื่อมต่อกันในเครือข่ายโดยใช้โปรโตคอล SNMP รวบรวมข้อมูลที่ได้จากอุปกรณ์เราเตอร์และสวิตช์ โดยพิจารณาจากค่าที่ได้จากตาราง ARP ของสวิตช์แต่ละตัว (ใช้ SNMP ออบเจกต์ชื่อ ipNetToMediaTable-OID 1.3.6.1.2.1.4.22) และใช้อัลกอริทึมในการค้นหาพอร์ตที่ต่อกับเครื่องผู้ใช้งานมาแสดงเครือข่ายการเชื่อมต่อ ซึ่งคล้ายกับงานนิพนธ์นี้ในการใช้โปรโตคอล SNMP รวบรวมข้อมูล

งานวิจัยเรื่อง Heterogeneous network topology discovery algorithm base on VLAN ของ Dancheng Li, Man Chen, Chunyan Han และ Yixian Liu (2012) แสดงให้เห็นถึงปัญหาของอุปกรณ์สวิตช์บางรายมีค่า MIB ที่ไม่เหมือนกัน ไม่สามารถสอบถามข้อมูลได้ เป็นอุปสรรคในการรวบรวมข้อมูล จึงให้วิธีค้นหารูปแบบการเชื่อมต่อ โดยวิเคราะห์จากตาราง MAC ที่เก็บในตัวสวิตช์ จากนั้นจึงใช้อัลกอริทึมในการค้นหารูปแบบการเชื่อมต่อในเครือข่าย ทำให้สามารถใช้งานได้ทั้งในระดับเครือข่ายขนาดใหญ่ แม้จะมีอุปกรณ์ที่ต่างผู้ผลิตกันเชื่อมต่ออยู่

บทที่ 3

วิธีดำเนินงาน

ขั้นตอนการพัฒนาระบบค้นหาโครงสร้าง VLAN ในเครือข่าย โดยใช้โปรโตคอล SNMP ในการเก็บข้อมูล มีการศึกษา วางแผนและออกแบบระบบ โดยมีรายละเอียดในแต่ละขั้นตอน ดังนี้

1. การวิเคราะห์และออกแบบระบบ ซึ่งแบ่งออกเป็นส่วนย่อย ดังนี้
 - 1.1 คุณสมบัติของระบบ
 - 1.2 การออกแบบ Usecase diagram, Usecase description
 - 1.3 การออกแบบส่วนติดต่อผู้ใช้งาน
 - 1.4 การออกแบบฐานข้อมูล
2. การหาค่า OID
 - 2.1 OIDVLAN สวิตช์ Cisco
 - 2.2 OIDVLAN สวิตช์ Huawei
 - 2.3 OIDVLAN สวิตช์ ZTE
3. ส่วนของการพัฒนาโปรแกรม ประกอบด้วย
 - 3.1 ภาพรวมของระบบ
 - 3.2 การนำขั้นตอนวิธีค้นหาในแนวคิดมาประยุกต์ใช้
 - 3.3 โครงสร้างทางกายภาพของระบบ

การวิเคราะห์และออกแบบระบบ

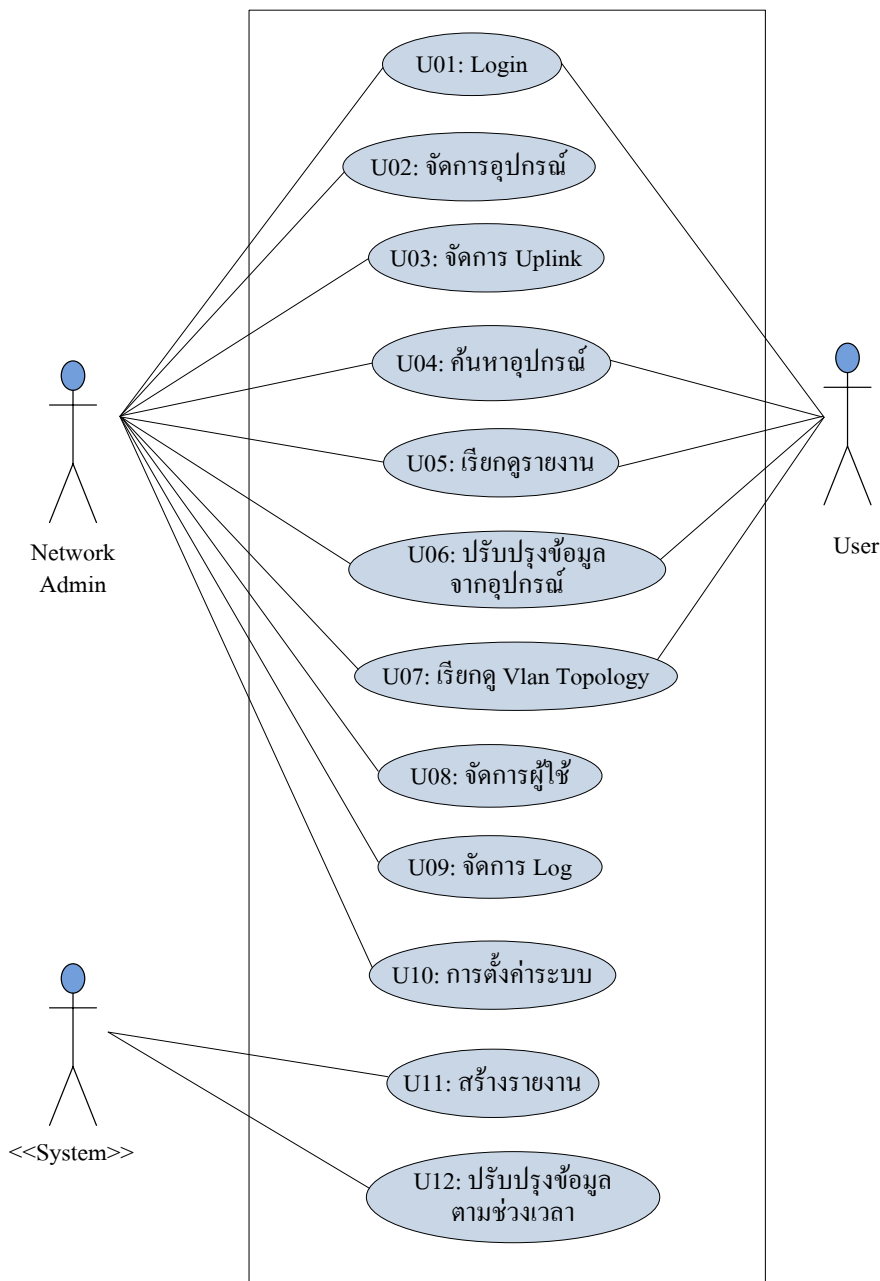
1. คุณสมบัติของระบบ
 - 1.1 การค้นหา VLAN ในสวิตช์และพอร์ต
 - 1.2 สามารถตรวจสอบหมายเลข VLAN ที่ไม่สอดคล้องกันระหว่างพอร์ตทั้งรังค์
 - 1.3 สามารถตรวจสอบและรายงานพอร์ตที่ VLAN สูญหาย
 - 1.4 แจ้งเตือน VLAN ที่คาดว่าไม่มีการใช้งาน
 - 1.5 VLAN ที่มีผู้ใช้เกินกว่าค่าที่กำหนด
 - 1.6 แจ้งเตือนการตั้งค่า VLAN ที่ไม่สมบูรณ์ เช่น มีใช้งานเพียงพอร์ตเดียว ไม่มี

การเชื่อมไปใช้งานที่โหนดอื่น

2. การออกแบบ Use case diagram และ Use case description

ผู้พัฒนาได้ใช้แผนภาพแสดงการใช้งานโปรแกรม (Use case diagram) เพื่อให้เห็นภาพรวมของระบบและผู้ที่เกี่ยวข้องว่ามีกิจกรรมใดเกิดขึ้นในระบบ ดังแสดงในภาพที่ 3-1

2.1 Use case diagram



ภาพที่ 3-1 Use case diagram ของระบบเฟิร์มแวร์ VLAN

จากภาพที่ 3-1 ประกอบด้วยผู้ที่เกี่ยวข้องในระบบ 3 กลุ่มคือ ผู้ดูแลระบบเครือข่าย, ผู้ใช้ และตัวระบบจัดการ VLAN

2.2 Use case description

จากภาพที่ 3-1 ผู้พัฒนาระบบได้เขียนคำอธิบายแผนภาพการทำงานของโปรแกรมไว้ดังตารางที่ 3-1 เพื่อแสดงให้เห็นถึงรายละเอียดของแต่ละยูสเคส

ตารางที่ 3-1 รายละเอียดของยูสเคสในระบบ

| ชื่อยูสเคส | คำอธิบาย |
|---------------------------------------|--|
| U01 : Login | การยืนยันตัวตนและพิสูจน์สิทธิ์การใช้งาน |
| U02 : จัดการอุปกรณ์ | ผู้ดูแลเครือข่ายสามารถเพิ่ม/ แก้ไข/ ลบ เกี่ยวกับข้อมูลอุปกรณ์ |
| U03 : จัดการ Uplink | ผู้ดูแลเครือข่ายสามารถ ค้นหา/ เพิ่ม/ แก้ไข/ ลบ ข้อมูลการเชื่อมต่ออุปกรณ์ (การเชื่อมต่อแบบ Uplink) |
| U04: ค้นหาอุปกรณ์ | ผู้ใช้สามารถตรวจสอบสถานะอุปกรณ์และ จำนวนVLAN ที่ใช้งานอยู่ |
| U05 : เรียกดูรายงาน | ผู้ใช้สามารถเรียกดูรายงานต่าง ๆ ได้แก่ <ol style="list-style-type: none"> 1. รายงาน VLAN ที่ไม่ใช้งาน 2. รายงาน VLAN ที่มีผู้ใช้มากเกินไปที่กำหนด 3. รายงานพอร์ตที่เป็นสมาชิก VLAN 4. รายงาน VLAN มีเส้นทางไม่ต่อเนื่อง 5. รายงานการเรียนรู้ MAC address จากอุปกรณ์ |
| U06 : ปรับปรุงข้อมูลจากอุปกรณ์ | ผู้ใช้สามารถดึงข้อมูล VLAN, พอร์ตที่เป็นสมาชิก จากอุปกรณ์ได้ |
| U07 : เรียกดูแผนภาพTopology เครือข่าย | ผู้ใช้สามารถเรียกดูการเชื่อมต่อแบบต่าง ๆ ได้แบ่งเป็น <ol style="list-style-type: none"> 1. การเชื่อมต่อ VLAN 2. การเชื่อมต่อทางกายภาพ 3. การเชื่อมต่อระหว่างจุดต่อจุด (คำนวณจำนวน hop) |
| U08 : จัดการผู้ใช้งาน | ผู้ดูแลเครือข่ายสามารถ ค้นหา/ สร้าง/ แก้ไข/ ลบ User login ในระบบได้ |

ตารางที่ 3-1 (ต่อ)

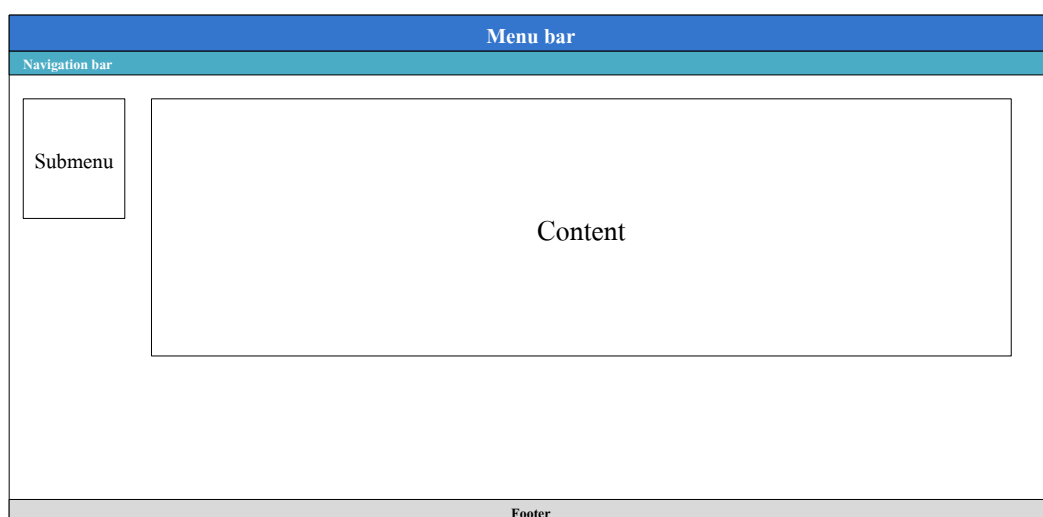
| ชื่อยูสเคส | คำอธิบาย |
|---------------------------------|--|
| U09 : จัดการ Log | <p>ให้ผู้ดูแลเครือข่ายค้นหาเหตุการณ์-การดำเนินงานของระบบ แบ่งออกเป็น 3 ส่วน คือ</p> <ol style="list-style-type: none"> 1. Operation log การกระทำที่เกิดจากผู้ใช้งาน 2. System log เกิดจากตัวระบบ เช่นการตั้งเวลาทำงาน 3. Security log เกิดจากการ login เข้าใช้งาน |
| U10 : การตั้งค่าระบบ | <p>ผู้ดูแลเครือข่ายสามารถกำหนดค่าต่าง ๆ ในกลุ่ม เช่น กลุ่มจังหวัด, กลุ่ม POP, ยี่ห้อสวิตช์ และค่าการแจ้งเตือนของระบบ</p> |
| U11 : สร้างรายงาน | <p>ระบบจะทำการสร้างรายงานอัตโนมัติตามช่วงเวลาที่กำหนด โดยมีรายละเอียดดังนี้</p> <ol style="list-style-type: none"> 1. นับจำนวน MAC address ต่อ VLAN 2. สรุป VLAN ที่ไม่มีการใช้งาน 3. การหา VLAN ที่ไม่ต่อเนื่องกัน |
| U12 : ปรับปรุงข้อมูลตามช่วงเวลา | <p>เป็นการปรับปรุงข้อมูล VLAN, การตั้งค่าพอร์ตของสวิตช์ให้ถูกต้องมากที่สุด โดยการตั้งเวลาทำงานตามที่กำหนด ซึ่งมีกระบวนการดังนี้</p> <ol style="list-style-type: none"> 1. ตรวจสอบสถานะอุปกรณ์ 2. สำรอง VLAN ของอุปกรณ์ทุกตัว 3. สำรองพอร์ตที่เป็นสมาชิก VLAN 4. เก็บไฟล์ตั้งค่าจากอุปกรณ์ที่ไม่รองรับ SNMP |

3. การออกแบบส่วนติดต่อผู้ใช้งาน (User interface)

ส่วนติดต่อผู้ใช้งานจะแสดงผลผ่านทางเว็บไซต์ ผู้พัฒนาระบบได้ยึดถือตามหลักออกแบบและพัฒนาหน้าเว็บ ให้ง่ายต่อการใช้งาน โดยมีการจัดองค์ประกอบต่าง ๆ ภายในเพจให้มีลักษณะสม่ำเสมอ เหมือนกันตลอดทั้งเว็บ ไม่สร้างความสับสนให้แก่ผู้ใช้งาน

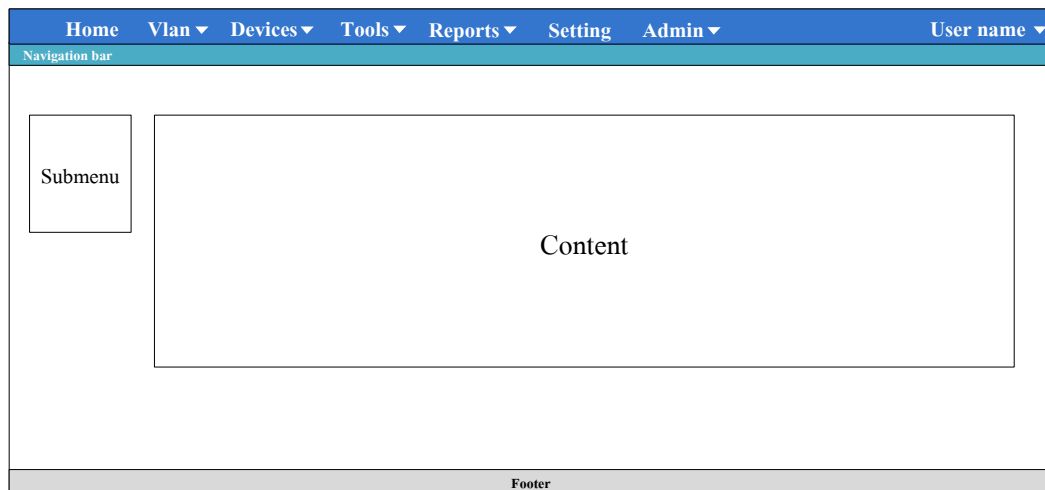
จากการวิเคราะห์ระบบสามารถออกแบบหน้าจอโดยมีการจัดแบ่งพื้นที่หน้าเว็บ (Page layout) แสดงในภาพที่ 3-2 ซึ่งมีส่วนประกอบต่าง ๆ ดังนี้

1. ส่วนหัว (Header) จะแสดงโลโก้และแถบเมนูต่าง ๆ ซึ่งจะเหมือนกันตลอดทั้งเว็บ
2. ระบบนำทางเนวิเกชัน (Navigationbar) จะวางไว้ได้แถบส่วนหัว สำหรับบอกว่ากำลังทำอยู่ในส่วนใดของโปรแกรม เป้าหมายของระบบนำทางคือช่วยให้ผู้ใช้งานเข้าถึงข้อมูลที่ต้องการได้อย่างรวดเร็วและไม่หลงทาง
3. ส่วนเนื้อหา (Page content) แสดงไว้ตรงกลางจอสำหรับวางเนื้อหาหรือตารางข้อมูลต่าง ๆ อาจมีเมนูเฉพาะกลุ่มวางอยู่ในส่วนนี้ด้วย
4. ส่วนท้ายของหน้า (Page footer) เป็นส่วนที่อยู่ล่างสุดของหน้า ระบุข้อความแสดงลิขสิทธิ์ และวิธีติดต่อกับผู้ดูแลเว็บไซต์



ภาพที่ 3-2 การจัดแบ่งพื้นที่หน้าเว็บ

ตัวอย่างหน้าจอในภาพที่ 3-3 แสดงภาพรวมการจัดวางตำแหน่งเมนูที่ส่วนหัวและตำแหน่งของเนื้อหาในหน้าจอ



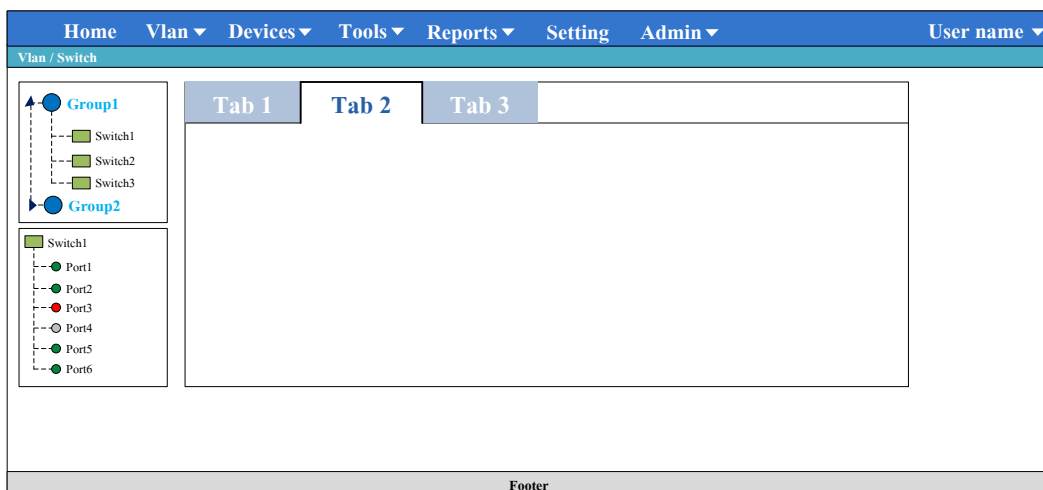
ภาพที่ 3-3 การวางตำแหน่งโดยรวม

ที่ส่วนหัวของทุกหน้าผู้ใช้งานจะพบเมนูต่าง ๆ ที่อยู่ด้านบนซึ่งมีทั้งสิ้น 8 เมนู โดยบางเมนูจะมีเมนูย่อย ดังภาพที่ 3-4 แสดงเมนูย่อยเมื่อมีการคลิกที่เมนูหลัก



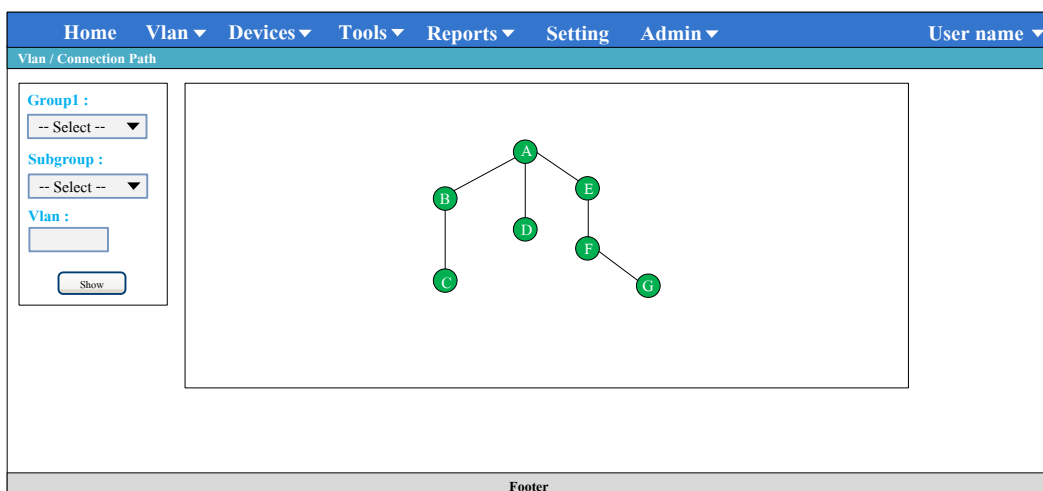
ภาพที่ 3-4 ตัวอย่างการแสดงผลเมนูย่อย

ในการแสดงผลบางหน้าผู้พัฒนาได้ใช้การแบ่งกลุ่มข้อมูล อุปกรณ์ในรูปแบบของ โครงสร้างแบบลำดับชั้น ตามกลุ่มที่จัดเก็บในฐานข้อมูล โดยเมื่อเลือกอุปกรณ์แต่ละตัวทางด้านบน ซ้าย จะปรากฏจำนวนพอร์ตทางด้านล่างซ้าย และข้อมูลรายละเอียดของอุปกรณ์ทางด้านขวา โดยมีการใช้เมนูแท็บ (Tab menu) ช่วยในการจัดแบ่งเนื้อหาอีกครั้ง ดังตัวอย่างการออกแบบในภาพที่ 3-5



ภาพที่ 3-5 หน้าจอการแสดงผลอุปกรณ์แบบโครงสร้างลำดับชั้น

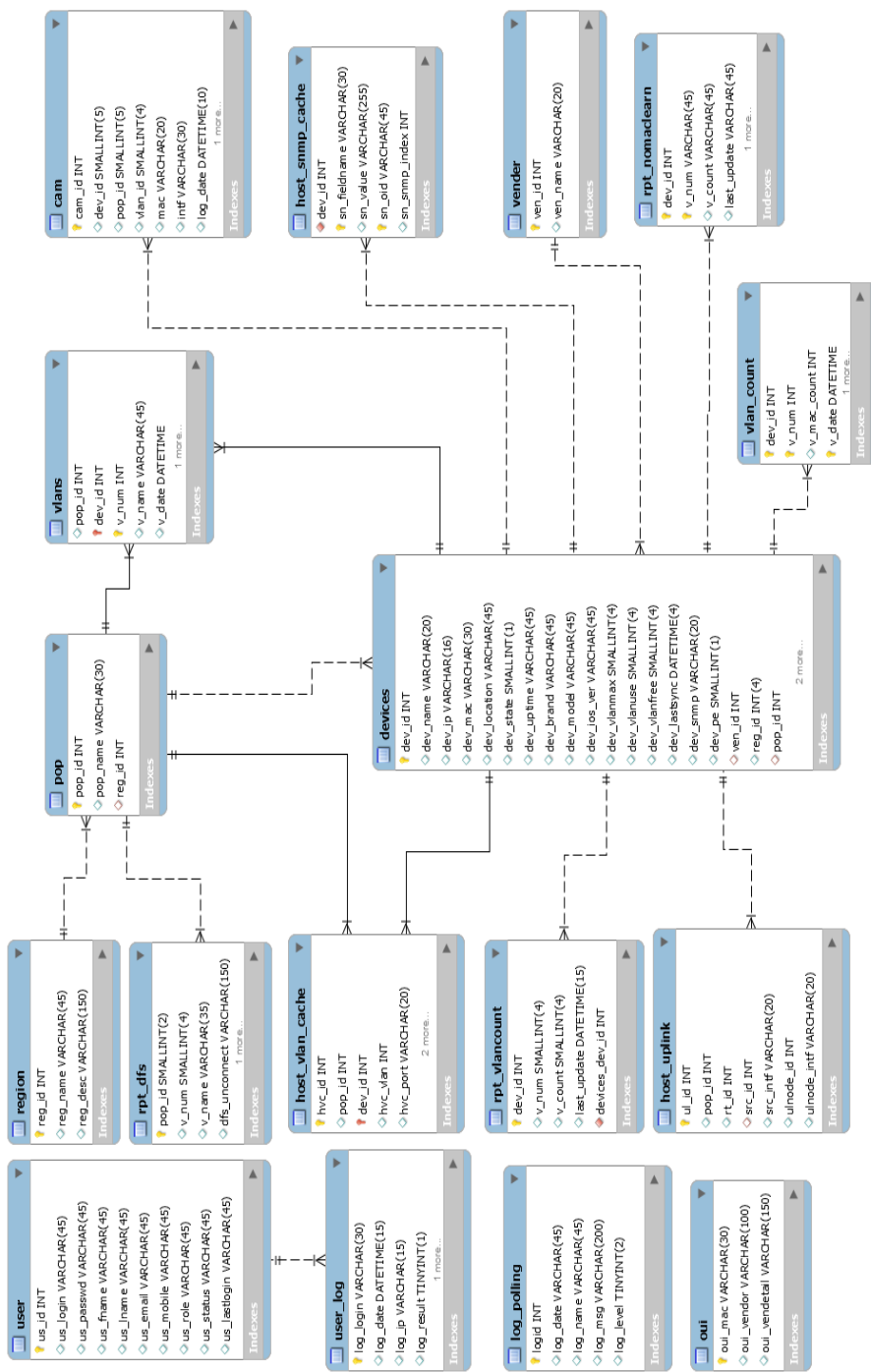
ภาพที่ 3-6 การแสดงผลของแผนภาพเครือข่าย โดยมีการป้อนข้อมูล VLAN ที่ต้องการแสดงทางด้านซ้ายมือ และแสดงผลลัพธ์ทางด้านขวา



ภาพที่ 3-6 หน้าจอแผนภาพเครือข่าย หลังเลือกกลุ่มและ VLAN ที่ต้องการ

4. การออกแบบฐานข้อมูล

4.1 Entity relationship diagram



ภาพที่ 3-7 ตาราง ER diagram

4.2 พจนานุกรมข้อมูล (Data dictionary)

จากตาราง ER diagram สามารถอธิบายรายละเอียดของแต่ละตารางได้ดังต่อไปนี้

ตารางที่ 3-2 ตาราง region

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|-----------|------------------|-------------|------|----------|
| reg_id | รหัสเขตพื้นที่ | INT | PK | 2 |
| reg_name | ชื่อเขตพื้นที่ | VARCHAR(45) | | ชลบุรี |
| reg_desc | อธิบายรายละเอียด | VARCHAR(45) | | |

ตารางที่ 3-3 ตาราง pop

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|-----------|--------------------------|-------------|------|----------|
| pop_id | รหัสพื้นที่ POP | INT | PK | 3 |
| pop_name | ชื่อย่อ POP ที่ให้บริการ | VARCHAR(45) | | CBI |
| reg_id | รหัสเขตพื้นที่ | INT | FK | 2 |

ตารางที่ 3-4 ตาราง vender

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|-----------|-------------------|-------------|------|----------|
| ven_id | รหัส | INT | PK | 3 |
| ven_name | ชื่อยี่ห้อผู้ผลิต | VARCHAR(45) | | Cisco |

ตารางที่ 3-5 ตาราง devices

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|--------------|-----------------------|-------------|------|----------------|
| dev_id | รหัสอุปกรณ์ | INT | PK | 12 |
| dev_name | ชื่อย่ออุปกรณ์ | VARCHAR(20) | | cbi_c3k_01 |
| dev_ip | หมายเลขไอพี | VARCHAR(15) | | 10.236.0.3 |
| dev_mac | หมายเลข mac-address | VARCHAR(14) | | 0023.0407.7c7f |
| dev_location | สถานที่ติดตั้งอุปกรณ์ | VARCHAR(45) | | บางแสน |

ตารางที่ 3-5 (ต่อ)

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|---------------|--|-------------|------|------------------------|
| dev_status | สถานะอุปกรณ์โดย นิยามค่าดังนี้ 0 = Down 1 = Up 2 = SNMP down 3 = UnMgmt | SMALLINT(1) | | 1 |
| dev_uptime | | VARCHAR(45) | | 385:18:49:14.6 |
| dev_model | รุ่นของอุปกรณ์ | VARCHAR(45) | | ME-3400 |
| dev_ios_img | ซอฟต์แวร์ที่ใช้ | VARCHAR(45) | | me340x- metrobases9 |
| dev_ios_ver | รุ่นของซอฟต์แวร์ที่ใช้ | VARCHAR(45) | | 12.2(55)SE3 |
| dev_vlanmax | VLAN สูงสุดที่รองรับ | INT | | 4094 |
| dev_vlanuse | VLAN ที่ใช้งาน | INT | | 512 |
| dev_vlanfree | VLAN ที่ว่าง | INT | | 3582 |
| dev_lastsync | เวลาที่ล่าสุดที่เช็คสถานะ อุปกรณ์ | DATETIME(0) | | 2015-04-27 10:40:01 |
| dev_snmp | ค่า community ที่ตั้งค่า ในอุปกรณ์ | VARCHAR(45) | | public |
| dev_teluser | ชื่อผู้ใช้สำหรับ telnet | VARCHAR(45) | | user1 |
| dev_telpasswd | รหัสผ่านที่ใช้ telnet | VARCHAR(45) | | 1234 |
| dev_enpasswd | รหัสผ่านที่ใช้ในโหมด enable | VARCHAR(45) | | 123456 |
| reg_id | รหัสเขตพื้นที่ | INT | FK | 2 |
| pop_id | รหัสพื้นที่ POP | INT | | 3 |
| rt_id | root id ของอุปกรณ์นี้ อ้างอิงจาก dev_id | SMALLINT(1) | | 2 |

ตารางที่ 3-6 ตาราง host_snmp_cache

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|-----------------|-----------------------------------|--------------|------|-----------------|
| dev_tree_degree | ลำดับชั้นการต่อนับ จาก root id | INT | | |
| dev_id | รหัสอุปกรณ์ | INT | PK | 3 |
| sn_fieldname | ชื่ออ็อบเจกต์ที่เก็บค่า | VARCHAR(30) | PK | ifName |
| sn_vlaue | ค่าจากการสอบถาม | VARCHAR(255) | | Gi0/3 |
| sn_oid | ค่า oid ประจำตัว | VARCHAR(45) | PK | .1.3.6.1.2.1.31 |
| sn_snmp_index | ค่าดัชนีที่ใช้สอบถาม | INT | | 10013 |

ตารางที่ 3-7 ตาราง host_vlan_cache

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|-----------|-----------------------|-------------|------|---------------------|
| hvc_id | รหัสอ้างอิงที่เก็บค่า | INT | PK | 1003 |
| pop_id | รหัสพื้นที่ POP | INT | FK | 1 |
| dev_id | รหัสอุปกรณ์ | INT | FK | 3 |
| hvc_vlan | หมายเลข VLAN | INT | | 300 |
| hvc_port | พอร์ตที่ตั้งค่าไว้ | VARCHAR(30) | | Gi0/2 |
| hvc_date | วันที่เก็บข้อมูล | DATETIME | | 2015-04-21 02:30:55 |

ตารางที่ 3-8 ตาราง host_uplink

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|-------------|---------------------------|-------------|------|----------|
| ul_id | รหัสอ้างอิง | INT | PK | 2 |
| pop_id | รหัสอ้างอิง pop | INT | | 1 |
| rt_id | root สวิตช์ในเครือข่าย | INT | | 1 |
| src_id | dev_id ของโหนดต้นทาง | INT | | 157 |
| src_intf | ชื่อพอร์ตของโหนดต้นทาง | VARCHAR(30) | | Gi0/3 |
| ulnode_id | dev_id ที่เป็นโหนด uplink | INT | | 35 |
| ulnode_intf | พอร์ตของโหนด uplink | VARCHAR(30) | | Gi1/0/12 |

ตารางที่ 3-9 ตาราง log_polling

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|-----------|---|--------------|------|--------------------------------------|
| logid | หมายเลขอ้างอิง log | INT | PK | 001 |
| log_date | วันที่เกิด log | DATETIME | | 2015-03-24 03:02:13 |
| log_name | ชื่อ process ที่สร้าง log | VARCHAR(45) | | readcfg |
| log_msg | ข้อความที่เกิดจากการ ทำงานของระบบ | VARCHAR(200) | | Read config file cbi_m7k_01 start |
| log_level | ระดับความรุนแรง 1 = ข้อมูลปกติ 2 = พบข้อผิดพลาด | TINYINT(2) | | 1 |

ตารางที่ 3-10 ตาราง oui

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|---------------|--------------------|-------------|------|--------------------|
| oui_mac | หมายเลข mac 3 หลัก | VARCHAR(10) | PK | 00:23:04 |
| oui_vendor | ชื่อผู้ผลิต | VARCHAR(30) | | Cisco |
| oui_vendetail | ชื่อเต็มของผู้ผลิต | VARCHAR(30) | | Cisco System, Inc. |

ตารางที่ 3-11 ตาราง rpt_dfs

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|---------------|--|--------------|------|-----------------------------------|
| pop_id | รหัสอ้างอิง pop | INT | | 2 |
| v_num | หมายเลข VLAN | SMALLINT(4) | | 4000 |
| v_name | ชื่อ VLAN | VARCHAR(35) | | Voice-floor2 |
| dfs_unconnect | ชื่อพอร์ตที่ไม่ ต่อเนื่อกันกันด้วย “,” อยู่ในรูปแบบ dev_id:port_name, | VARCHAR(150) | | 157:Gi0/2,354:Gi1/0/12, 178:g3 |

ตารางที่ 3-12 ตาราง rpt_nomaclearn

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|-------------|-------------------------------|-------------|------|---------------------|
| dev_id | รหัสอ้างอิงอุปกรณ์ | VARCHAR(10) | | 157 |
| v_num | หมายเลข VLAN | VARCHAR(30) | | 4000 |
| v_count | จำนวนวันที่นับแล้วมีค่าเป็น 0 | VARCHAR(30) | | 120 |
| last_update | วันที่เวลาเช็คล่าสุด | DATETIME | | 2015-03-26 15:23:03 |

ตารางที่ 3-13 ตาราง rpt_vlancount

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|-------------|----------------------|-------------|------|---------------------|
| dev_id | รหัสอ้างอิงอุปกรณ์ | VARCHAR(10) | PK | 00:23:04 |
| v_num | หมายเลข VLAN | VARCHAR(30) | PK | 4000 |
| v_count | จำนวน MAC ที่นับได้ | VARCHAR(30) | | 300 |
| last_update | วันที่เวลาเช็คล่าสุด | DATETIME | | 2015-03-26 15:23:03 |

ตารางที่ 3-14 ตาราง user

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|--------------|--|-------------|------|---------------------|
| us_id | รหัสอ้างอิงผู้ใช้ | VARCHAR(20) | PK | 001 |
| us_login | ชื่อผู้ใช้ | VARCHAR(30) | | somsak |
| us_passwd | รหัสผ่านผู้ใช้ | VARCHAR(30) | | ***** |
| us_fname | ชื่อหน้าผู้ใช้ | VARCHAR(30) | | |
| us_lname | ชื่อสกุลผู้ใช้ | VARCHAR(30) | | |
| us_email | email | VARCHAR(30) | | somsak@gmail.com |
| us_mobile | เบอร์โทรศัพท์ | VARCHAR(10) | | 0893452220 |
| us_role | สิทธิ์ผู้ใช้นิยามเป็น 1 = User 2 = Admin | INT | | 2 |
| us_status | สถานะผู้ใช้งาน | INT | | Y |
| us_lastlogin | วันเข้าใช้งานล่าสุด | DATETIME | | 2015-03-26 15:23:03 |

ตารางที่ 3-15 ตาราง user_log

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|------------|--|-------------|------|------------------------|
| log_login | ชื่อผู้ใช้งานในระบบ | VARCHAR(10) | PK | somsak |
| log_date | วันที่ล็อกอินเข้าใช้งาน | DATETIME | PK | 2015-03-26 15:23:03 |
| log_ip | หมายเลขไอพีเครื่อง | VARCHAR(30) | | 10.255.100.23 |
| log_result | ผลการ login (1 = ผ่าน, 0 = ไม่ผ่าน) | TINYINT(1) | | 1 |

ตารางที่ 3-16 ตาราง vlans

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|-----------|--------------------|-------------|------|---------------------|
| pop_id | รหัสอ้างอิง pop | VARCHAR(10) | PK | 1 |
| dev_id | รหัสอ้างอิงอุปกรณ์ | VARCHAR(30) | PK | 3 |
| v_num | หมายเลข VLAN | VARCHAR(30) | PK | 4000 |
| v_name | ชื่อ VLAN | VARCHAR(30) | | Internet |
| v_date | วันที่นำเข้า | DATETIME | | 2015-03-26 15:23:03 |

ตารางที่ 3-17 ตาราง vlan_count

| ชื่อฟิลด์ | คำอธิบาย | ชนิดข้อมูล | คีย์ | ตัวอย่าง |
|-----------|---------------------|-------------|------|---------------------|
| dev_id | รหัสอ้างอิงอุปกรณ์ | VARCHAR(10) | PK | 2 |
| v_num | หมายเลข VLAN | VARCHAR(30) | PK | 1500 |
| v_mac | จำนวน MAC ที่นับได้ | VARCHAR(30) | | 308 |
| v_date | วันที่เช็คล่าสุด | | PK | 2015-03-26 15:23:03 |

การหาค่า OID

ขั้นตอนนี้เป็นการศึกษาเพื่อหาค่า OID ที่จำเป็นในการออกแบบระบบ เนื่องจากเครือข่ายที่ทำการศึกษามีการใช้สวิตช์ต่างยี่ห้อกัน ค่า OID บางค่าสามารถใช้งานร่วมกันได้ แต่ยังมีบางค่าที่ผู้ผลิตอุปกรณ์แต่ละรายมีรูปแบบการใช้ OID ที่แตกต่างกัน ซึ่งในการออกแบบระบบนี้ต้องการเก็บข้อมูลการทำงานของอุปกรณ์ ที่ประกอบด้วย 3 ค่าหลักต่อไปนี้

1. การหาหมายเลข VLAN และชื่อ
2. การหาพอร์ตที่เป็นสมาชิกของ VLAN
3. การหาตาราง MAC address

การศึกษานี้ทำการเก็บตัวอย่างจากข้อมูลสวิตช์ 3 ยี่ห้อ คือ Cisco, Huawei และ ZTE

1. OID VLAN สวิตช์ Cisco

ข้อมูลที่เกี่ยวข้องกับ VLAN จะอยู่ใน MIB ชื่อ CISCO-VTP-MIB และ BRIDGE-MIB

1.1 การหาหมายเลข VLAN และชื่อ

ตัวอย่างการสอบถามหมายเลข VLAN ของสวิตช์ยี่ห้อ Cisco จะมีอ็อบเจกต์ที่เกี่ยวข้องกับ VLAN ซึ่งอยู่ภายใต้อ็อบเจกต์ vtpVlanEntry (OID .1.3.6.1.4.1.9.9.46.1.3.1.1) โดยอ็อบเจกต์ที่รายงานชื่อและหมายเลข VLAN คือ vtpVlanName (OID .1.3.6.1.4.1.9.9.46.1.3.1.1.4) สำหรับข้อมูลโครงสร้าง MIB ของ Cisco สามารถหาข้อมูลเพิ่มเติมได้จาก <http://tools.cisco.com/Support/SNMP>

```
$snmpwalk -v2c -On -c public 10.236.0.230 .1.3.6.1.4.1.9.9.46.1.3.1.1.4
.1.3.6.1.4.1.9.9.46.1.3.1.1.4.1.1 = STRING: "default"
.1.3.6.1.4.1.9.9.46.1.3.1.1.4.1.8 = STRING: "lan,pfsense"
.1.3.6.1.4.1.9.9.46.1.3.1.1.4.1.49 = STRING: "nms49"
.1.3.6.1.4.1.9.9.46.1.3.1.1.4.1.107 = STRING: "opnet"
.1.3.6.1.4.1.9.9.46.1.3.1.1.4.1.109 = STRING: "nms,nec-fttx"
.1.3.6.1.4.1.9.9.46.1.3.1.1.4.1.116 = STRING: "nms,cot"
.1.3.6.1.4.1.9.9.46.1.3.1.1.4.1.302 = STRING: "nms,fttx(pty_v103)"
```

ภาพที่ 3-8 การหาหมายเลข VLAN และชื่อของสวิตช์ Cisco

จากภาพที่ 3-8 แสดงตัวอย่างการใช้เครื่องมือ Net-SNMP ด้วยคำสั่ง snmpwalk เพื่อสอบถามชื่อและหมายเลข VLAN ของสวิตช์หมายเลขไอพี 10.236.0.230 ซึ่งหมายเลข VLAN จะอยู่ในหลักสุดท้ายของ OID ของแต่ละบรรทัด

1.2 การหาพอร์ตสมาชิกของแต่ละ VLAN

สำหรับพอร์ตสมาชิกของ VLAN สวิตช์ Cisco จะใช้อ็อบเจกต์ชื่อ

dot1dBasePortIfIndex (OID .1.3.6.1.2.1.17.1.4.1.2) โดยวิธีการสอบถาม เมื่อต้องการรายชื่อพอร์ตที่เป็นสมาชิก VLAN ใดให้ใช้หมายเลข VLAN นั้น ต่อท้าย Community string ในรูปแบบ *Community-string@Vlan-id* เช่น ตัวอย่างในภาพที่ 3-9 เป็นการสอบถามว่า VLAN 104 ถูกตั้งค่าไว้ที่พอร์ตใดบ้าง คำสั่งที่ใช้จึงเป็น

```
snmpwalk -c public@104 <หมายเลขไอดี>.1.3.6.1.2.1.17.1.4.1.2
```

(ตัวอย่างนี้ที่อุปกรณ์มีการตั้งค่า Community string คือ public)

```
$snmpwalk -v2c -On -c public@104 10.236.0.230.1.3.6.1.2.1.17.1.4.1.2
.1.3.6.1.2.1.17.1.4.1.2.11 = INTEGER: 10111
.1.3.6.1.2.1.17.1.4.1.2.13 = INTEGER: 10113
.1.3.6.1.2.1.17.1.4.1.2.28 = INTEGER: 10128
```

ภาพที่ 3-9 จำนวนพอร์ตสมาชิกของ VLAN 104 ในรูปดัชนี

ผลลัพธ์ที่ได้ในภาพ 3-9 คือหมายเลขพอร์ตที่อยู่ในรูปของดัชนี (ifIndex) ซึ่งต้องนำค่าที่ได้มาแปลงต่อด้วยอ็อบเจกต์ifName (OID .1.3.6.1.2.1.31.1.1.1.1) จึงจะแสดงชื่อพอร์ตนั้น ๆ จากตัวอย่างมีการตอบกลับมาเป็นตัวเลข 3 ค่า คือ 10111, 10113 และ 10128 เมื่อนำค่าเหล่านี้ไปสอบถามด้วย snmpget จะได้ชื่อพอร์ต ดังตัวอย่างในภาพที่ 3-10

```
$snmpget -v2c -On -c public 10.236.0.230.1.3.6.1.2.1.31.1.1.1.1.10111
.1.3.6.1.2.1.31.1.1.1.1.10111 = STRING: Gi0/11
$snmpget -v2c -On -c public 10.236.0.230 .1.3.6.1.2.1.31.1.1.1.1.10113
.1.3.6.1.2.1.31.1.1.1.1.10113 = STRING: Gi0/13
$snmpget -v2c -On -c public 10.236.0.230 .1.3.6.1.2.1.31.1.1.1.1.10128
.1.3.6.1.2.1.31.1.1.1.1.10128 = STRING: Gi0/28
```

ภาพที่ 3-10 การแปลงหมายเลขดัชนีให้อยู่ในรูปแบบของชื่อ

1.3 การหาตาราง MAC address

อ็อบเจกต์ dot1dTpFdbAddress (OID .1.3.6.1.2.1.17.4.3.1.1) ใช้สำหรับสอบถามค่า MAC address ที่เรียนรู้มาจากพอร์ตต่าง ๆ ของสวิตช์ (เป็น Unicast MAC address) โดยสามารถระบุ VLAN ที่ต้องการสอบถามได้ เช่น หากต้องการรู้หมายเลข MAC address ของ VLAN 104 รูปแบบคำสั่งที่ใช้แสดงดังภาพที่ 3-11 ผลลัพธ์ที่ได้เป็นค่า OID ตามด้วยเลขขนาด 6 ไบต์คั่นด้วยจุด หากนำมาแปลงเป็นเลขฐาน 16 จะได้ค่าเท่ากับฝั่งขวา แต่ค่าที่ได้เป็นเพียงค่าของ MAC address อย่างเดียว ไม่ได้แสดงถึงหมายเลขพอร์ตที่เรียนรู้เข้ามา

```
$snmpwalk -v2c -On -c public@104 10.236.0.230 .1.3.6.1.2.1.17.4.3.1.1
.1.3.6.1.2.1.17.4.3.1.1.0.5.101.113.215.218= Hex-STRING:00 05 65 71 D7 DA
.1.3.6.1.2.1.17.4.3.1.1.0.9.107.139.83.224= Hex-STRING:00 09 6B 8B 53 E0
.1.3.6.1.2.1.17.4.3.1.1.0.12.66.89.227.138= Hex-STRING:00 0C 42 59 E3 8A
.1.3.6.1.2.1.17.4.3.1.1.0.27.13.236.11.0= Hex-STRING:00 1B 0D EC 0B 00
.1.3.6.1.2.1.17.4.3.1.1.0.31.41.215.241.212= Hex-STRING:00 1F 29 D7 F1 D4
```

ภาพที่ 3-11 หมายเลข MAC address ตาม VLAN 104

ดังนั้นหากต้องการทราบว่า MAC address นั้น ๆ เรียนรู้เข้ามาจากพอร์ตใด ต้องใช้อ็อบเจกต์ที่ชื่อ dot1dTpFdbPort (OID .1.3.6.1.2.1.17.4.3.1.2) แต่ค่าที่ได้คือหมายเลข Bridge port เพื่อให้ได้ชื่อพอร์ตที่ถูกต้อง จะต้องทำตามขั้นตอนดังนี้

- แปลงค่าจาก Bridge port ให้เป็นหมายเลข ifIndex
- แปลงค่าจาก ifIndex ให้เป็น ifName

ดังภาพที่ 3-12 ตัวอย่างการหา MAC address และการหาค่า ifName เพื่อให้ได้ชื่อพอร์ตที่ง่ายต่อการจดจำ

```
$snmpwalk -v2c -On -c public@104 10.236.0.230 .1.3.6.1.2.1.17.4.3.1.2
.1.3.6.1.2.1.17.4.3.1.2.0.5.101.113.201.249 = INTEGER: 28
.1.3.6.1.2.1.17.4.3.1.2.0.9.107.139.83.224 = INTEGER: 28
.1.3.6.1.2.1.17.4.3.1.2.0.12.66.89.227.138 = INTEGER: 28
.1.3.6.1.2.1.17.4.3.1.2.0.27.13.236.11.0 = INTEGER: 28
.1.3.6.1.2.1.17.4.3.1.2.0.30.11.115.106.124 = INTEGER: 28
$snmpget -v2c -On -c public 10.236.0.230 .1.3.6.1.2.1.17.1.4.1.2.28
.1.3.6.1.2.1.17.1.4.1.2.28 = INTEGER: 10128
$snmpget -v2c -On -c public 10.236.0.230 .1.3.6.1.2.1.31.1.1.1.1.10128
.1.3.6.1.2.1.31.1.1.1.1.10128 = STRING: Gi0/28
```

ภาพที่ 3-12 หมายเลข MAC address และหมายเลขพอร์ตที่เรียนรู้เข้ามา

2. OID VLAN สวิตช์ Huawei

สำหรับสวิตช์ยี่ห้อ Huawei ที่ใช้ทำการศึกษาคือเป็นตระกูล S5300 รุ่น S5328C-EI-24S โดยข้อมูลที่เกี่ยวข้องกับ โครงสร้างของ MIB สามารถศึกษาเพิ่มเติมได้ที่ <http://support.huawei.com/enterprise/productsupport> ชื่ออ็อบเจกต์ที่เกี่ยวข้องกับ VLAN จะอยู่ในกลุ่มของ MIB ที่ชื่อ HUAWEI-L2VLAN-MIB

2.1 การหาหมายเลข VLAN และชื่อ

การสอบถามชื่อและหมายเลข VLAN จะใช้อ็อบเจกต์ hwL2VlanDescr (OID .1.3.6.1.4.1.2011.5.25.42.3.1.1.1.2) ผลลัพธ์ที่อุปกรณ์ตอบกลับมีลักษณะเดียวกับสวิตช์ Cisco เช่นในภาพที่ 3-13 แสดงการใช้คำสั่ง snmpwalk เพื่อหาหมายเลข VLAN และชื่อของ VLAN จากสวิตช์ที่มีหมายเลขไอพี 10.236.74.252 (หมายเลขไอพีสำหรับการจัดการ) และมีค่า community string คือ "public"

```
$snmpwalk -v2c -c public -On 10.236.74.252
.1.3.6.1.4.1.2011.5.25.42.3.1.1.1.2
.1.3.6.1.4.1.2011.5.25.42.3.1.1.1.2.1= STRING:"VLAN 0001"
.1.3.6.1.4.1.2011.5.25.42.3.1.1.1.2.34= STRING:"nms,forth160k"
.1.3.6.1.4.1.2011.5.25.42.3.1.1.1.2.111= STRING:"voice,msan-forth"
.1.3.6.1.4.1.2011.5.25.42.3.1.1.1.2.112 = STRING:"VLAN 0112"
.1.3.6.1.4.1.2011.5.25.42.3.1.1.1.2.113 = STRING:"VLAN 0113"
.1.3.6.1.4.1.2011.5.25.42.3.1.1.1.2.3205 = STRING:"NikhomPinThong1"
.1.3.6.1.4.1.2011.5.25.42.3.1.1.1.2.3841 = STRING:"VLAN 3841"
```

ภาพที่ 3-13 การสอบถามหมายเลข VLAN และชื่อ

2.2 การหาพอร์ตสมาชิกของแต่ละ VLAN

ข้อมูล VLAN ของพอร์ตที่เป็นสมาชิก จะใช้อ็อบเจกต์ชื่อ hwL2VlanPortList (OID .1.3.6.1.4.1.2011.5.25.42.3.1.1.1.3) ซึ่งเมื่อใช้คำสั่ง snmpwalk สอบถาม จะแสดงหมายเลข VLAN ทั้งหมดที่ตั้งค่าไว้ในสวิตช์ พร้อมตำแหน่งพอร์ตสมาชิกของแต่ละ VLAN ซึ่งอยู่ในรูปแบบเลขฐาน 16 จะต้องแปลงให้เป็นเลขฐานสอง (แปลงเป็นบิตเวกเตอร์) จึงจะได้ตำแหน่งของพอร์ตที่แท้จริง โดยบิตที่มีค่าเป็น 1 หมายถึง ตำแหน่งพอร์ตที่เป็นสมาชิกของ VLAN นั้น ผลลัพธ์ดังภาพที่ 3-14

```

$snmpwalk -v2c -On -c public
10.236.74.252.1.3.6.1.4.1.2011.5.25.42.3.1.1.1.3
.1.3.6.1.4.1.2011.5.25.42.3.1.1.1.3.1 = Hex-STRING: 1F FF FO 00 00 00
00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00
.1.3.6.1.4.1.2011.5.25.42.3.1.1.1.3.34 = Hex-STRING: 10 00 00 80 00 00
00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00
.1.3.6.1.4.1.2011.5.25.42.3.1.1.1.3.112 = Hex-STRING: 60 00 08 80 00 00
00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00
.1.3.6.1.4.1.2011.5.25.42.3.1.1.1.3.3205 = Hex-STRING: 10 00 00 80 00
00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00

```

ภาพที่ 3-14 พอร์ตที่เป็นสมาชิกแต่ละ VLAN ที่อยู่ในรูปแบบเลขฐาน 16

จากภาพที่ 3-14 ตัวอย่างการหาดำแหน่งพอร์ตที่เป็นสมาชิกของ VLAN 112 ซึ่งมีค่าผลเป็นเลขฐาน 16 ดังนี้

60 00 08 80 00 00 ...

เมื่อนำมาแปลงให้อยู่ในเลขฐานสอง จะได้

01100000 00000000 00001000 1000000 00000000 (เลขฐานสอง)

0 8 16 24 (ตำแหน่งบิต)

หากนับตามตำแหน่งบิตที่มีค่าเป็น 1 โดยเริ่มต้นที่ 0 จะได้ตำแหน่ง 1, 2, 20 และ 24 ดังนั้นหมายเลขพอร์ตที่เป็นสมาชิกของ VLAN 112 ตามตัวอย่างนี้คือพอร์ต Gi0/0/1, Gi0/0/2, Gi0/0/20 และ Gi0/0/24 เมื่อนำไปตรวจสอบกับคำสั่งแบบ Command line ในสวิตช์เพื่อเปรียบเทียบกับซึ่งได้ผลของคำสั่งดังในภาพที่ 3-15

```
[pty_bnp_hw1]display vlan 112
VLAN ID   Type           Status           MAC Learning
-----
112       common        enable          enable
-----
Tagged    Port: GigabitEthernet0/0/1      GigabitEthernet0/0/2
          GigabitEthernet0/0/20        GigabitEthernet0/0/24
-----
Interface           Physical
GigabitEthernet0/0/1  UP
GigabitEthernet0/0/2  DOWN
GigabitEthernet0/0/20 DOWN
GigabitEthernet0/0/24 UP
```

ภาพที่ 3-15 การใช้คำสั่งแบบ Command-line เพื่อเปรียบเทียบกับการใช้ SNMP

2.3 การหาตาราง MAC address

การเรียกดูข้อมูล MAC address จะใช้อ็อบเจกต์ชื่อ hwDynFdbPort (OID .1.3.6.1.4.1.2011.5.25.42.2.1.3.1.4) เมื่อใช้คำสั่ง snmpwalk ดังภาพที่ 3-16 ค่าที่ตอบกลับมาเป็นกลุ่มของ OID ซึ่งประกอบด้วยหมายเลข MAC address ที่แสดงเป็นเลขฐานสิบ ตามด้วยหมายเลข VLAN และปิดท้ายด้วย “.1.48” ส่วนค่าที่ได้จากแต่ละ OID คือหมายเลขพอร์ต ifIndex ที่รับ MAC address นั้นเข้ามา สังเกตว่าเราไม่สามารถระบุ VLAN ที่ต้องการสอบถามได้ ค่าที่ตอบกลับมาเป็นค่า MAC address ทั้งหมดที่มีอยู่ในสวิตช์

จากตัวอย่างชุด OID ที่ตอบกลับมาเช่น

.1.3.6.1.4.1.2011.5.25.42.2.1.3.1.4.244.236.56.223.53.100.3841.1.48 = INTEGER: 641

```
$snmpwalk -On -v2c -c public 10.236.74.252
.1.3.6.1.4.1.2011.5.25.42.2.1.3.1.4
.1.3.6.1.4.1.2011.5.25.42.2.1.3.1.4.244.236.56.223.53.100.3841.1.48 =
INTEGER: 641
.1.3.6.1.4.1.2011.5.25.42.2.1.3.1.4.0.28.203.91.54.146.34.1.48 = INTEGER:
3585
.1.3.6.1.4.1.2011.5.25.42.2.1.3.1.4.216.93.76.184.200.226.3841.1.48 =
INTEGER: 641
.1.3.6.1.4.1.2011.5.25.42.2.1.3.1.4.248.26.103.115.81.206.3841.1.48 =
INTEGER: 641
```

ภาพที่ 3-16 การหาที่อยู่ MAC และพอร์ตที่เรียนรู้

ภาพที่ 3-16 ส่วนที่ตัดจาก OID คือ 244.236.56.223.53.100.3841.1.48 ซึ่งใน 6 ไบต์แรกจะเป็นค่าของ mac-address ส่วน 1 ไบต์ถัดมาก็คือหมายเลข VLAN และมี ifIndex เท่ากับ 641 ซึ่งต้องใช้ snmpget หาค่าจาก OID ifDescr (.1.3.6.1.2.1.2.2.1.2) จึงจะได้เป็นชื่อพอร์ตที่ใช้งานจริง

```
$snmpget -Ofn -v 2c -c public 10.236.74.252 .1.3.6.1.2.1.2.2.1.2.641
.1.3.6.1.2.1.2.2.1.2.641 = STRING: GigabitEthernet0/0/1
```

ภาพที่ 3-17 การหาชื่อพอร์ต (ifDescr) จากหมายเลข ifIndex

ชุดตัวเลข 244.236.56.223.53.100 เมื่อแปลงให้อยู่ในเลขฐาน 16 จะมีค่าเท่ากับ f4.ec.38.df.35.64 ซึ่งเมื่อทดลองเปรียบเทียบจากการใช้คำสั่งแบบ Command-line ผลลัพธ์ที่ได้มีค่าตรงกัน ดังตัวอย่างในภาพที่ 3-18

```
[pty_bnp_hw1]
[pty_bnp_hw1]display mac-address dynamic
MAC Address      VLAN/VSI      Port
-----
f4ec-38df-3564  3841          GigabitEthernet0/0/1
d85d-4cb8-c8e2  3841          GigabitEthernet0/0/1
001c-cb5b-3230  34            GigabitEthernet0/0/24
0030-48f4-5d93  112           GigabitEthernet0/0/24
f81a-6773-51ce  3841          GigabitEthernet0/0/1
286e-d4a5-0075  113           GigabitEthernet0/0/24
001c-cb5b-2b41  34            GigabitEthernet0/0/24
0021-912b-fa43  3841          GigabitEthernet0/0/1
286e-d4a5-0009  113           GigabitEthernet0/0/24
286e-d4a5-002d  113           GigabitEthernet0/0/24
0030-48f4-1a17  113           GigabitEthernet0/0/24
1078-d278-c9ca  112           GigabitEthernet0/0/24
```

ภาพที่ 3-18 ผลจากการใช้คำสั่งแบบ command-line เพื่อแสดงที่อยู่ MAC

3. OID VLAN สวิตช์ ZTE

ตัวอย่างสวิตช์ ZTE ที่ใช้ทำการศึกษาคือ รุ่น 5900 ZXR10

3.1 การหาหมายเลข VLAN และชื่อ

สวิตช์ ZTE จัดเก็บหมายเลข VLAN และชื่อภายใต้ OID.1.3.6.1.4.1.3902.3.102.

เมื่อทดลองใช้คำสั่ง snmpwalk ให้ผลลัพธ์ดังภาพที่ 3-19 ซึ่งเหมือนกับ Cisco และ Huawei

```
$snmpwalk -v2c -On -c public 10.251.157.201
.1.3.6.1.4.1.3902.3.102.1.1.1.6
.1.3.6.1.4.1.3902.3.102.1.1.1.6.1 = STRING:"VLAN0001"
.1.3.6.1.4.1.3902.3.102.1.1.1.6.9 = STRING:"nex-sw"
.1.3.6.1.4.1.3902.3.102.1.1.1.6.29 = STRING:"Test-Traffic"
.1.3.6.1.4.1.3902.3.102.1.1.1.6.34 = STRING:"NMS_Dslam"
.1.3.6.1.4.1.3902.3.102.1.1.1.6.36 = STRING:"nms-msan-huawei (577K) "
.1.3.6.1.4.1.3902.3.102.1.1.1.6.49 = STRING:"nms49"
.1.3.6.1.4.1.3902.3.102.1.1.1.6.104 = STRING:"nmsdev-dsl"
.1.3.6.1.4.1.3902.3.102.1.1.1.6.105 = STRING:"NMS105"
.1.3.6.1.4.1.3902.3.102.1.1.1.6.106 = STRING:"nms106"
.1.3.6.1.4.1.3902.3.102.1.1.1.6.111 = STRING:"Voip"
```

ภาพที่ 3-19 การหาหมายเลข VLAN และชื่อของสวิตช์ ZTE

3.2 การหาพอร์ตสมาชิกของแต่ละ VLAN

OID ที่ใช้สำหรับหาพอร์ตที่เป็นสมาชิกแต่ละ VLAN คือ .1.3.6.1.4.1.3902.3.102.

1.1.1.17 ซึ่งค่าที่ได้อยู่ในรูปแบบที่คล้ายกันกับสวิตช์ Huawei คือเลขฐาน 16 ดังในภาพที่ 3-20

```
$snmpwalk -v2c -On -c public 10.251.157.201
.1.3.6.1.4.1.3902.3.102.1.1.1.17
.1.3.6.1.4.1.3902.3.102.1.1.1.17.1 = Hex-STRING: 00 00 00 00 00 00 00 00
.1.3.6.1.4.1.3902.3.102.1.1.1.17.9 = Hex-STRING: 41 80 01 00 00 00 00 00
.1.3.6.1.4.1.3902.3.102.1.1.1.17.29 = Hex-STRING: 00 84 00 00 00 00 00 00
.1.3.6.1.4.1.3902.3.102.1.1.1.17.34 = Hex-STRING: 5C 80 01 00 00 00 00 00
.1.3.6.1.4.1.3902.3.102.1.1.1.17.36 = Hex-STRING: 00 82 00 00 00 00 00 00
```

ภาพที่ 3-20 การหาพอร์ตที่เป็นสมาชิกของแต่ละ VLAN

จากภาพที่ 3-20 เมื่อนำเลขฐาน 16 ที่ได้จาก VLAN 34 แปลงเป็นเลขฐานสองเพื่อหาตำแหน่งของพอร์ต โดยเริ่มต้นนับที่จาก 1 (ของ Huawei เริ่มนับจาก 0)

5C 80 01 00 00

01011100 10000000 00000001 00000000 00000000

เมื่อนับบิต “1” ตามตำแหน่งต่าง ๆ แล้ว ทำให้ได้ตำแหน่งดังต่อไปนี้คือ 2, 4, 5, 6, 9

และ 24 ซึ่งหมายถึง VLAN 34 ของสวิตช์ ZTE มีพอร์ตที่เป็นสมาชิก คือ gei_1/2, gei_1/4, gei_1/5, gei_1/6, gei_1/9 และ gei_1/24

3.3 การหาตาราง mac-address

สวิตช์ ZTE สามารถหาค่า MAC address ที่เรียนรู้จากพอร์ตต่าง ๆ ได้จากค่า OID “1.3.6.1.2.1.17.7.1.2.2.1.2” ถ้าใช้คำสั่ง snmpwalk โดยไม่ระบุหมายเลข VLAN ต่อท้าย จะเป็นการแสดงหมายเลข MAC address ทั้งหมดในระบบ แต่ถ้าต้องการดูเฉพาะ VLAN ที่ต้องการให้เพิ่มหมายเลข VLAN นั้นเข้าไป เช่นตัวอย่างในภาพที่ 3-21 แสดงการหา MAC address และพอร์ตที่รับเข้ามาของ VLAN 34 จึงใช้ OID เป็น .1.3.6.1.2.1.17.7.1.2.2.1.2.34 ค่าที่ตอบกลับมาแสดงดังภาพที่ 3-21

```
$snmpwalk -v2c -On -c public 10.251.157.201.1.3.6.1.2.1.17.7.1.2.2.1.2.34
.1.3.6.1.2.1.17.7.1.2.2.1.2.34.0.27.13.231.159.192 = INTEGER: 11
.1.3.6.1.2.1.17.7.1.2.2.1.2.34.0.28.203.91.0.74 = INTEGER: 7
.1.3.6.1.2.1.17.7.1.2.2.1.2.34.0.28.203.91.21.59 = INTEGER: 8
.1.3.6.1.2.1.17.7.1.2.2.1.2.34.0.28.203.91.43.39 = INTEGER: 11
.1.3.6.1.2.1.17.7.1.2.2.1.2.34.0.28.203.91.43.65 = INTEGER: 11
.1.3.6.1.2.1.17.7.1.2.2.1.2.34.0.28.203.91.43.110 = INTEGER: 11
```

ภาพที่ 3-21 ค่า MAC address ของ VLAN 34 และพอร์ต ifIndex

จากภาพที่ 3-21 ตัวอย่างค่า OID ที่ตอบกลับมีค่าเท่ากับ 0.28.203.91.21.59 เมื่อแปลงเป็นเลขฐาน 16 จะมีค่าเป็น 00.1c.cb.5b.15.3b ซึ่งเป็นหมายเลข MAC address ที่ได้รับเข้ามาจากพอร์ต ifIndex ที่ 8 ดังนั้นเราต้องหาค่า ifIndex ที่ 8 คือชื่อพอร์ตของใด โดยใช้คำสั่ง snmpwalk เพื่อดูค่า ifName จากOID .1.3.6.1.2.1.31.1.1.1.1.1 ดังภาพที่ 3-22

```
$snmpwalk -v2c -On -c public 10.251.157.201.1.3.6.1.2.1.31.1.1.1.1
.1.3.6.1.2.1.31.1.1.1.1.3 = STRING: gei_1/1
.1.3.6.1.2.1.31.1.1.1.1.4 = STRING: gei_1/2
.1.3.6.1.2.1.31.1.1.1.1.5 = STRING: gei_1/3
.1.3.6.1.2.1.31.1.1.1.1.6 = STRING: gei_1/4
.1.3.6.1.2.1.31.1.1.1.1.7 = STRING: gei_1/5
.1.3.6.1.2.1.31.1.1.1.1.8 = STRING: gei_1/6 ← ifIndex 8
.1.3.6.1.2.1.31.1.1.1.1.9 = STRING: gei_1/7
.1.3.6.1.2.1.31.1.1.1.1.10 = STRING: gei_1/8
.1.3.6.1.2.1.31.1.1.1.1.11 = STRING: gei_1/9
.1.3.6.1.2.1.31.1.1.1.1.12 = STRING: gei_1/10
```

ภาพที่ 3-22 การหาค่า ifName เพื่อเทียบกับค่า ifIndex ของสวิตช์ ZTE

จากภาพที่ 3-22 เมื่อเทียบระหว่างค่า ifIndex กับค่า ifName ที่ตอบกลับมา ทำให้รู้ว่า ifIndex 8 คือพอร์ต gei_1/6 จึงกล่าวได้ว่า VLAN 34 มีหมายเลข MAC address “00.1c.cb.5b.15.3b” ซึ่งเรียนรู้มาจากพอร์ตที่ gei_1/6 ของสวิตช์ ZTE ซึ่งหากนำมาเปรียบเทียบกับการใช้คำสั่ง “show mac address vlan 34” ด้วยการ Telnet ไปที่สวิตช์นั้น ผลปรากฏว่ามีค่าตรงกัน

```

cbi_bbg_zte1#
cbi_bbg_zte1#show mac vlan 34
Total MAC address : 27

Flags: vid    --VLAN id,      stc    --static
        per    --permanent,  toS    --to-static
        srF    --source filter, dsF    --destination filter
        time   --day:hour:min:sec

```

| MAC_Address | port | vid | stc | per | toS | srF | dsF |
|-----------------------|----------------|-----|-----|-----|-----|-----|-----|
| 001c.cb5b.3185 | gei_1/9 | 34 | 0 | 0 | 0 | 0 | 0 |
| 001c.cb5b.2b80 | gei_1/9 | 34 | 0 | 0 | 0 | 0 | 0 |
| 001c.cb5b.153b | gei_1/6 | 34 | 0 | 0 | 0 | 0 | 0 |
| 001c.cb5b.3199 | gei_1/9 | 34 | 0 | 0 | 0 | 0 | 0 |
| 001c.cb5b.319c | gei_1/9 | 34 | 0 | 0 | 0 | 0 | 0 |
| 001c.cb5b.38e5 | gei_1/9 | 34 | 0 | 0 | 0 | 0 | 0 |
| 001c.cb5b.360f | gei_1/9 | 34 | 0 | 0 | 0 | 0 | 0 |
| 04da.d214.4360 | gei_1/9 | 34 | 0 | 0 | 0 | 0 | 0 |
| 001c.cb5b.3674 | gei_1/9 | 34 | 0 | 0 | 0 | 0 | 0 |

ภาพที่ 3-23 การใช้คำสั่งแบบ command-line แสดง MAC address VLAN 34

ตารางที่ 3-18 สรุปค่า OID ที่เกี่ยวข้องกับ VLAN ของสวิตช์ยี่ห้อต่าง ๆ

| อ็อบเจกต์ | ยี่ห้อ | OID |
|-------------|--------|--------------------------------------|
| Vlan name | Cisco | 1.3.6.1.4.1.9.9.46.1.3.1.1.4 |
| | Huawei | 1.3.6.1.4.1.2011.5.25.42.3.1.1.1.1.2 |
| | ZTE | 1.3.6.1.4.1.3902.3.102.1.1.1.6 |
| Port member | Cisco | 1.3.6.1.2.1.17.1.4.1.2 |
| | Huawei | 1.3.6.1.4.1.2011.5.25.42.3.1.1.1.1.3 |
| | ZTE | 1.3.6.1.4.1.3902.3.102.1.1.1.17 |
| MACAddress | Cisco | 1.3.6.1.2.1.17.4.3.1.2 |
| | Huawei | 1.3.6.1.4.1.2011.5.25.42.2.1.3.1.4 |
| | ZTE | 1.3.6.1.2.1.17.7.1.2.2.1.2 |

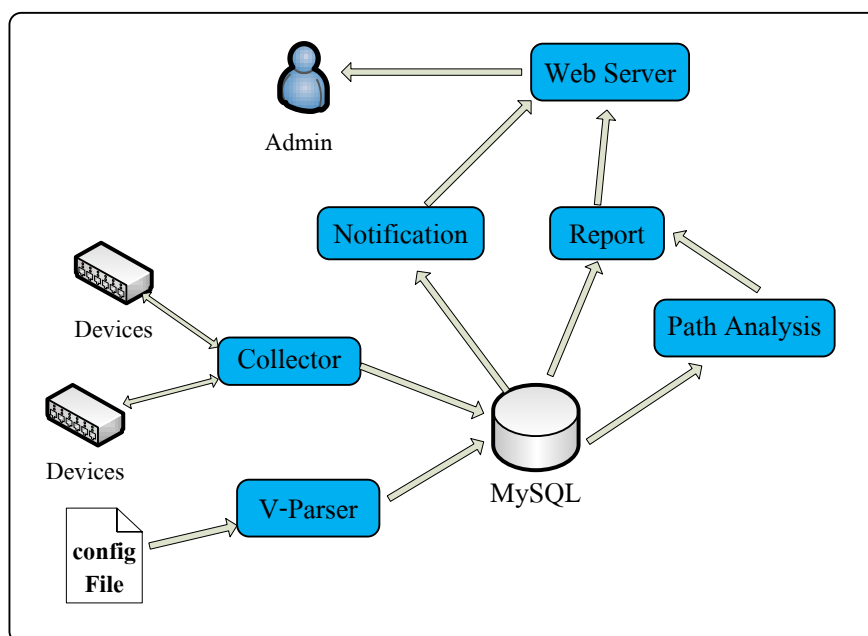
ตารางที่ 3-18 สรุปค่า OID ของสวิตช์ยี่ห้อต่าง ๆ โดยเปรียบเทียบกับอีกเจกต์ที่ต้องการนำไปใช้ ซึ่งจากตัวอย่างวิธีการหาค่าที่เกี่ยวกับ VLAN นอกจากแต่ละยี่ห้อจะใช้ค่า OID ที่แตกต่างกันแล้ว ผลลัพธ์ที่ได้กลับมาจากอุปกรณ์ก็ไม่เหมือนกัน ใช้วิธีการถอดความหมายที่แตกต่างกันไป จึงต้องนำข้อมูลในส่วนนี้ไปใช้ในการออกแบบระบบ

ส่วนของการพัฒนาโปรแกรม

1. ภาพรวมของระบบ

ระบบค้นหาโครงสร้าง VLAN ทำการรวบรวมข้อมูลต่าง ๆ จากอุปกรณ์ในเครือข่าย มาวิเคราะห์ เปรียบเทียบ แจ้งเตือน และแสดงผลผ่านทางเว็บเบราว์เซอร์ เพื่อให้โปรแกรมทำงานได้รวดเร็วและมีประสิทธิภาพจึงต้องมีการแบ่งการทำงานออกเป็นโมดูลย่อย ได้แก่

1.1 Collector คือส่วนที่ทำหน้าที่สอบถามข้อมูลจากอุปกรณ์ด้วยโพรโทคอล SNMP ข้อมูลที่ได้จะถูกจัดเก็บลงฐานข้อมูล MySQL เช่น ข้อมูลหมายเลข VLAN พอร์ตสมาชิกของ VLAN ค่า MAC address รวมไปถึงข้อมูลพื้นฐานทั่วไป เช่น รายชื่อพอร์ต รุ่นและสถานะของอุปกรณ์



ภาพที่ 3-24 การเชื่อมโยงส่วนประกอบของระบบ

1.2 V-Parser เป็นโมดูลที่ใช้สำหรับตรวจสอบโครงสร้างของประโยคที่เกี่ยวข้องกับการตั้งค่า VLAN โดยจะนำไปใช้สกัดข้อมูล VLAN ที่ได้จากไฟล์คอนฟิกของอุปกรณ์ ใช้ในกรณีนี้

ระบบไม่สามารถสอบถามข้อมูลด้วย SNMP ได้ อาจเพราะนโยบายด้านความปลอดภัยต่อตัวอุปกรณ์ จึงไม่เปิดบริการ SNMP ไว้

โดย V-Parser จะทำการดาวน์โหลดไฟล์คอนฟิกจากตัวอุปกรณ์มาเก็บไว้ที่เครื่องแม่ข่ายตามช่วงเวลาที่กำหนด จากนั้นจะอ่านข้อมูลจากไฟล์เหล่านั้น เพื่อสกัดข้อมูลที่เกี่ยวข้องกับ VLAN จัดเก็บลงในฐานข้อมูล เพื่อรอการประมวลผลต่อไป

1.3 Path Analysis ทำหน้าที่ค้นหา VLAN ที่มีเส้นทางไม่ต่อเนื่องกันในเครือข่าย โดยใช้อัลกอริทึมแบบการค้นหาในแนวลึก (Depth first search) โดยแทนจำนวนสวิตช์และพอร์ตที่ช่วยค้นหาสวิตช์และพอร์ตที่ตั้งค่า VLAN ไม่ครบ (ค่า VLAN สูญหาย) ผลลัพธ์ที่ได้จะถูกส่งต่อไปยังโมดูล Report เพื่อเสนอเป็นรายงานให้แก่ผู้ใช้

1.4 Notification เป็นโมดูลทำหน้าที่แจ้งเตือนให้ผู้ใช้ทราบเมื่อผู้ใช้ล็อกอินเข้ามาดูที่หน้าแรกของระบบ เมื่อโมดูลนี้พบค่าเกินกว่าค่าที่ตั้งไว้ในระบบ เช่น จำนวนผู้ใช้ต่อ VLAN หรือความผิดปกติที่รับมาจากโมดูลอื่นเช่น จากโมดูล Path analysis

1.5 Report ทำหน้าที่สรุปรายงานต่าง ๆ จากฐานข้อมูล เนื่องจากข้อมูลในรายงานบางส่วนมีปริมาณมาก การคำนวณเพื่อหาผลสรุปต้องใช้เวลาในการคิวรีนาน โมดูลในส่วนนี้จะช่วยสร้างผลสรุปในภาพรวมเบื้องต้น โดยอัตโนมัติโดยไม่ต้องรอผู้ใช้เรียกถาม ลงในตารางรายงานอำนวยความสะดวก รวดเร็ว ในการดึงข้อมูลรายงานไปใช้งาน

1.6 GUI ส่วนของ user interface ที่แสดงผลผ่านทางบราวเซอร์ เพื่อความสะดวกและรวดเร็วในการพัฒนา ผู้พัฒนาระบบจึงใช้เครื่องมือแบบ Front-end framework ชื่อ Bootstrap ซึ่งข้อดีของการใช้ framework คือช่วยแก้ปัญหาการแสดงผลที่แตกต่างกันของแต่ละบราวเซอร์ซึ่งมักเป็นปัญหาหนึ่งของการพัฒนาโปรแกรมด้วยเว็บ

2. การนำขั้นตอนวิธีค้นหาในแนวลึกมาประยุกต์ใช้

หลังจากเก็บรวบรวมข้อมูลการตั้งค่า VLAN จากสวิตช์ทั้งหมดเรียบร้อยแล้ว ขั้นตอนต่อไปคือการตรวจสอบโครงสร้าง VLAN ที่มีเส้นทางไม่ครบหรือสูญหายเพื่อหาความถูกต้องของการตั้งค่า VLAN ในการศึกษาเราใช้วิธีค้นหาในแนวลึกมาประยุกต์ใช้ โดยการเชื่อมต่อของสวิตช์มีลักษณะเป็นโครงสร้างแบบต้นไม้และพอร์ตที่เป็นสมาชิก VLAN มีลักษณะเทียบเท่าโหนดที่ต้องตรวจสอบหรือทำการท่องไปให้ครบทุกโหนด สามารถแสดงรหัสเทียมดังภาพที่ 3-25

```

initial VLAN = array() // list all VLAN in system

Visited = array()

// set default each Portmember Visited[] = False

foreach VLANmember in VLAN do
    key = node_id.port_id;
    Visited[key] = False;
end for

// start check connected and mark if visited

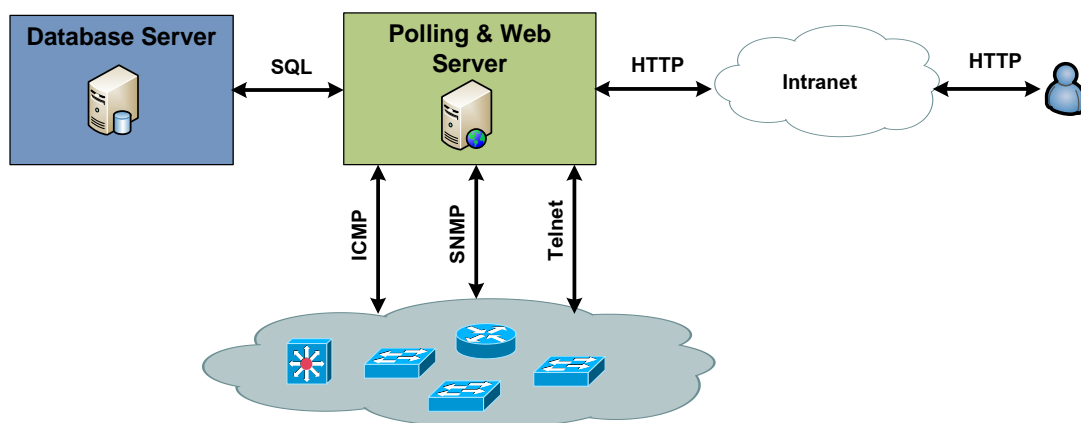
foreach VLANmember do
    current_key = node_id.port_id
    if Visited[current_key] == False
        connected_node[] = Check_adjacent(node_id,port_id); // check and return adjacent node id
        if connected_node[] not empty
            connected_key = connected_node_id.connected_port_id
            if (array_key_exists(connected_key,current_key) Visited[conneted_key] = True;
            else Unconnected[] = connected_key
            end if
            Visited[current_key] = True; //mark current node is visited
        end if
    end for
return Unconnected[];

```

ภาพที่ 3-25 รหัสเทียมที่ใช้ในการหา VLAN ที่สูญหาย

3. โครงสร้างทางกายภาพของระบบ

ภาพที่ 3-26 แนวคิดการออกแบบระบบประกอบด้วยเครื่องแม่ข่าย 2 เครื่องแบ่งหน้าที่การทำงานและวิธีที่ใช้ติดต่อระหว่างเครื่องแม่ข่ายกับเครื่องแม่ข่าย เครื่องแม่ข่ายกับอุปกรณ์และเครื่องแม่ข่ายกับผู้ใช้งาน



ภาพที่ 3-26 แนวคิดการออกแบบระบบค้นหาโครงสร้าง VLAN

บทที่ 4

ผลการดำเนินงาน

การพัฒนาระบบค้นหาโครงสร้าง VLAN เพื่อเป็นเครื่องมือสนับสนุนการจัดการ VLAN ในเครือข่าย ผลจากการดำเนินงานแบ่งออกเป็น 2 หัวข้อ คือ ผลการพัฒนาโปรแกรม และสรุปผลจากการนำโปรแกรมไปใช้งาน

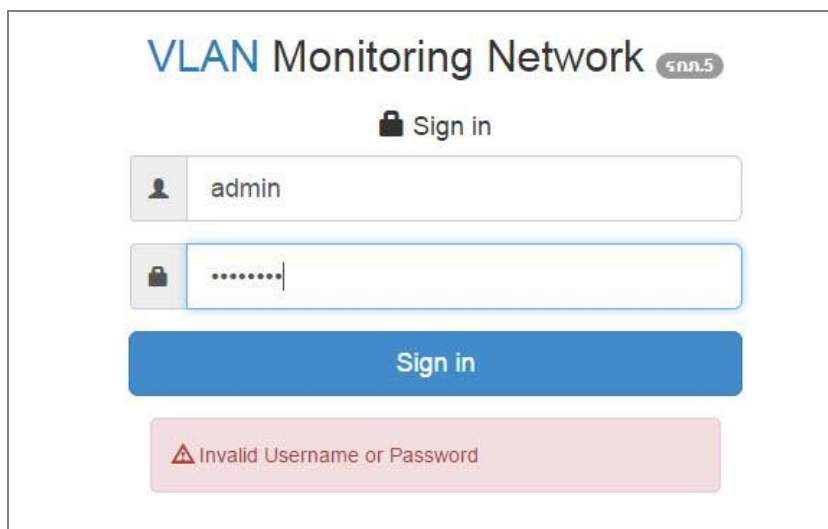
ผลการพัฒนาโปรแกรม

1. แนะนำการใช้งานเบื้องต้น

ในส่วนนี้จะกล่าวถึงวิธีการเข้าสู่ระบบ การเปลี่ยนรหัสผ่าน และวิธีใช้ตารางรายงาน ระบบค้นหาโครงสร้าง VLAN มีส่วนติดต่อผู้ใช้ผ่านทางเว็บเบราว์เซอร์ ผู้ใช้ไม่จำเป็นต้องติดตั้งโปรแกรมอื่นเพิ่มเติม เพียงมีชื่อผู้ใช้และรหัสผ่านที่ออกให้โดยผู้ดูแลระบบก็สามารถใช้งานได้

1.1 การเข้าสู่ระบบ

เริ่มต้นการเข้าระบบโดยพิมพ์ url `http://server_ip/vmon` ที่เว็บเบราว์เซอร์ จะแสดงหน้าจอคังภาพที่ 4-1 หน้าจอยืนยันตัวตนและตรวจสอบสิทธิ์ หากมีการกรอกชื่อผู้ใช้หรือรหัสผ่าน ผิดจะปรากฏข้อความเตือนในกรอบสีแดงด้านล่าง โดยสิทธิ์การใช้งานแบ่งออกเป็น 2 ระดับคือ ผู้ดูแลระบบ (Admin) และผู้ใช้ทั่วไป (Viewer)



ภาพที่ 4-1 หน้าจอตรวจสอบสิทธิ์เข้าใช้งาน

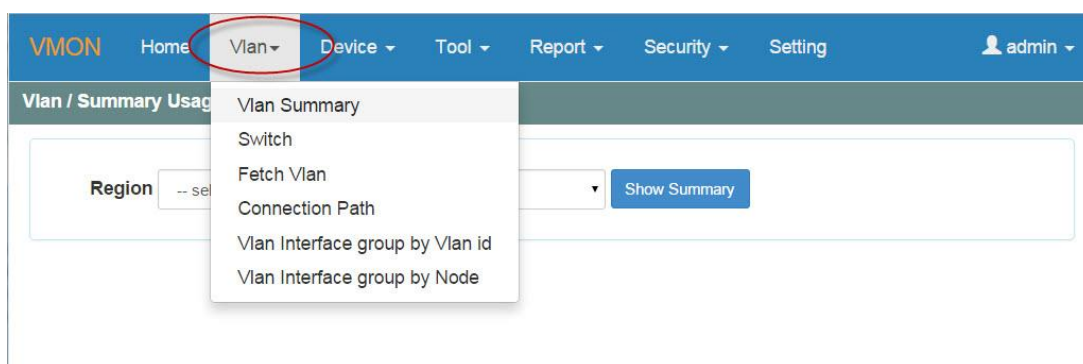
1.2 เมนูควบคุม

เมนูหลักที่ใช้เข้าถึงการทำงานของระบบแสดงดังภาพที่ 4-2 ประกอบด้วยเมนูทั้งสิ้น 8 เมนู ได้แก่ Home, Vlan, Device, Tool, Report, Security, Setting, และ User Profile ผู้ใช้ที่ได้รับสิทธิ์ “ผู้ใช้ทั่วไป” อาจไม่เห็นบางเมนูตามที่แสดงในภาพที่ 4-2 เนื่องจากระดับสิทธิ์ในการเข้าถึงต่างกัน



ภาพที่ 4-2 เมนูหลักของระบบค้นหาโครงสร้าง VLAN

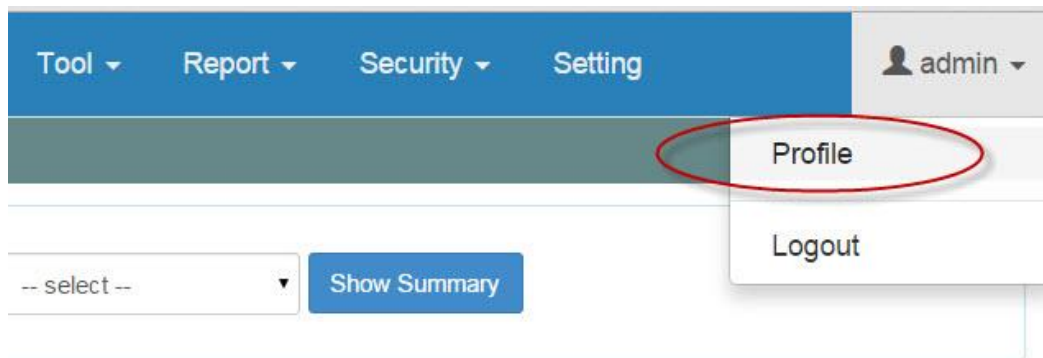
ภาพที่ 4-3 แสดงตัวอย่างเมื่อผู้ใช้เลือกที่เมนูหลัก “Vlan” จะปรากฏเมนูย่อยดังภาพ



ภาพที่ 4-3 เมนูย่อยของเมนู Vlan

1.3 การเปลี่ยนรหัสผ่าน

ผู้ใช้งานควรเปลี่ยนรหัสผ่านทันทีหลังจากเข้าระบบในครั้งแรก วิธีเปลี่ยนรหัสผ่านหรือข้อมูลส่วนตัว ทำได้โดยเลือกที่เมนูมุมด้านขวา ซึ่งเป็นชื่อของผู้ใช้งาน จากนั้นเลือกที่เมนู “Profile” ดังภาพที่ 4-4



ภาพที่ 4-4 การเปลี่ยนรหัสผ่าน

ภาพที่ 4-5 แสดงหน้าจอข้อมูลส่วนตัวของผู้ใช้งานการเปลี่ยนรหัสผ่านให้ผู้ใช้งานใส่รหัสผ่านใหม่ลงในช่อง “Password” และยืนยันรหัสผ่านอีกครั้งในช่อง “Re-enter Password” จากนั้นกดปุ่ม “Update”

 A screenshot of a 'User Profile' form. The form has a title bar with a close button (X). The fields are:

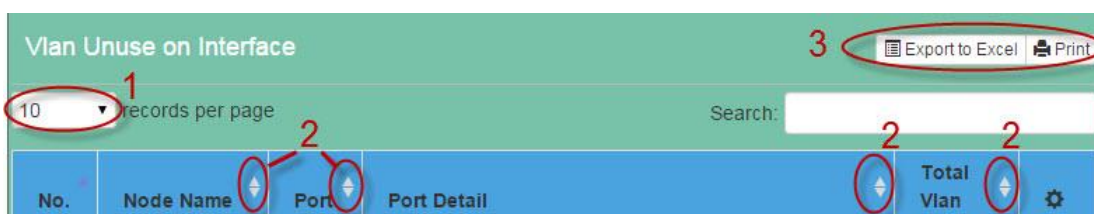
- Username: admin
- First Name: System
- Last Name: Admin2
- Password: (empty field with a cursor)
- Re-enter Password: (empty field)
- Email: (empty field)
- Mobile: 038322256
- User Group: Admin (dropdown menu)
- Division: ชลบุรี (dropdown menu)

 At the bottom right, there are two buttons: 'Cancel' (orange) and 'Update' (blue).

ภาพที่ 4-5 การเปลี่ยนข้อมูลผู้ใช้งานและรหัสผ่าน

1.4 การใช้ตารางรายงาน

ข้อมูลที่นำเสนอในรูปแบบตารางจะใช้เครื่องมือเสริมชื่อ DataTables (www.datatables.net) ช่วยในการแสดงผล ดังภาพที่ 4-6 เมื่อผู้ใช้เลือก 1) จำนวนแถวที่ต้องการแสดงในหนึ่งหน้า 2) การเรียงลำดับข้อมูลโดยเลือกที่ส่วนหัวของคอลัมน์ 3) สามารถส่งข้อมูลออกในรูปแบบของไฟล์ Excel หรือพิมพ์ออกทางเครื่องพิมพ์และผู้ใช้สามารถคัดกรองค่าที่มีในตารางโดยป้อนค่าที่ต้องการคัดกรองลงในช่อง Search



ภาพที่ 4-6 ส่วนหัวของตารางข้อมูล

ภาพที่ 4-7 ส่วนท้ายของตารางจะบอกจำนวนแถวทั้งหมดของข้อมูลนั้น และมีหมายเลขหน้าสำหรับควบคุมการเข้าถึงแต่ละหน้าของตาราง หากข้อมูลมีมากกว่า 5 หน้า ผู้ใช้สามารถกดปุ่ม “Next” เพื่อแสดงผลหน้าถัดไป และกดปุ่ม “Previous” เพื่อแสดงผลย้อนหลัง



ภาพที่ 4-7 ส่วนควบคุมตารางส่วนท้าย

1.5 หน้าจอแสดงผลรวม

หน้าจอหลักของระบบเมื่อผู้ใช้เข้าสู่ระบบสำเร็จแล้ว จะปรากฏหน้าจอแสดงผลรวม ดังภาพที่ 4-8 เป็นการสรุปรายงานแบบย่อโดยแบ่งออกเป็นส่วนย่อย เพื่อให้ผู้ใช้งานสังเกตเห็นได้ง่าย สามารถเห็นข้อมูลการทำงานของระบบได้จากหน้าจอเดียว

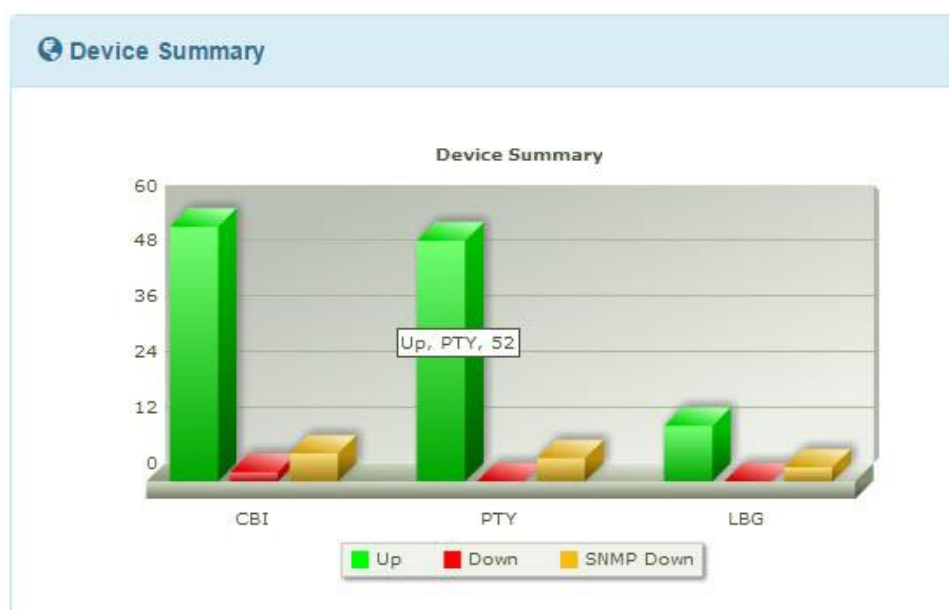
จากภาพที่ 4-8 สามารถอธิบายแต่ละส่วนของหน้าจอได้ดังนี้



ภาพที่ 4-8 ลักษณะของหน้าจอแสดงผลรวม

1.5.1 ส่วนสรุปสถานะสวิตช์ (Device Summary)

เป็นการแสดงสถานะของสวิตช์จากการสำรวจโดยเครื่องแม่ข่าย



ภาพที่ 4-9 สรุปสถานะของสวิตช์ทั้งหมดในระบบ

1.5.2 ส่วนสรุป MAC ต่อ VLAN

ภาพที่ 4-10 เป็นการแสดงความหนาแน่นของ MAC address ต่อ VLAN โดยเลือกสวิตช์ที่มี VLAN หนาแน่นสูงสุด 10 อันดับมาแสดงเช่น VLAN 460 มีความหนาแน่นมากที่สุด (มีที่อยู่ MAC ทั้งหมด 305 ที่อยู่)



ภาพที่ 4-10 สวิตช์ที่มี MAC หนาแน่น 10 อันดับ

1.5.3 ส่วนสรุป VLAN ต่อพอร์ต

ภาพที่ 4-11 แสดงรายชื่อสวิตช์และพอร์ตที่มี VLAN เป็นสมาชิกสูงสุด 10 อันดับ เพื่อแสดงให้เห็นว่าพอร์ตของสวิตช์ตัวใดประกาศ VLAN ออกไปมากที่สุดเช่น ที่ Interface Po12 ของสวิตช์ amt_m3k_03 มีจำนวน VLAN มากถึง 416 VLAN ผู้ดูแลเครือข่ายควรตรวจสอบการตั้งค่า VLAN ที่พอร์ตนี้ว่าถูกต้องหรือไม่

| ✦ Top 10 Vlan per Interface | | | |
|-----------------------------|-----------------|-----------|------------|
| Node Name | IP Address | Interface | จำนวน Vlan |
| amt_m3k_03 | 10.236.72.3 | Po12 | 416 |
| cbi_f7k_01 | 118.174.224.129 | Te9/3 | 217 |
| lbg_m3k_02 | 10.236.12.195 | Gi1/0/12 | 207 |
| hik_m3k_02 | 10.236.12.197 | Gi1/0/12 | 207 |
| hik_m3k_02 | 10.236.12.197 | Gi1/0/10 | 207 |
| bwn_m3k_02 | 10.236.12.199 | Gi1/0/10 | 207 |

ภาพที่ 4-11 พอร์ตของสวิตช์ที่มี VLAN ประกาศไว้สูงสุด 10 อันดับ

1.5.4 สรุป VLAN ที่ไม่มี MAC

ภาพที่ 4-12 แสดงสวิตช์ที่มี VLAN ซึ่งไม่ได้เรียนรู้ที่อยู่ MAC เลยภายในระยะเวลาที่กำหนด ซึ่งคาดว่าจะเป็น VLAN ที่ไม่มีการใช้งานเลยภายใน 30 วัน

| ✦ Top 10 Nodes No MAC Learning | | | |
|--------------------------------|---------------|------------|------------------------|
| Node Name | IP Address | จำนวน Vlan | Detail |
| nmd2_m3k_02 | 10.236.0.196 | 129 | Detail |
| lbg_m3k_02 | 10.236.12.195 | 119 | Detail |
| nmd3_m3k_02 | 10.236.0.198 | 109 | Detail |
| hik_m3k_02 | 10.236.12.197 | 100 | Detail |
| lbg_lbg_02 | 10.255.85.239 | 99 | Detail |
| nmd1_m3k_02 | 10.236.0.194 | 90 | Detail |

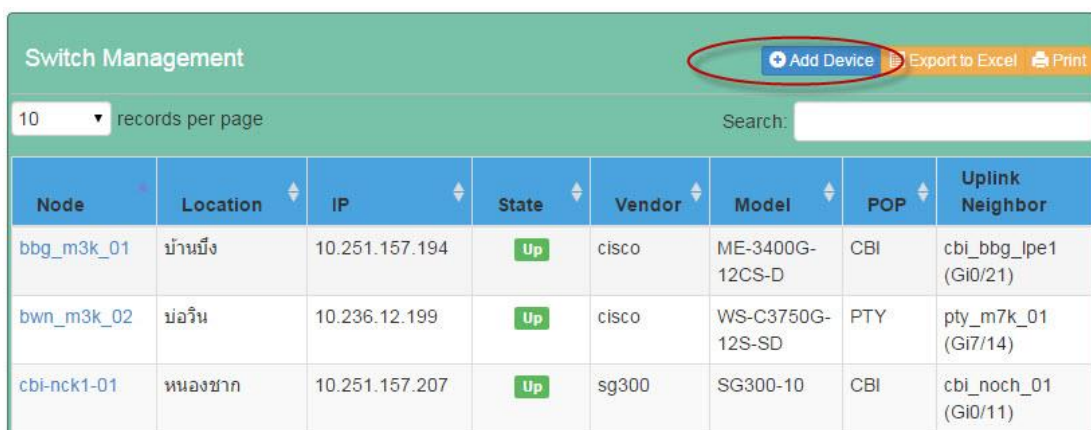
ภาพที่ 4-12 รายชื่อสวิตช์ที่มีจำนวน VLAN (ที่ไม่เรียนรู้ที่อยู่ MAC ภายใน 30 วัน) สูงสุด 10 อันดับ (กดปุ่ม Detail เพื่อแสดงรายละเอียด VLAN ดังกล่าว)

2. การจัดการข้อมูลอุปกรณ์ (Device setup)

ในส่วนของการจัดการข้อมูลสวิตช์และข้อมูลการเชื่อมต่อ เมื่อผู้ใช้เลือกที่เมนู Device → Switch จะแสดงรายชื่อสวิตช์ หมายเลขไอพี ยี่ห้อ รุ่น และสถานะ ดังภาพที่ 4-13 โดยสถานะสวิตช์ที่แสดงในตารางแบ่งออกเป็น 3 สถานะคือ

- Up คือเครื่องแม่ข่ายสามารถใช้ SNMP สอบถามได้
- Down คือเครื่องแม่ข่ายไม่สามารถติดต่อกับสวิตช์ได้ อาจมีเหตุเสียในเครือข่าย
- SNMP down คือเครื่องแม่ข่ายติดต่อกับสวิตช์ได้แต่ใช้ SNMP สอบถามไม่ได้

อาจเกิดจากการตั้งค่า SNMP community ไม่ตรงกันหรือเครื่องแม่ข่ายไม่มีสิทธิ์ในการเข้าถึงข้อมูลของอุปกรณ์



| Node | Location | IP | State | Vendor | Model | POP | Uplink Neighbor |
|-------------|----------|----------------|-------|--------|------------------|-----|-----------------------|
| bbg_m3k_01 | บ้านมิ่ง | 10.251.157.194 | Up | cisco | ME-3400G-12CS-D | CBI | cbi_bbg_lpe1 (Gi0/21) |
| bwn_m3k_02 | บ่อวิน | 10.236.12.199 | Up | cisco | WS-C3750G-12S-SD | PTY | pty_m7k_01 (Gi7/14) |
| cbi-nck1-01 | หนองซาก | 10.251.157.207 | Up | sg300 | SG300-10 | CBI | cbi_noch_01 (Gi0/11) |

ภาพที่ 4-13 รายชื่อสวิตช์ทั้งหมดที่มีในระบบ

ผู้ใช้สามารถจัดการข้อมูลสวิตช์และข้อมูลการเชื่อมต่อได้ดังต่อไปนี้

2.1 การเพิ่มสวิตช์

การเพิ่มสวิตช์ใหม่ในระบบเกิดขึ้นเมื่อผู้ใช้คลิกปุ่ม “Add Device” (ดังภาพที่ 4-13) ระบบจะแสดงหน้าจอการเพิ่มสวิตช์ ดังภาพที่ 4-14 ให้ผู้ใช้เลือก Region, POP, Root switch, และสถานที่ติดตั้ง เมื่อผู้ใช้ป้อนหมายเลขไอพีระบบจะตรวจสอบหมายเลขไอพีนั้นว่ามีในระบบหรือไม่ หากไม่ซ้ำจะแสดงเป็นเครื่องหมายถูก แต่หากมีข้อมูลอยู่แล้ว จะมีการเตือนดังภาพที่ 4-15

i Add Node Information

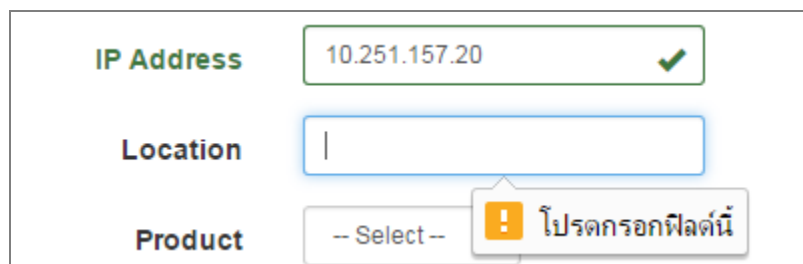
| | |
|------------------------|--|
| Region | <input type="text" value="ชลบุรี"/> |
| POP | <input type="text" value="CBI"/> <input type="checkbox"/> Root sw. |
| Root switch | <input type="text" value="cbi_m7k_01"/> |
| Node name | <input type="text" value="cbi_bsn_03"/> |
| IP Address | <input type="text" value="10.255.105.250"/> ✔ |
| Location | <input type="text" value="บางแสน"/> |
| Product | <input type="text" value="Cisco"/> |
| SNMP Community | <input type="text" value="public"/> |
| Telnet Username | <input type="text" value="nmsadmin"/> |
| Telnet Password | <input type="password" value="....."/> |
| Enable Password | <input type="password" value="....."/> |

ภาพที่ 4-14 หน้าจอการเพิ่มสวิตช์เข้าสู่ระบบ

| | |
|-------------------|--|
| Node name | <input type="text" value="cbi_bbg_05"/> |
| IP Address | <input style="border: 2px solid red;" type="text" value="10.251.157.194"/> ✘ |
| Location | <input type="text"/> |

ภาพที่ 4-15 การเตือนเมื่อป้อนหมายเลขไอพีที่มีอยู่แล้วในระบบ

กรณีที่ผู้ใช้ป้อนข้อมูลไม่ครบ เมื่อกดปุ่ม “Add Device” จะมีการเตือนดังภาพที่ 4-16 เช่นผู้ใช้ไม่ป้อนข้อมูลสถานที่ติดตั้งจะมีข้อความเตือนที่ช่องรับข้อมูล ทำให้ไม่สามารถเพิ่มข้อมูลได้



ภาพที่ 4-16 การเตือนเมื่อป้อนข้อมูลไม่ครบ

2.2 การแก้ไขสวิตช์

เมื่อผู้ใช้ต้องการแก้ไขข้อมูลสวิตช์ โดยเลือกชื่อสวิตช์ที่ต้องการแก้ไขจะแสดงหน้าจอสถานะข้อมูลของสวิตช์ (ซึ่งดึงมาจาก MIB) ส่วนด้านล่างของภาพที่ 4-17 แสดงปุ่มควบคุมทั้งหมด 4 ปุ่ม ให้ผู้ใช้กดปุ่ม “Edit” เพื่อเข้าสู่หน้าจอแก้ไขข้อมูลดังภาพที่ 4-18

| Node | Location | IP |
|------------|----------|----------------|
| bbg_m3k_01 | บ้านบึง | 10.251.157.194 |
| bwn_m3k_02 | บ่อวิน | 10.236.12.199 |

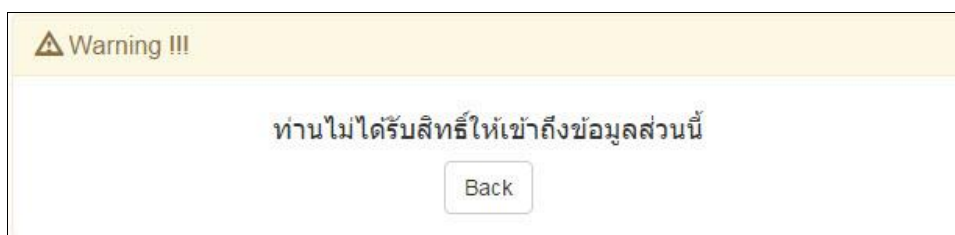
| | |
|---|--|
| sysName : bbg_m3k_01 Node Up | |
| ★ IP Address : | 10.251.157.194 |
| 🔍 sysDescr | Cisco IOS Software, ME340x Software (ME3 RELEASE SOFTWARE (fc1) Technical Supp 1986-2011 by Cisco Systems, Inc. Compiled |
| 🕒 sysUpTime | 387:23:12:09.79 |
| ⚙️ MAC Base | a418.7563.6dc2 |
| 🔧 Action | back Refresh Port Edit Delete |

ภาพที่ 4-17 การเข้าสู่หน้าจอจัดการข้อมูลสวิตช์

| | |
|------------------------|---|
| Location | <input type="text" value="บ้านมิ่ง"/> |
| Product | <input type="text" value="Cisco"/> |
| SNMP Community | <input type="text" value="public"/> |
| Telnet Username | <input type="text" value="nopadolc"/> |
| Telnet Password | <input type="password" value="*****"/> |
| Enable Password | <input type="password" value="*****"/> |
| | <input type="button" value="Cancel"/> <input type="button" value="Update"/> |

ภาพที่ 4-18 หน้าจอการแก้ไขข้อมูลสวิตช์

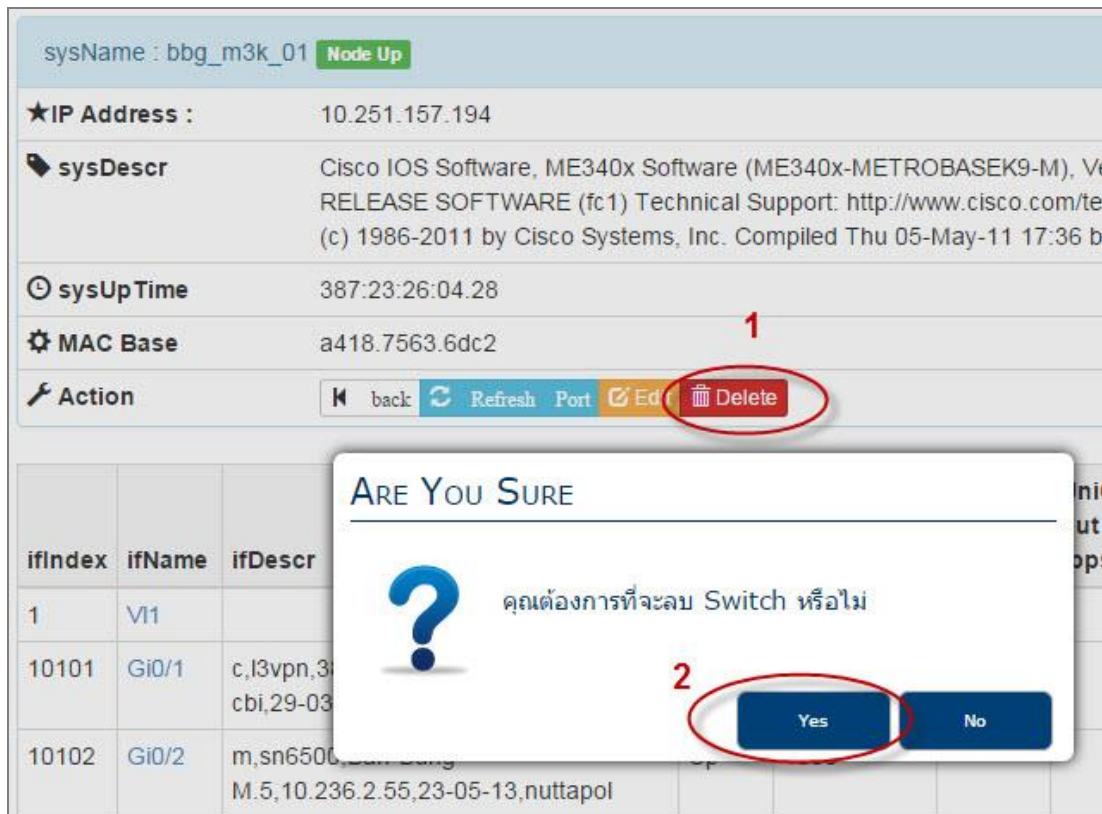
ภาพที่ 4-18 เมื่อผู้ใช้แก้ไขข้อมูลสวิตช์เรียบร้อยแล้ว ให้กดปุ่ม “Update” เพื่อบันทึกข้อมูลเข้าสู่ระบบ กรณีที่ผู้ใช้กดปุ่ม “Edit” แต่ไม่มีสิทธิ์ในการแก้ไขข้อมูล ระบบจะแจ้งเตือนดังภาพที่ 4-19



ภาพที่ 4-19 การแจ้งเตือนเมื่อผู้ใช้ไม่มีสิทธิ์ในการแก้ไขข้อมูล

2.3 การลบสวิตช์

การลบข้อมูลสวิตช์ออกจากระบบทำได้โดยให้ผู้ใช้กดปุ่ม “Delete” ดังภาพที่ 4-20 จะปรากฏกล่องโต้ตอบ เพื่อยืนยันการลบข้อมูล เมื่อกดปุ่ม “Yes” ระบบจะตรวจสอบสิทธิ์ว่าเป็นผู้ดูแลระบบหรือไม่ หากมีสิทธิ์ถูกต้อง ระบบจะลบข้อมูลที่สัมพันธ์กับสวิตช์ตัวนี้ออกจากฐานข้อมูล เช่น ข้อมูลหมายเลข VLAN ข้อมูลพอร์ต ข้อมูลตาราง MAC address



ภาพที่ 4-20 การลบข้อมูลสวิตช์ออกจากระบบ

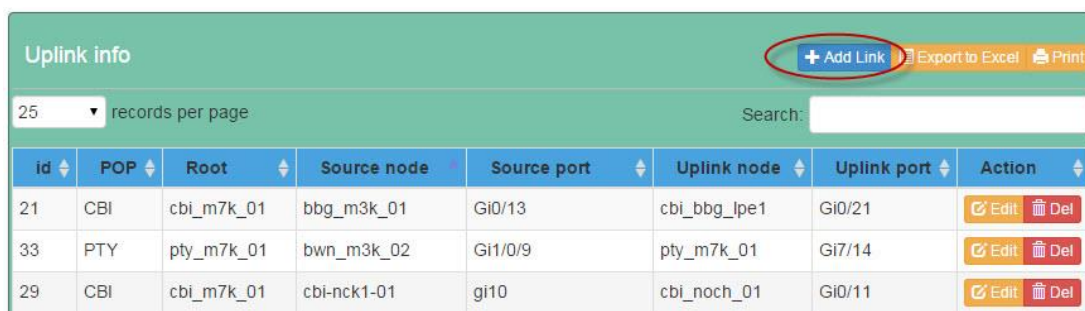
หากผู้ใช้ไม่มีสิทธิ์ในการลบข้อมูล จะแสดงกล่องข้อความแจ้งเตือนดังในภาพที่ 4-21



ภาพที่ 4-21 การแจ้งเมื่อผู้ใช้ไม่มีสิทธิ์ลบข้อมูล

2.4 การเพิ่มการเชื่อมต่อ

หลังจากที่ผู้ใช้เพิ่มสวิตช์ใหม่ในระบบเรียบร้อยแล้ว ขั้นตอนต่อไปคือการเพิ่มข้อมูลการเชื่อมต่อของสวิตช์ โดยเลือกเมนู Device → Uplink Node จะแสดงข้อมูลการเชื่อมต่อของสวิตช์ที่มีอยู่ในระบบ ดังภาพที่ 4-22 แสดงตารางข้อมูลสายเชื่อมโยงขาขึ้น (Uplink) ของสวิตช์แต่ละตัวว่าเชื่อมต่อมาจากสวิตช์ด้านบนตัวใด (Uplink node) เมื่อต้องการเพิ่มข้อมูลสายเชื่อมโยงให้กดปุ่ม “Add Link”



| Uplink info | | | | | | | |
|----------------------------------|-----|------------|-------------|-------------|--------------|-------------|----------|
| + Add Link Export to Excel Print | | | | | | | |
| 25 records per page | | Search: | | | | | |
| id | POP | Root | Source node | Source port | Uplink node | Uplink port | Action |
| 21 | CBI | cbi_m7k_01 | bbg_m3k_01 | Gi0/13 | cbi_bbg_lpe1 | Gi0/21 | Edit Del |
| 33 | PTY | pty_m7k_01 | bwn_m3k_02 | Gi1/0/9 | pty_m7k_01 | Gi7/14 | Edit Del |
| 29 | CBI | cbi_m7k_01 | cbi-nck1-01 | gi10 | cbi_noch_01 | Gi0/11 | Edit Del |

ภาพที่ 4-22 ข้อมูลการเชื่อมต่อสวิตช์ในระบบ

ภาพที่ 4-22 แสดงหน้าจอเพิ่มสายเชื่อมโยงขาขึ้น เมื่อผู้ใช้เลือก Region, POP และ Root ที่ต้องการแล้ว ระบบจะแสดงชื่อสวิตช์ต้นทาง (Source node) และแสดงชื่อพอร์ตของสวิตช์ดังกล่าวในช่อง Source interface เพื่อเลือกพอร์ตซึ่งทำหน้าที่เชื่อมโยงขาขึ้นของสวิตช์ตัวนี้ จากนั้นเลือกประเภทการเชื่อมต่อว่าเป็นเลขอร์ 2 หรือเลขอร์ 3 เลือกสวิตช์ที่เชื่อมต่อขึ้นไป (Uplink Node) เลือกพอร์ตให้ถูกต้อง จากนั้นกดปุ่ม “Add” เพื่อบันทึกข้อมูล

Add Uplink Node

Region ชลบุรี ▼

POP CBI ▼

Root cbi_m7k_01 ▼

Source Node cbi_m3k_03 (10.236.0.154) ▼

Source Interface Fa0/24 :up link to cbi_m7k_01 gi7/1 ▼

Link Type Layer 2 ▼

Uplink Node cbi_m7k_01 (118.174.224.136) ▼

Uplink Interface Gi7/1 :### cbi_m3k_03 ,10.236.0.154 ### ▼

Back
Add

ภาพที่ 4-23 การเพิ่มข้อมูลการเชื่อมต่อ

2.5 การแก้ไขการเชื่อมต่อ

เมื่อต้องการแก้ไขข้อมูลการเชื่อมต่อสวิตช์ให้กดปุ่ม “Edit” ในแถวที่ต้องการแก้ไข

ดังภาพที่ 4-24

| id | POP | Root | Source node | Source port | Uplink node | Uplink port | Action |
|----|-----|------------|-------------|-------------|--------------|-------------|--|
| 21 | CBI | cbi_m7k_01 | bbg_m3k_01 | Gi0/13 | cbi_bbg_lpe1 | Gi0/21 | ✎ Edit ✖ Del |

ภาพที่ 4-24 การเลือกแถวที่ต้องการแก้ไขการเชื่อมต่อ

ภาพที่ 4-24 แสดงหน้าจอการแก้ไขข้อมูลการเชื่อมต่อ ผู้ใช้สามารถแก้ไขตำแหน่งพอร์ตต้นทาง, ประเภทของการเชื่อมต่อ สวิตช์และพอร์ตสวิตช์ฝั่งเชื่อมโยงขึ้นเท่านั้น (ไม่ให้แก้ไขสวิตช์ต้นทางเนื่องจากเป็นตัวอ้างอิงหลัก)

ภาพที่ 4-25 หน้าจอการแก้ไขการเชื่อมต่อ

2.6 การค้นหาและลบการเชื่อมต่อ

ผู้ใช้งานสามารถค้นหาและลบข้อมูลการเชื่อมต่อได้ ดังภาพที่ 4-26 สามารถค้นหาข้อมูลที่ต้องการลบได้จากช่อง “Search” เมื่อพบข้อมูลที่ต้องการแล้วให้กดปุ่ม “Del” จะพบข้อความยืนยันการลบข้อมูล เมื่อลบข้อมูลแล้ว หน้าจอจะถูกโหลดเพื่อปรับปรุงข้อมูลในตาราง

| id | POP | Root | Source node | Source port | Uplink node | Uplink port | Action |
|----|-----|------------|-------------|-------------|-------------|-------------|----------|
| 21 | CBI | cbi_m7k_01 | bbg | | | /21 | Edit Del |
| 45 | CBI | cbi_m7k_01 | cbi | | | /14 | Edit Del |
| 30 | CBI | cbi_m7k_01 | cbi | | | /3 | Edit Del |

ภาพที่ 4-26 การลบข้อมูลการเชื่อมต่อ

3. แสดงข้อมูล VLAN

3.1 สรุปการใช้งาน VLAN

ข้อมูลส่วนนี้เป็นการดูจำนวนหมายเลข VLAN ที่ถูกใช้งานและจำนวนที่เหลือในแต่ละสวิตช์ โดยผู้ใช้เลือกที่เมนู “Vlan Summary” จะแสดงหน้าจอให้เลือก Region และ Point-of-Presence (POP) ที่ต้องการตรวจสอบ จากนั้นกดปุ่ม “Show” ดังภาพที่ 4-27

The screenshot shows a web interface for displaying VLAN information. It features two dropdown menus: 'Region' with the selected value 'เมืองพัทยา' and 'POP' with the selected value '-- select --'. To the right of these dropdowns is a blue button labeled 'Show' with a magnifying glass icon.

ภาพที่ 4-27 การเลือกสรุปจำนวนการใช้งาน VLAN แยกตามพื้นที่

ระบบจะแสดงรายชื่อสวิตช์ตาม POP ที่เลือก โดยแสดงจำนวน VLAN ที่รองรับได้ของแต่ละสวิตช์ จำนวนหมายเลข VLAN ที่ถูกใช้ไป จำนวนร้อยละของการใช้งาน และบอกจำนวน VLAN ที่เหลือ ดังภาพที่ 4-28 ข้อมูลการใช้งาน VLAN โดยเรียงลำดับตามการใช้งานสูงสุด นอกจากนี้ผู้ใช้สามารถเลือกคอลัมน์อื่นที่ต้องการเรียงลำดับได้

| จำนวนหมายเลข Vlan ที่ถูกใช้งาน และจำนวนหมายเลข Vlan ที่ยังไม่ได้ใช้ | | | | | | |
|---|----------------|------|------|-------|------|--|
| เมืองพัทยา (POP : PTY) | | | | | | |
| No. | Node | Vlan | | | | |
| | | Max | Use | Use % | Free | |
| 1 | pty_m7k_01 | 4095 | 1204 | 29.40 | 2891 | |
| 2 | pty_c3k_01_nec | 1005 | 246 | 24.48 | 759 | |
| 3 | lbg_m3k_02 | 1005 | 197 | 19.60 | 808 | |

ภาพที่ 4-28 สรุปจำนวน VLAN ที่ใช้งานของแต่ละสวิตช์

จากตารางผลสรุป ถ้าการใช้งาน VLAN ของสวิตช์ตัวใดมีค่าสูงเกินร้อยละ 80 (ส่งผลให้รองรับจำนวนลูกค้าใหม่ได้น้อย) ระบบจะแสดงข้อมูลในแถวด้วยพื้นหลังสีแดง เพื่อให้เป็นที่สังเกตเห็นได้ง่าย ดังภาพที่ 4-29

| เมืองพญา (POP : PTY) | | | | | |
|----------------------|------------|------|-----|-------|------|
| No. | Node | Vlan | | | |
| | | Max | Use | Use % | Free |
| 31 | pty_pty_03 | 64 | 58 | 90.63 | 6 |
| 46 | pty_bnp_02 | 36 | 29 | 80.56 | 7 |
| 10 | pty_pty_02 | 255 | 154 | 60.39 | 101 |

ภาพที่ 4-29 การแจ้งเตือนเมื่อสวิตช์ที่มีการใช้งาน VLAN เกินร้อยละ 80

3.2 VLAN แยกตามสวิตช์

ผู้ใช้งานสามารถค้นหา VLAN ที่ถูกตั้งค่าในแต่ละสวิตช์ซึ่งแยกตามกลุ่มของพื้นที่บริการ เมื่อเลือกที่เมนูย่อย “Switch” จะปรากฏหน้าจอซึ่งแบ่งออกเป็น 3 ส่วน ดังภาพที่ 4-30 ส่วนที่หนึ่งแสดงกลุ่มของสวิตช์แยกตามพื้นที่ ส่วนที่สองแสดงรายชื่อพอร์ตสวิตช์ และส่วนที่สามแสดงข้อมูลจากการเลือกในส่วนที่หนึ่งและส่วนที่สอง โดยแบ่งการแสดงผลออกเป็นแท็บ (Tab) คือแท็บ

Information และแท็บ VLAN

แท็บ Information จะบอกถึงข้อมูลเบื้องต้น เช่น ระยะเวลาที่อุปกรณ์ทำงานมาแล้ว รุ่น และซอฟต์แวร์ที่ใช้ สถานที่ติดตั้ง จำนวนหมายเลข VLAN ที่ถูกใช้ไป

ภาพที่ 5

Information Vlan

HostName : cbi_bbg_04

IP Address : 10.251.157.199

SysUpTime : 396 วัน 8 ชม. 16 นาที 42.15 วินาที

Product : cisco

Model : ME-3400G-12CS-D

IOS Image : me340x-metroaccess-mz.122-25.SEG3.bin

IOS Version : N/A

Location : บ้านมิ่ง

Vlan Use / Max : 121 / 1005

ภาพที่ 4-30 การแบ่งหน้าจอแสดงผลออกเป็น 3 ส่วน

Information Vlan

10 records per page Search:

| Vlan | Vlan name | MAC Count | Update | Action |
|------|-------------------|-----------|---------------------|-----------|
| 1 | default | 0 | 2015-06-01 01:04:11 | MAC Graph |
| 9 | nex-sw | 10 | 2015-06-01 01:04:11 | MAC Graph |
| 17 | nex-msan | 1 | 2015-06-01 01:04:11 | MAC Graph |
| 34 | NMS34 | 14 | 2015-06-01 01:04:11 | MAC Graph |
| 43 | nms.ddn-keymile | 3 | 2015-06-01 01:04:11 | MAC Graph |
| 45 | NMS45 | 26 | 2015-06-01 01:04:11 | MAC Graph |
| 49 | FORTH_DSLAM_NMS | 46 | 2015-06-01 01:04:11 | MAC Graph |
| 57 | FORTH_BanBung&TPC | 1 | 2015-06-01 01:04:11 | MAC Graph |
| 74 | FORTH_NongSak | 1 | 2015-06-01 01:04:11 | MAC Graph |
| 77 | FORTH_NongYai | 22 | 2015-06-01 01:04:11 | MAC Graph |

Showing 1 to 10 of 121 entries

← Previous 1 2 3 4 5 Next →

ภาพที่ 4-31 ข้อมูล VLAN ของแต่ละสวิตช์เมื่อเลือกที่แท็บ VLAN

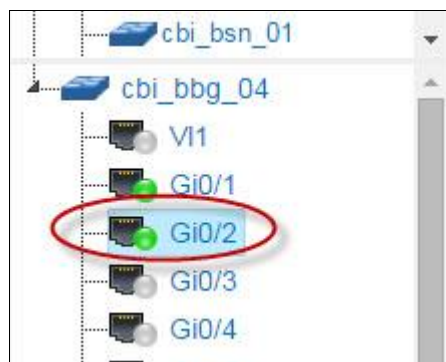
ภาพที่ 4-31 เมื่อเลือกที่แท็บ VLAN จะแสดงชื่อและหมายเลข VLAN ที่มีการตั้งค่าไว้ในสวิตช์ โดยมีจำนวนที่อยู่ MAC และวันที่ได้เก็บข้อมูลจากสวิตช์ เมื่อเลือกที่ปุ่ม “MAC” ของแต่ละ VLAN จะปรากฏหน้าต่างขึ้นมา ดังภาพที่ 4-32 พร้อมกับระบุที่อยู่ผู้ผลิตอุปกรณ์ของ MAC นั้น และพอร์ตที่เรียนรู้ MAC นั้นเข้ามา



| Vlan : 43 | |
|---|-----------|
| MAC address | Interface |
| 00:1b:0d:e7:9f:c0 (CISCO SYSTEMS, INC.) | Gi0/15 |
| 00:e0:df:54:62:b7 (KEYMILE GmbH) | Gi0/11 |

Total Mac Addresses for this vlan : 2

ภาพที่ 4-32 ข้อมูลที่อยู่ MAC ในแต่ละ VLAN



ภาพที่ 4-33 การเลือกพอร์ตเพื่อดูการตั้งค่า VLAN

ภาพที่ 4-33 เมื่อผู้ใช้เลือกที่ชื่อพอร์ตจะแสดงข้อมูลตั้งค่าพอร์ตนั้น ข้อมูลของพอร์ต เช่น ข้อมูล ifIndex, ความเร็วของพอร์ต, ประเภทของพอร์ตว่าเป็นทริงค์หรือแอกเซส หมายเลขของ VLAN ที่มีการตั้งค่าไว้ ดังภาพที่ 4-34

| Node: cbi_bbg_04 , Interface: GigabitEthernet0/2 | |
|--|--|
| Interface Name | GigabitEthernet0/2 |
| Ifindex | 10102 |
| Description | d,zte(u300),Nong-Chak,10.236.3.6,10-03-14,nuttapol |
| Speed (Kbits) | 1,000,000 |
| Port Mode | Trunk |
| Vlan Allowed | 104,663,2108,2328,2392,2393,2472,3135 |

ภาพที่ 4-34 การแสดงข้อมูล VLAN ที่ตั้งค่าที่พอร์ต

3.3 ปรับปรุงข้อมูล VLAN

ข้อมูล VLAN จะถูกปรับปรุง (update) ตามระยะเวลาที่ตั้งไว้ในระบบนอกจากนี้ผู้ใช้สามารถปรับปรุงข้อมูล VLAN ได้ด้วยตนเอง โดยเลือกที่เมนูย่อย “Fetch Vlan” เลือกสวิตช์ที่ต้องการปรับปรุง VLAN จากนั้นกดปุ่ม “Discovery” ดังภาพที่ 4-35

The image shows a configuration panel with three dropdown menus and a button. The 'Region' dropdown is set to 'ชลบุรี', the 'POP' dropdown is set to 'CBI', and the 'Node' dropdown is set to 'bbg_m3k_01'. Below these is a green button labeled 'Discovery', which is circled in red.

ภาพที่ 4-35 การเลือกสวิตช์ที่ต้องการปรับปรุงข้อมูลของ VLAN

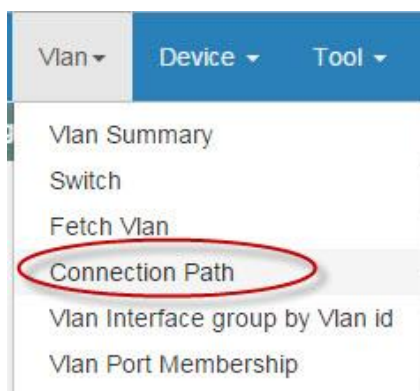
เมื่อผู้ใช้กดปุ่ม “Discovery” ระบบจะสอบถามข้อมูล VLAN และพอร์ตที่เป็นสมาชิกของ VLAN โดยใช้โปรโตคอล SNMP ระยะเวลาในการดำเนินการขึ้นอยู่กับจำนวน VLAN ที่มีในสวิตช์นั้น ๆ เมื่อระบบดำเนินการเสร็จจะแสดงหมายเลข VLAN และชื่อ ดังภาพที่ 4-36

| No. | VLAN | Vlan Name |
|-----|------|--------------|
| 1 | 1 | default |
| 2 | 9 | nex-sw |
| 3 | 17 | nex-msan |
| 4 | 29 | Test-Traffic |

ภาพที่ 4-36 ข้อมูล VLAN ที่ได้จากการปรับปรุง

3.4 การแสดงผังภาพเส้นทาง VLAN

เมื่อผู้ใช้เลือกที่เมนูย่อย “Connection path” ดังภาพที่ 4-37 จะปรากฏกล่องโต้ตอบด้านซ้ายมือสำหรับเลือกหมายเลข VLAN ที่มีอยู่ในระบบแยกตาม Region และ POP ดังภาพที่ 4-37



ภาพที่ 4-37 เมนูย่อยภายใต้เมนู Vlan

Region :
 ชลบุรี ▼

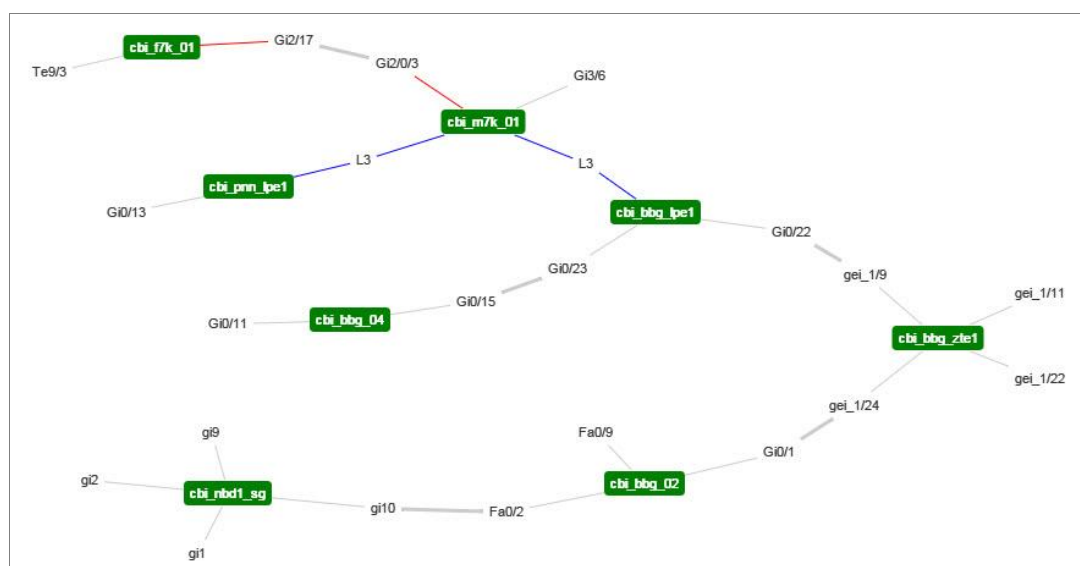
POP :
 CBI ▼

Vlan :
 3005 (mini_ms) ▼

Search

ภาพที่ 4-38 การเลือกหมายเลข VLAN ที่ต้องการดูเส้นทาง

ภาพที่ 4-39 ข้อมูลที่แสดงในผังภาพการเชื่อมต่อ ประกอบด้วยชื่อสวิตช์ (สีเขียว) และชื่อพอร์ตที่เป็นสมาชิก VLAN เชื่อมกับสวิตช์ตัวอื่น ๆ ประเภทการเชื่อมต่อถ้าเป็นแบบเลเยอร์ 2 จะแทนด้วยเส้นสีเทา แต่หากเป็นแบบเลเยอร์ 3 จะแทนด้วยเส้นสีน้ำเงินและเขียนว่า “L3” หากพอร์ตนั้นไม่มี VLAN สร้างไว้แต่สวิตช์ปลายทางมี VLAN นั้นสร้างอยู่ จะถูกแทนด้วยเส้นสีแดง เพื่อแสดงถึงเส้นทาง VLAN ไม่ต่อเนื่องกัน ตัวอย่างจากภาพ พอร์ต Gi2/0/3 ของสวิตช์ cbi_m7k_01 ไม่มี VLAN 3005 ประกาศไปหา cbi_f7k_01 แต่ที่พอร์ต Ten9/3 ของ cbi_f7k_01 มี VLAN 3005 สร้างไว้

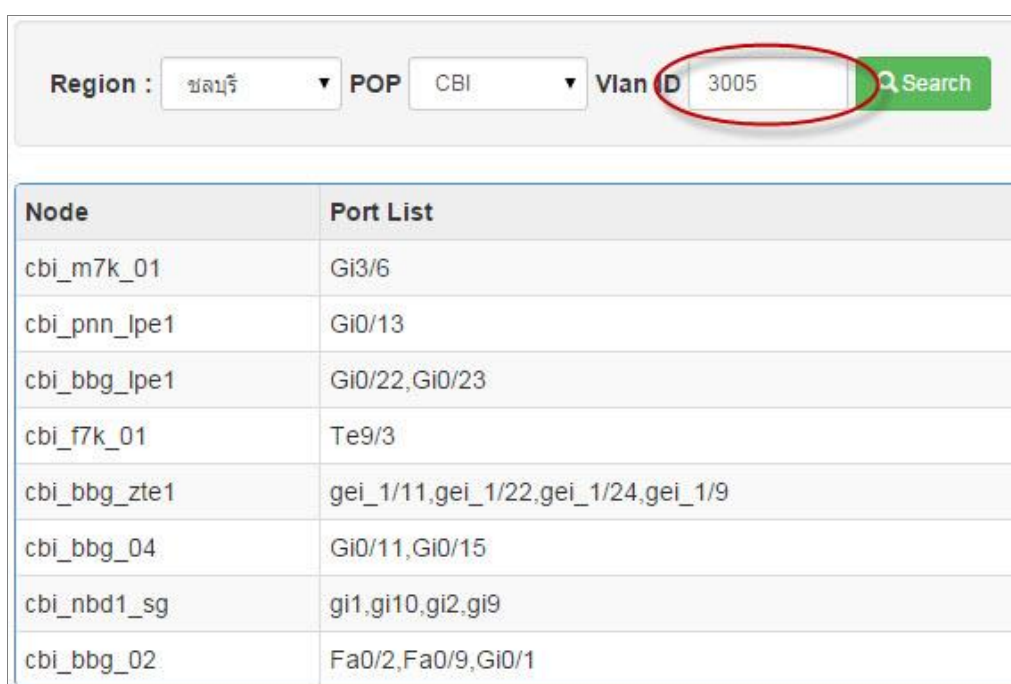


ภาพที่ 4-39 แพนภาพเส้นทางของ VLAN ตามที่ผู้ใช้เลือก

3.5 การแสดงพอร์ตที่เป็นสมาชิกของ VLAN

เมื่อผู้ใช้งานต้องการค้นหาพอร์ตสวิตช์ที่เป็นสมาชิก VLAN เพื่อเป็นข้อมูลว่า VLAN ดังกล่าวถูกตั้งค่าไว้ที่พอร์ตสวิตช์ตัวใดบ้าง โดยผู้ใช้เลือกจากเมนูย่อย “Vlan Port Membership” (ดูภาพที่ 4-37) ระบบจะแสดงหน้าจอการค้นหา VLAN ดังภาพที่ 4-40 ผู้ใช้เลือก Region, POP และหมายเลข VLAN ที่ต้องการค้นหาและกดปุ่ม Search

ผลการค้นหาตามภาพที่ 4-40 แสดงรายชื่อสวิตช์และพอร์ตที่เป็นสมาชิกของ VLAN ที่ผู้ใช้งานต้องการค้นหา



| Node | Port List |
|--------------|------------------------------------|
| cbi_m7k_01 | Gi3/6 |
| cbi_pnn_lpe1 | Gi0/13 |
| cbi_bbg_lpe1 | Gi0/22,Gi0/23 |
| cbi_f7k_01 | Te9/3 |
| cbi_bbg_zte1 | gei_1/11,gei_1/22,gei_1/24,gei_1/9 |
| cbi_bbg_04 | Gi0/11,Gi0/15 |
| cbi_nbd1_sg | gi1,gi10,gi2,gi9 |
| cbi_bbg_02 | Fa0/2,Fa0/9,Gi0/1 |

ภาพที่ 4-40 การแสดงพอร์ตที่เป็นสมาชิก VLAN

4. เครื่องมือ (Tool)

ระบบค้นหาโครงสร้าง VLAN มีเครื่องมือที่สนับสนุนการทำงานแก่ผู้ใช้งาน ช่วยอำนวยความสะดวกในการใช้ข้อมูล VLAN เพื่อนำมาปรับปรุงการตั้งค่าสวิตช์ที่ไม่ถูกต้องในเครือข่าย โดยมีเครื่องมือให้ใช้งานดังนี้

4.1 การเปรียบเทียบ VLAN ระหว่างพอร์ต

ตามหลักปฏิบัติการตั้งค่า VLAN ที่ถูกต้อง พอร์ตทั้ง 2 ฝั่งของสวิตช์ที่เชื่อมต่อกัน จะต้องมีจำนวน VLAN ที่สมมาตรกัน หากพอร์ตด้านใดมี VLAN ที่เกินหรือขาด อาจส่งผลกระทบต่อ การสื่อสาร

ผู้ใช้งานสามารถเปรียบเทียบ VLAN ระหว่างพอร์ตทั้ง 2 ฝั่งของสวิตช์ที่เชื่อมต่อกัน โดยเลือกที่เมนูย่อย “Vlan Trunk Inconsistent” จะแสดงหน้าจอ ดังภาพที่ 4-41 เมื่อผู้ใช้เลือกสวิตช์ที่ต้องการ ตัวเลือกในช่อง Link Interface จะแสดงชื่อพอร์ตและสวิตช์ที่เชื่อมต่อกัน จากตัวอย่าง จะเห็นว่าสวิตช์ cbi_bbg_lpe1 มีพอร์ตเชื่อมไปหาสวิตช์ตัวอื่นทั้งหมด 5 พอร์ต เมื่อเลือกที่พอร์ต Gi0/21 ซึ่งต่อไปหาสวิตช์ bbg_m3k_01 ที่พอร์ต Gi0/13 จะแสดงจำนวน VLAN ที่มีการตั้งค่าไว้ทั้งสองพอร์ต เมื่อผู้ใช้กดปุ่ม “Compare” ระบบจะทำการเปรียบเทียบ VLAN ที่ไม่ตรงกันของทั้งสองด้าน โดยแสดงผลดังภาพที่ 4-41

POP: CBI

Source Node: cbi_bbg_lpe1 (118.174.2)

Link Interface: cbi_bbg_lpe1(Gi0/21) -> bbg_m3k_01 (Gi0/13)

Source Intf (Downlink)(Gi0/21):

| | |
|--|---|
| cbi_bbg_lpe1(Gi0/21) -> bbg_m3k_01 (Gi0/13) | |
| cbi_bbg_lpe1(Gi0/23) -> cbi_bbg_04 (Gi0/15) | 383,386 |
| cbi_bbg_lpe1(Gi0/22) -> cbi_bbg_zte1 (gei_1/9) | 7,664,69 |
| cbi_bbg_lpe1(Gi0/6) -> cbi_hkc_01 (Gi0/24) | 97,1629 |
| cbi_bbg_lpe1(Gi0/2) -> cbi_noch_01 (Gi0/16) | 1638,1649,2384,2451,3011,3044,3045,3046,3117,3417,397 |

Destination Intf (Uplink)(Gi0/13):

| |
|---|
| 9,17,33,34,45,49,52,104,105,106,111,116,169,383,386,413,432,460,467,472,492,493,494,495,496,555,637,664,690,699,723,828,880,1500,1514,1534,1536,1542,1592,1597,1629,1635,1636,1638,1649,2384,2451,3011,3044,3045,3046,311 |
|---|

Compare

ภาพที่ 4-41 การเลือกพอร์ตเพื่อเปรียบเทียบ VLAN

ภาพที่ 4-41 แสดงผลของ VLAN ที่ได้จากการเปรียบเทียบสองพอร์ตข้างต้น จากตัวอย่างจะเห็นว่าที่พอร์ต Gi0/21 มี VLAN 340 เกินมาเนื่องจากพอร์ต Gi0/13 ไม่มีใช้งานและในทางตรงกันข้ามที่พอร์ต Gi0/13 มี VLAN 732 และ 1635 ที่ไม่จำเป็นเนื่องจากพอร์ต Gi0/13 ไม่มี

การตั้งค่า VLAN ดังกล่าว ระบบจึงแจ้งว่าควรลบ VLAN ดังกล่าวออกจากพอร์ตทั้งสอง



ภาพที่ 4-42 ผลลัพธ์ที่ได้จากการเปรียบเทียบ VLAN

4.2 การหาเส้นทางระหว่างสวิตช์

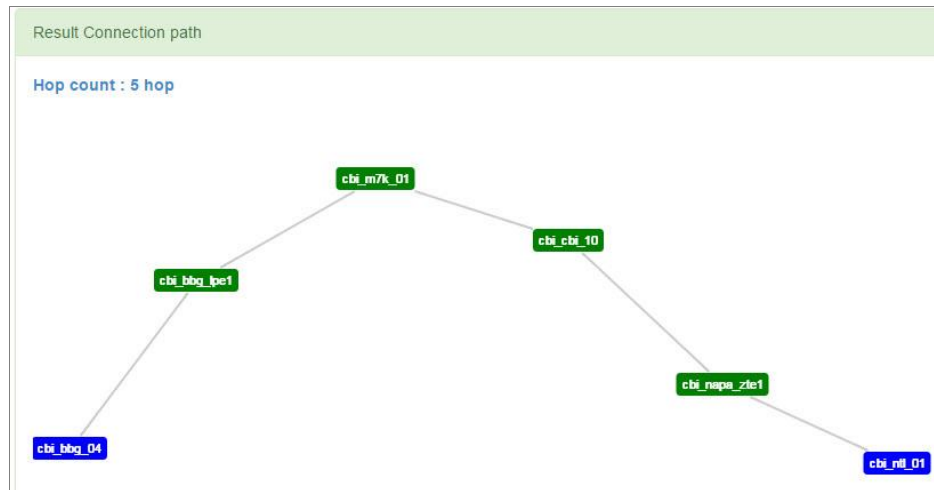
เครื่องมือนี้ใช้ค้นหาเส้นทางเชื่อมต่อและนับจำนวน hop ระหว่างสวิตช์ต้นทาง และสวิตช์ปลายทาง โดยแสดงเป็นผังภาพเส้นทางแต่ละ hop ต้องผ่านสวิตช์ตัวใดบ้าง เป็นจำนวนทั้งหมดกี่ hop เพื่อใช้เป็นข้อมูลในการตั้งค่า VLAN

เมื่อผู้ใช้เลือกเมนู “Switch Path” จะแสดงหน้าจอดังภาพที่ 4-43 จากนั้นให้เลือก POP สวิตช์ต้นทาง และสวิตช์ปลายทาง เมื่อกดปุ่ม “View Path” ระบบจะค้นหาเส้นทาง (Physical path) และแสดงผลดังภาพที่ 4-44



ภาพที่ 4-43 การเลือกสวิตช์ต้นทางและปลายทางที่ต้องการหาเส้นทาง

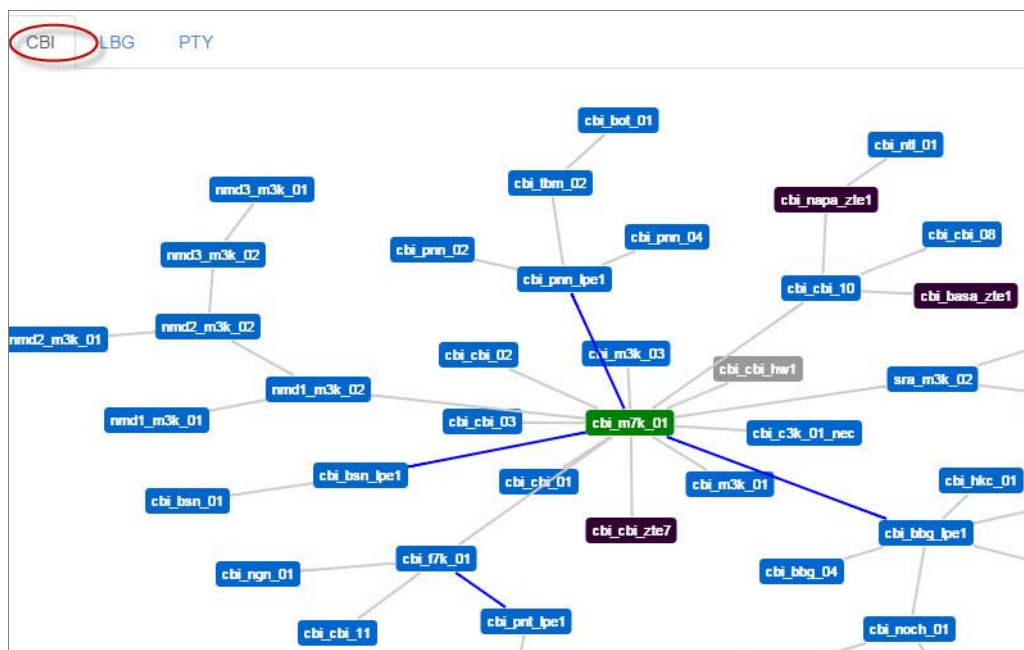
ภาพที่ 4-44 ผลของเส้นทางระหว่างสวิตช์ cbi_bbg_04 และ cbi_ntl_01 ต้องผ่านสวิตช์ทั้งสิ้น 5 hop



ภาพที่ 4-44 เครื่องมือการหาจำนวน hop ของสวิตช์

4.3 Network Topology

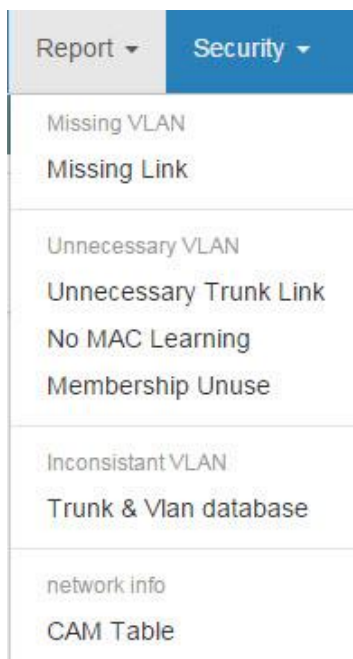
เครื่องมือแสดงผังภาพการเชื่อมต่อสวิตช์แยกตาม POP สามารถเรียกใช้งานจากเมนูย่อย “Topology All” ดังภาพที่ 4-45 เมื่อเลือกที่ POPCBI จะปรากฏผังภาพการเชื่อมต่อสวิตช์ โดยแต่ละยี่ห้อจะแทนด้วยสีที่ต่างกัน โดยมีคำอธิบายที่ได้ผังภาพ



ภาพที่ 4-45 การแสดงผังภาพเครือข่ายแยกตามพื้นที่

5. รายงาน (Report)

หากแบ่งตามผลกระทบที่อาจส่งผลต่อประสิทธิภาพการใช้งาน สามารถแบ่งรายงานการใช้และการตั้งค่า VLAN ออกเป็น 4 กลุ่มคือ VLAN สูญหาย, VLAN ที่ไม่จำเป็น, VLAN ที่ไม่สอดคล้องกัน และข้อมูลของเครือข่ายเมนูรายงานแสดงดังภาพที่ 4-46



ภาพที่ 4-46 เมนูรายงานแบ่งออกเป็น 4 กลุ่ม

5.1 รายงาน Missing Link

สายเชื่อมโยงที่หายไป (อาจเกิดจากการตั้งค่า VLAN ไม่ครบ) ทำให้ VLAN ถูกแบ่งเป็นส่วน (isolated VLAN) ผู้ใช้งานที่อยู่ใน VLAN คนละส่วนไม่สามารถสื่อสารถึงกันได้โดยรายงานนี้สามารถแสดงหมายเลข VLAN ที่สูญหายแยกตาม Region และ POP ที่ต้องการค้นหา ดังแสดงในภาพที่ 4-47

Region: ชลบุรี POP: CBI Show

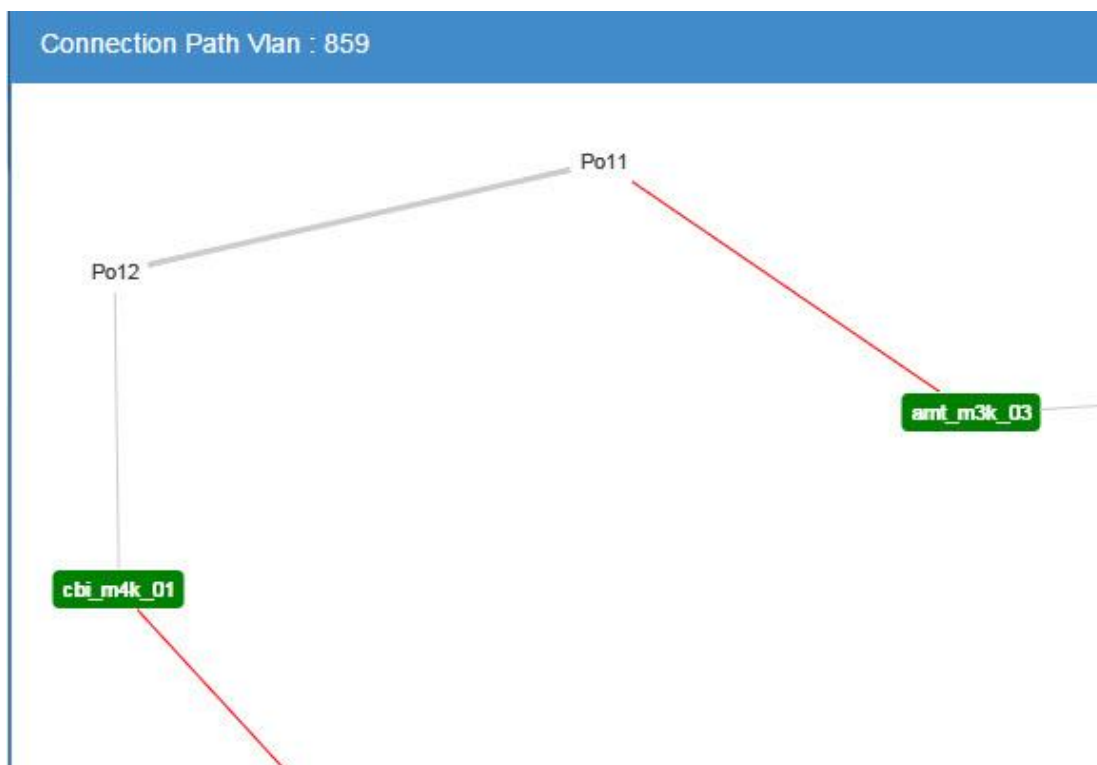
Missing Vlan Info Export

25 records per page Search:

| POP | Vlan | Vlan Name | Node Missing |
|-----|------|---------------------------|--|
| CBI | 943 | 3844ID005 | cbi_nyi_01(Gi1/0/12) |
| CBI | 906 | icc-dsl,3828d0217,1M/512k | nmd2_m3k_02(Po2),nmd3_m3k_02(Po1) |
| CBI | 9 | nex-sw,-,- | cbi-nck1-02(ch1) |
| CBI | 893 | scbvpn_panat_nikom | cbi_pnn_02(Gi0/24),cbi_bbg_zte1(gei_1/9) |
| CBI | 867 | 3828x0156,I2,local | cbi_m4k_01(Gi1/5) |
| CBI | 859 | data_fttx_cbi | amt_m3k_03(Po11) |

ภาพที่ 4-47 รายงาน VLAN ที่มีเส้นทางไม่ครบ

จากภาพที่ 4-48 ข้อมูลในรายงานประกอบด้วยหมายเลขและชื่อของ VLAN ชื่อสวิตช์ และพอร์ตที่ VLAN นั้นสูญหาย สวิตช์ที่มีชื่อสีแดงหมายถึง ที่พอร์ตของสวิตช์นั้นไม่มี VLAN สร้างไว้ แต่พอร์ตอีกฝั่งหนึ่งได้ตั้งค่า VLAN ไว้แล้ว เมื่อผู้ใช้เลือกที่หมายเลข VLAN ระบบจะแสดงผังภาพการเชื่อมต่อของ VLAN นั้น ดังแสดงในภาพที่ 4-48 (เส้นสีแดงแสดงว่าที่พอร์ต Po11 ไม่มีการตั้งค่า VLAN 859)



ภาพที่ 4-48 ผังการเชื่อมต่อเมื่อผู้ใช้เลือกที่หมายเลข VLAN

5.2 รายงานสายเชื่อมโยงแบบที่รั้งคี่ที่ไม่จำเป็น (Unnecessery Trunk Link)

การตั้งค่า VLAN ที่พอร์ตไม่ตรงกับใช้งานจริง มีพอร์ตเป็นสมาชิก VLAN มากเกินไป อาจเกิดปัญหาเช่น ด้านความปลอดภัยมีปริมาณข้อมูลที่ไม่จำเป็นผ่านเข้ามาในสวิตช์ได้

สำหรับรายงาน VLAN ที่มีสายเชื่อมโยงที่ไม่จำเป็น ระบบจะนับจำนวนพอร์ตของแต่ละ VLAN โดยพิจารณาที่สวิตช์ที่เป็นต้นกำเนิด (Root bridge) ผู้ใช้สามารถเลือกจำนวนพอร์ตสูงสุดที่ยอมให้ตั้งค่า VLAN ซ้ำกันได้ดังในภาพที่ 4-49

ภาพที่ 4-49 การเลือกแสดงจำนวนพอร์ตที่ยอมให้ตั้งค่า VLAN ซ้ำกันได้

ผลของรายงานมีลักษณะดังภาพที่ 4-49 ประกอบด้วยหมายเลขและชื่อ VLAN จำนวนเส้นทางที่เข้าซ้อนเรียงตามลำดับจากมากไปน้อย ผู้ใช้สามารถเลือกที่ปุ่มรูปภาพเพื่อแสดงเส้นทางการเชื่อมต่อของแต่ละ VLAN ที่ต้องการ

| Node Name | Vlan id | Vlan name | Unnecessary Link | Map |
|------------|---------|-------------------------|------------------|-----|
| cbi_m7k_01 | 106 | I3nms,totintra5,zte-cbi | 14 | |
| cbi_m7k_01 | 49 | networkchonburi | 10 | |
| cbi_m7k_01 | 34 | nms-forth160k | 9 | |
| cbi_m7k_01 | 45 | MGMT_WiNet_cbi | 9 | |

ภาพที่ 4-50 หมายเลข VLAN และจำนวนลิงค์ที่ซ้ำกัน

5.3 รายงาน VLAN ที่ไม่ได้เรียนรู้ที่อยู่ MAC

รายงาน VLAN ที่ไม่เรียนรู้ที่อยู่ MAC เลยในระยะเวลาที่กำหนด (ค่าระยะเวลานี้สามารถเปลี่ยนแปลงได้โดยผู้ดูแลระบบ) ตัวอย่างของรายงานแสดงดังภาพที่ 4-51 ประกอบด้วยรายชื่อสวิตช์และจำนวนหมายเลข VLAN ที่ไม่มี MAC โดยเรียงตามลำดับจากมากไปน้อย ผู้ใช้สามารถเรียกดูหมายเลข VLAN ของแต่ละสวิตช์ได้โดยเลือกที่ปุ่ม “Detail” จะแสดงหน้าต่างใหม่ขึ้นมาดังแสดงในภาพที่ 4-52

| Device | IP | จำนวน Vlan ที่ไม่มี MAC | Detail |
|----------------|----------------|-------------------------|--------|
| pty_pty_01 | 10.255.82.251 | 181 | |
| cbi_c3k_01_nec | 10.236.2.250 | 98 | |
| pty_pty_02 | 10.255.82.252 | 90 | |
| cbi_cbi_10 | 10.255.105.203 | 83 | |
| cbi_pnn_02 | 10.255.105.245 | 81 | |

ภาพที่ 4-51 รายงานจำนวน VLAN ของแต่ละสวิตช์ที่ไม่เรียนรู้ที่อยู่ MAC

ภาพที่ 4-52 รายละเอียดของหมายเลข VLAN ที่ไม่มี MAC โดยแต่ละ VLAN จะแสดงพอร์ตที่เป็นสมาชิก และจำนวนครั้งที่ระบบได้ตรวจสอบไว้ หากผู้ใช้ต้องการรีเซ็ตค่าการตรวจสอบ VLAN ใหม่ให้กดปุ่ม “Clear Counter” จะเป็นการลบข้อมูลการนับ MAC ของ VLAN ที่เลือก

| รายละเอียดหมายเลข Vlan ที่ไม่มี MAC-Address ใช้งานเกิน 30 วัน | | | | | |
|---|---------|-------------|--------------|---------|---------------|
| Switch : pty_c3k_01_nec [10.236.73.241] | | | | | |
| Brand : cisco / WS-C3550-12G | | | | | |
| No. | Vlan id | Vlan Name | Port Member | Counter | Action |
| 1 | 191 | dslam_pty2 | Gi0/11 | 142 | Clear Counter |
| 2 | 197 | dslam_pty8 | Gi0/8,Gi0/11 | 142 | Clear Counter |
| 3 | 202 | dslam_pty13 | Gi0/2,Gi0/11 | 142 | Clear Counter |
| 4 | 212 | dslam_pty23 | Gi0/8,Gi0/11 | 142 | Clear Counter |
| 5 | 213 | dslam_pty24 | Gi0/8,Gi0/11 | 142 | Clear Counter |

ภาพที่ 4-52 รายละเอียดแต่ละ VLAN ที่ไม่เรียนรู้ที่อยู่ MAC และพอร์ตที่เป็นสมาชิก

5.4 รายงานพอร์ตสมาชิกที่ไม่ใช้งาน

รายงาน VLAN ที่มีสมาชิกเพียงพอร์ตเดียวหรือไม่มีเลย เนื่องจากอาจเคยใช้งานแต่ถูกลบออกจากรายชื่อข้อมูล VLAN ของสวิตช์ไม่สมบูรณ์ ตัวอย่างของรายงานแสดงดังภาพที่ 4-53

| Vlan Unuse on Interface | | | | | |
|-------------------------|----------------|----------|--|------------|--|
| No. | Node Name | Port | Port Detail | Total Vlan | |
| 3 | pty_pty_01 | Gi1/0/2 | === Up Link to pty_c3k_01_nec === | 66 | |
| 27 | pty_c3k_01_nec | Gi0/11 | t,lan,u,pty_pty_01(10.255.82.251),cbi,utp,29-0 | | |
| 99 | pty_npty_01 | Gi1/0/12 | uplink,pty_naa_lpe1,gi0/20 | | |

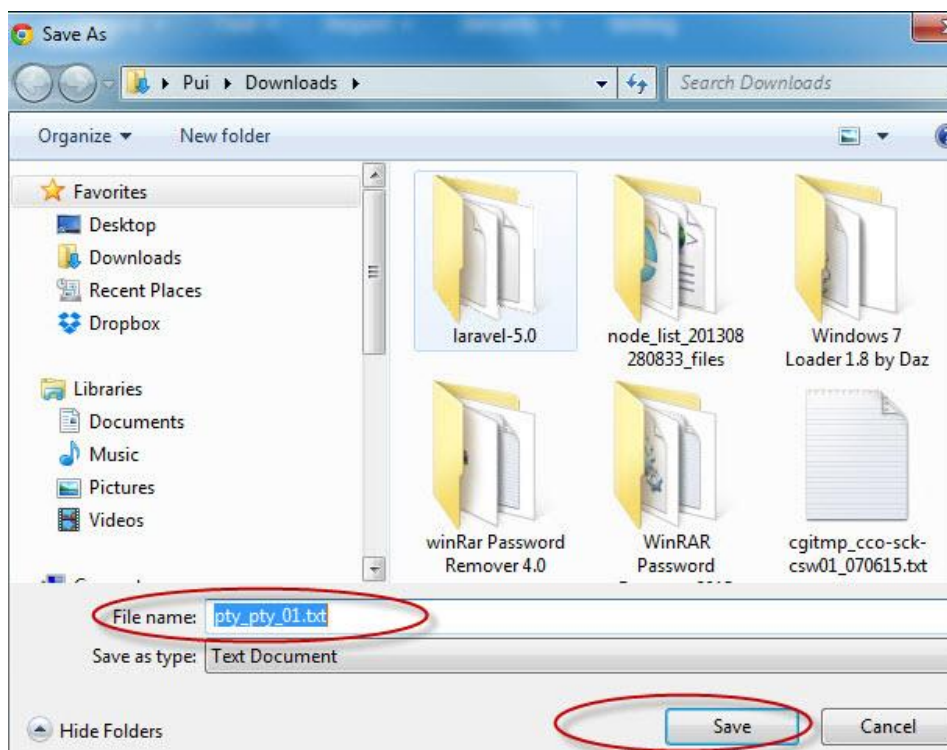
Showing 1 to 3 of 3 entries (filtered from 139 total entries)

VLAN List

355,409,412,488,513,699,726,755,
851,878,929,952,953,954,955,
956,957,958,959,960,961,962,
963,969,986,987,1052,1060,1087,
1200,1501,2100,2109,2206,2391,2401,
2405,2416,2420,2422,2424,2425,2429,
2431,2432,2433,2439,2441,2443,2444,
2446,2449,2456,2463,2490,2499,2521,
2522,2528,2531,2539,2544,2751,2761,
3337,3343

ภาพที่ 4-53 รายงาน VLAN ที่มีสมาชิกเพียงพอร์ตเดียว

จากภาพที่ 4-53 เมื่อผู้ใช้กดปุ่มจำนวน VLAN จะแสดงหมายเลข VLAN ที่ถูกตั้งค่าไว้ที่พอร์ตของสวิตช์ ซึ่ง VLAN เหล่านี้ควรลบออกจากสวิตช์เพราะไม่จำเป็นต่อการใช้งานและเมื่อกดปุ่ม “Download command” ระบบจะสร้างชุดคำสั่งเกี่ยวกับการลบ VLAN ออกจากสวิตช์ในรูปแบบของไฟล์ ให้ผู้ใช้บันทึกไฟล์ดังกล่าวลงในเครื่อง ดังภาพที่ 4-54



ภาพที่ 4-54 การโหลดไฟล์คำสั่งในการลบ VLAN ที่ไม่ใช้งานออกจากสวิตช์

ภาพที่ 4-55 แสดงตัวอย่างคำสั่งจากไฟล์ที่สร้างจากระบบเพื่อใช้ลบ VLAN โดยแบ่งการใช้คำสั่งออกทีละขั้นตอน ผู้ใช้สามารถทำตามขั้นตอนดังกล่าว ช่วยอำนวยความสะดวกให้แก่ผู้ใช้งานเมื่อมี VLAN จำนวนมาก

```

Step-by-Step
1. Telnet ไปที่สวิตช์ด้วยคำสั่ง
telnet 10.255.82.251
ใส่ username และ password

2. เข้าสู่โหมดคอนฟิกด้วยคำสั่ง
conf t

3. เข้าสู่โหมดอินเทอร์เฟซและลบ VLAN ออกจากพอร์ต ด้วยคำสั่ง
interface Gi1/0/2
switchport trunk allowed vlan remove 355,409,412,488,513,699,726,755,851,878,929,952,953,954,955
exit

4. ลบ VLAN ออกจาก vlan database ของสวิตช์ ด้วยคำสั่ง
no vlan 355
no vlan 409
no vlan 412
no vlan 488
no vlan 513

```

ภาพที่ 4-55 ตัวอย่างไฟล์คำสั่งที่ใช้ลบ VLAN

5.5 รายงาน VLAN ที่พอร์ตไม่สอดคล้องกับฐานข้อมูล VLAN

รายงาน “Trunk & Vlan database” แสดงผลการเทียบระหว่างรายการ VLAN ที่ถูกตั้งค่าที่พอร์ตกับรายการ VLAN ที่อยู่ในฐานข้อมูล VLAN ของสวิตช์ เป็นการรายงาน VLAN ที่ไม่มีอยู่จริงในสวิตช์แต่มีประกาศไว้ที่พอร์ต อาจเกิดจากการลบ VLAN ไม่สมบูรณ์หรือตั้งค่าไม่ถูกวิธี ดังภาพที่ 4-56 แสดงชื่อสวิตช์และพอร์ตที่พบ VLAN ไม่สอดคล้อง ไม่มีอยู่จริงในสวิตช์ดังกล่าว

| Node Name | IP | Port | Total vlan | Vlan list |
|--------------|-----------------|--------|------------|--|
| cbi_pnt_lpe1 | 118.174.252.12 | Gi0/22 | 24 | 344,350,357,731,845,864,996,1153,1599,1600,1601,1602,1603,1604,1605,1606,1608,1609,1610,1612,1632,1654,1659,2484 |
| cbi_f7k_01 | 118.174.224.129 | Te9/3 | 15 | 3151,3153,3154,3155,3171,3173,3174,3175,3176,3177,3178,3179,3405,3406,3660 |
| cbi_bbg_lpe1 | 118.174.240.136 | Gi0/22 | 14 | 475,477,478,479,719,739,741,742,743,744,745,746,893,2381 |

ภาพที่ 4-56 VLAN ที่ไม่สอดคล้องระหว่างพอร์ตกับฐานข้อมูล VLAN

5.6 รายงานความหนาแน่นของโฮสต์ต่อ VLAN

รายงาน “MAC per VLAN” คือจำนวนความหนาแน่นของโฮสต์ต่อ VLAN หากมีจำนวนโฮสต์มากเกินไป อาจเกิดบรอดคาสต์จำนวนมาก ซึ่งอาจกระทบต่อประสิทธิภาพการทำงานของสวิตช์ ภาพที่ 4-57 แสดงลำดับรายชื่อสวิตช์ที่มี MAC address ต่อ VLAN ที่มีค่าสูงสุด 10 อันดับ

จากบทความของ Minlan Yu และ Xin Sun (2011) กล่าวว่า เราควรควบคุมจำนวนโฮสต์ต่อ VLAN ให้มีขนาดเหมาะสม เพื่อป้องกันการเกิดบรอดคาสต์หรือมัลติคาสต์ที่เข้ามารบกวน



ภาพที่ 4-57 สวิตช์ที่มี MAC address ต่อ VLAN สูงสุด

5.7 รายงาน CAM Table

ผู้ใช้สามารถสืบค้นค่า MAC address ที่เรียนรู้โดยสวิตช์ โดยเลือกที่เมนู “CAM Table” จะปรากฏตัวเลือกที่ใช้สำหรับค้นหาดังภาพที่ 4-58

Region: เมืองพญา POP: PTY Node: -- All Node --

Vlan: MAC: 00:23:f8:93:5e:f5 Show

ภาพที่ 4-58 หน้าจอการค้นหา MAC address ในระบบ

ภาพที่ 4-58 ผู้ใช้สามารถค้นหา MAC address ได้ตาม Region และ POP โดยที่หากเลือกโหนดเป็น “All Node” หมายถึงค้นหา MAC ที่สวิตช์ทุกตัวใน POP และสามารถระบุ VLAN หรือ MAC ที่ต้องการค้นหาได้ จากตัวอย่างเป็นการค้นหาค่า MAC address ที่มีค่า “00:23:f8:93:5e:f5” (สังเกตว่าผู้ใช้งานต้องใส่ค่า MAC ให้ตรงตามรูปแบบที่กำหนด)

ภาพที่ 4-59 แสดงผลการค้นหาการเรียนรู้ที่อยู่ MAC ซึ่งจะแสดงหมายเลข VLAN ที่ใช้งานและบอกว่า MAC นั้นเป็นของอุปกรณ์ยี่ห้อใด เรียนรู้มาจากสวิตช์และพอร์ตใด

| CAM Table | | | |
|------------|---------|--|-----------|
| Node | Vlan id | MAC Address | Interface |
| pty_m3k_01 | 3123 | 00:23:f8:93:5e:f5 (ZyXEL Communications Corporation) | Gi0/1 |
| pty_pty_06 | 3123 | 00:23:f8:93:5e:f5 (ZyXEL Communications Corporation) | Fa0/10 |

Showing 1 to 2 of 2 entries

ภาพที่ 4-59 ผลที่ได้จากการค้นหา MAC address

6. การตั้งค่า (Setting)

โมดูลนี้ทำหน้าที่เกี่ยวกับการตั้งค่าตัวแปรพื้นฐานที่ใช้อ้างอิงในระบบเช่น การตั้งค่าชื่อจังหวัด, การตั้งชื่อ POP, การจัดการยี่ห้อสวิตช์ โดยการใช้งานในส่วนนี้สำหรับผู้ใช้ที่ได้สิทธิ์เป็นผู้ดูแลระบบเท่านั้น เมื่อผู้ใช้เลือกที่เมนู “Setting” จะปรากฏเมนูย่อยทางด้านขวาดังภาพที่ 4-60

| |
|------------|
| Global |
| Region |
| POP |
| Product |
| Alert Rule |

ภาพที่ 4-60 เมนูที่เกี่ยวข้องกับการตั้งค่าในระบบ

หน้าที่และการทำงานของแต่ละส่วนสามารถอธิบายได้ดังต่อไปนี้

6.1 การตั้งค่าทั่วไป

ภาพที่ 4-61 การตั้งค่าส่วนนี้ทำหน้าที่กำหนดค่าปริยาย (default) ให้แก่อินพุตในระบบช่วยอำนวยความสะดวกให้แก่ผู้ใช้ ไม่ต้องใส่ข้อมูลด้วยตนเองหากค่าเหล่านั้นมีการตั้งค่าที่อุปกรณ์เหมือนกันทั้งหมดในระบบ เช่น ค่า SNMP community, ค่า User และ Password สำหรับใช้ Telnet ไปที่สวิตช์

The screenshot shows a web interface titled "Global Setting". It contains four input fields: "SNMP community" with the value "nmsPublic", "User Telnet" with the value "nmsip", "Password Telnet" with masked characters "*****", and "Enable Password" with masked characters "*****". A green button labeled "Save Change" is located at the bottom left of the form area.

ภาพที่ 4-61 การตั้งค่าตัวแปรที่เป็น default ในระบบ

The screenshot shows a web interface for adding a device. It features a "Product" dropdown menu currently set to "Cisco". Below it are four input fields: "SNMP Community" (nmsPublic), "Telnet Username" (nmsip), "Telnet Password" (masked with asterisks), and "Enable Password" (masked with asterisks). At the bottom, there are two buttons: a white "Back" button and a blue "Add Device" button.

ภาพที่ 4-62 การตั้งค่าที่ Global จะส่งผลต่อหน้าจอการเพิ่มอุปกรณ์

6.2 การตั้งค่า Region

การจัดกลุ่มของสวิตช์ในระบบมีลักษณะเป็นแบบลำดับชั้น โดยแบ่งออกเป็น 2 ระดับ คือ Region และ POP ในหนึ่ง Region อาจมีได้หลาย POP ผู้ดูแลระบบสามารถจัดการข้อมูล Region ได้โดยเลือกที่เมนู “Region” จะแสดงรายละเอียดดังภาพที่ 4-63 ผู้ดูแลระบบสามารถเพิ่มข้อมูล Region ใหม่ได้โดยกดปุ่ม Add ส่วนการแก้ไขหรือลบข้อมูลทำได้โดยกดปุ่ม “Edit” หรือปุ่ม “Delete” ของแต่ละแถว

| ID | Region Name | Action |
|----|-------------|---|
| 1 | ชลบุรี | Edit Delete |
| 2 | เมืองพัทยา | Edit Delete |

ภาพที่ 4-63 หน้าจอจัดการข้อมูล Region

6.3 การตั้งค่า POP

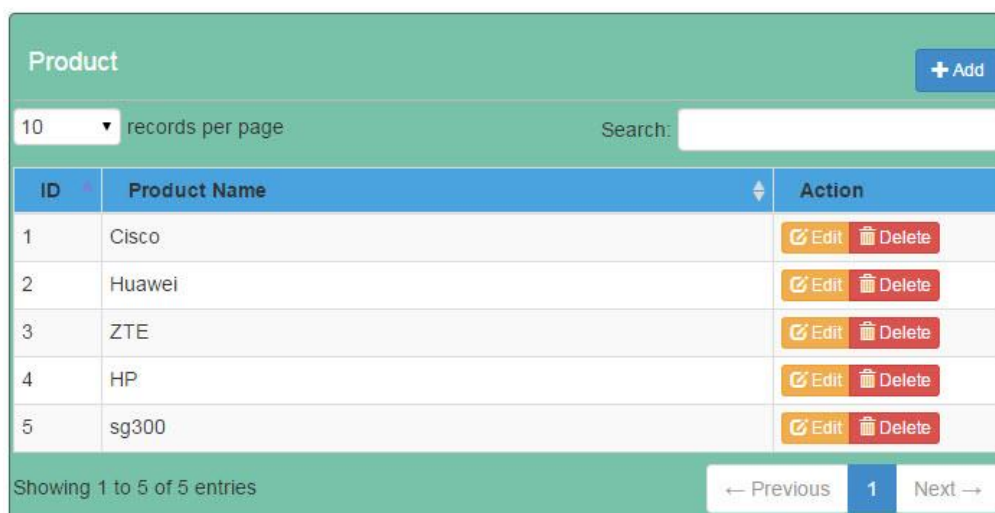
POP หรือ Point of presence คือจุดที่อุปกรณ์ตั้งอยู่ในพื้นที่เดียวกับผู้ใช้งาน สวิตช์ที่มีรูทบริดจ์ (Root bridge) เดียวกันจะถูกจัดให้อยู่ในกลุ่ม POP เดียวกัน ซึ่ง POP จะอยู่ภายใต้ Region ดังภาพที่ 4-64 POP ชื่อ CBI และ LBG ถูกจัดให้อยู่ใน Region ชลบุรี เนื่องจากในชลบุรี มีสวิตช์ที่ทำหน้าที่เป็นรูทบริดจ์อยู่ 2 ตัว ทำให้ต้องแยกออกเป็น 2 POP ขึ้นตอนและวิธีการจัดการข้อมูลใน POP มีลักษณะคล้ายกับการจัดการข้อมูลใน Region

| ID | Name | Region | Action |
|----|------|------------|---|
| 1 | CBI | ชลบุรี | Edit Delete |
| 2 | PTY | เมืองพัทยา | Edit Delete |
| 3 | LBG | ชลบุรี | Edit Delete |

ภาพที่ 4-64 หน้าจอจัดการข้อมูล POP

6.4 การตั้งค่ายี่ห้ออุปกรณ์

กรณีมีการติดตั้งสวิตช์ยี่ห้อใหม่ในเครือข่าย ผู้ดูแลระบบจะต้องเพิ่มยี่ห้อสวิตช์เข้าไปในฐานข้อมูลก่อน โดยเลือกที่เมนู “Product” หน้าจอจัดการยี่ห้อจะปรากฏขึ้น ดังภาพที่ 4-65 เมื่อต้องการเพิ่มยี่ห้อใหม่ให้กดปุ่ม “Add” หากต้องการแก้ไขหรือลบข้อมูลให้กดปุ่ม “Edit” หรือ ปุ่ม “Delete” ของแต่ละแถวที่ต้องการ



| ID | Product Name | Action |
|----|--------------|---|
| 1 | Cisco | Edit Delete |
| 2 | Huawei | Edit Delete |
| 3 | ZTE | Edit Delete |
| 4 | HP | Edit Delete |
| 5 | sg300 | Edit Delete |

ภาพที่ 4-65 หน้าจอจัดการยี่ห้อสวิตช์

6.5 การตั้งค่าการแจ้งเตือน

ระบบค้นหาโครงสร้าง VLAN อนุญาตให้ผู้ดูแลระบบสามารถตั้งค่าเงื่อนไขสำหรับการแจ้งเตือนเมื่อมีเหตุการณ์ตรงกับเงื่อนไขที่ตั้งค่าไว้ รวมถึงเงื่อนไขเพื่อใช้สำหรับสร้างรายงานโดยเงื่อนไขที่ระบบใช้ตรวจสอบ VLAN ในเครือข่ายมีดังนี้

จำนวนที่อยู่ MAC ต่อหนึ่ง VLAN มากกว่า 255 ที่อยู่

ระดับของหมายเลข VLAN ที่ถูกใช้ไปในสวิตช์ (หน่วยเป็นร้อยละ) มากกว่า ร้อยละ 80

ระยะเวลาที่ VLAN ไม่มีการใช้งานในสวิตช์นั้น เป็นเวลาไม่ต่ำกว่า 120 วัน

จำนวน hop ของสวิตช์สูงสุดโดยเริ่มนับจากรูทบริดจ์ (5 hop)

การเข้าสู่หน้าจอตั้งค่าการแจ้งเตือน ให้ผู้ดูแลระบบเลือกที่เมนู “Alert Rule” จะแสดงหน้าจอ ดังภาพที่ 4-66 สามารถเปลี่ยนค่าเงื่อนไขตามที่ต้องการ ค่าทั้งหมดจะถูกบันทึกเมื่อกดปุ่ม “Save change”

Alert Rule

Maximum Host per Vlan

(นับจำนวน mac address ต่อ vlan)

Vlan Usage Threshold

(การใช้งาน Vlan ที่มีค่าเกินที่กำหนด : %)

Day no MAC learning

(ระยะเวลาที่ไม่มี MAC เข้ามา : วัน)

Maximum Hop count

[Save Change](#)

ภาพที่ 4-66 การตั้งค่าแจ้งเตือนในระบบ

6.6 การจัดการผู้ใช้งาน

การจัดการผู้ใช้และกำหนดสิทธิ์ เมื่อผู้ดูแลระบบเลือกที่เมนู “Security”→“User Management” จะแสดงรายชื่อผู้ใช้งานทั้งหมดในระบบ ซึ่งข้อมูลในตารางจะบอกถึงสิทธิ์ที่ได้รับ และสถานะของผู้ใช้ว่าใช้งานได้ปกติ (แทนด้วย Y) หรือถูกระงับการใช้งานไว้ (แทนด้วย N) วันเวลาการเข้าใช้งานครั้งล่าสุด ดังในภาพที่ 4-67

| User Management + Add User | | | | | | | |
|---|----------------|------------------------------|--------|----------|--------|---------------------|---|
| 10 records per page | | Search: <input type="text"/> | | | | | |
| User | ชื่อ สกุล | Mobile | Role | Province | Status | Last login | Action |
| admin | System Admin | | Admin | ชลบุรี | Y | 2015-06-10 11:29:24 | Edit Delete |
| guest | Guest ชลบุรี | | Viewer | ชลบุรี | Y | 2013-12-13 01:34:25 | Edit Delete |
| noppadol | นพปฎล เจยศิริ | 0868271617 | Admin | ชลบุรี | Y | 2015-05-30 14:50:16 | Edit Delete |
| somsak | Somsak Oapirak | | Viewer | แหลมฉบัง | Y | 2015-06-02 14:02:13 | Edit Delete |

Showing 1 to 4 of 4 entries ← Previous **1** Next →

ภาพที่ 4-67 ส่วนจัดการผู้ใช้งานในระบบ

ภาพที่ 4-68 การเพิ่มผู้ใช้งานและกำหนดสิทธิ์เข้าใช้งานในระบบ

เมื่อต้องการเพิ่มผู้ใช้งานในระบบให้กดปุ่ม “Add User” จะปรากฏหน้าจอดังภาพที่ 4-68 เมื่อต้องการเพิ่มผู้ใช้งานใหม่ ผู้ดูแลระบบจำเป็นต้องใส่ชื่อผู้ใช้งานที่ไม่ซ้ำกับชื่อเดิมในระบบ ใส่รหัสผ่านและยืนยันรหัสผ่านให้เหมือนกันทั้งสองช่อง ใส่ชื่อและนามสกุลของผู้ใช้งาน ส่วนการกำหนดสิทธิ์ให้แก่ผู้ใช้งานให้เลือก 2 ระดับคือผู้ดูแลระบบ (Admin) และผู้ใช้งานทั่วไป (Viewer) เมื่อใส่ข้อมูลที่เป็นครบแล้วให้กดปุ่ม “Create User”

หากผู้ใช้งานใส่ข้อมูลไม่ครบหรือไม่ถูกต้อง เช่น ใส่ชื่อที่มีผู้ใช้งานอยู่แล้วในระบบใส่ Password ไม่เหมือนกันทั้ง 2 ช่อง ไม่ใส่ชื่อและนามสกุล เมื่อกดปุ่ม “Create User” ระบบจะตรวจสอบและแจ้งข้อผิดพลาดให้ผู้ใช้งานทราบ ดังแสดงในภาพที่ 4-69

ภาพที่ 4-69 การแจ้งข้อผิดพลาดเนื่องจากใส่ข้อมูลผู้ใช้งานไม่ครบ ไม่ถูกต้อง

เมื่อแก้ไขข้อมูลผู้ใช้ถูกต้องแล้ว หากไม่มีข้อผิดพลาดระบบจะแจ้งผลการดำเนินการเพิ่มข้อมูลผู้ใช้ ดังแสดงในภาพที่ 4-70



ภาพที่ 4-70 หน้าจอหลังจากเพิ่มผู้ใช้งานสำเร็จ

สรุปผลการนำโปรแกรมไปใช้ตรวจสอบการตั้งค่า VLAN

การทดสอบระบบค้นหาโครงสร้าง VLAN ผู้พัฒนานำไปทดสอบกับเครือข่ายบริการลูกค้าของบริษัททีโอที โดยทดสอบในพื้นที่ให้บริการ 3 แห่งคือ ชลบุรี แลพมฉบังและพัทยา ประกอบด้วยจำนวนสวิตช์และ VLAN แสดงในตารางที่ 4-1

ตารางที่ 4-1 จำนวนสวิตช์และจำนวน VLAN ที่ใช้ในการทดสอบ

| ลำดับ | POP | Root bridge | จำนวนสวิตช์ | จำนวน VLAN |
|-------|-----|-------------|-------------|------------|
| 1 | CBI | cbi_m7k_01 | 68 | 941 |
| 2 | LBG | lbg_pe_01 | 15 | 265 |
| 3 | PTY | pty_m7k_01 | 57 | 1239 |

ผลการทดสอบ โปรแกรม เราพบความผิดพลาดซึ่งเกิดจากการตั้งค่า VLAN ไม่เหมาะสมระหว่างพอร์ตทรีนค์ ซึ่งสามารถแบ่งความผิดพลาดได้ 3 ประเภทคือ VLAN สูญหาย, VLAN ที่ไม่จำเป็นและ VLAN ที่ไม่สอดคล้อง สามารถอธิบายผลที่ได้จาก โปรแกรมดังต่อไปนี้

1. VLAN สูญหาย

เมื่อใช้ขั้นตอนวิธีค้นหาในแนวคิดตรวจสอบ VLAN ในแต่ละพื้นที่บริการ ระบบพบว่า มี VLAN สูญหายดังแสดงในตารางที่เมื่อพิจารณาในแต่ละ VLAN พบว่ามากกว่า 90% ของ VLAN ที่พบปัญหาเกิดจากการตั้งค่าพอร์ตที่เป็นสมาชิกของ VLAN มากเกินกว่าที่ใช้จริง ซึ่งอาจเกิดจากการไม่ควบคุมการตั้งค่า VLAN ในพอร์ตทรีนค์ ปล่อยให้ VLAN วิ่งผ่านพอร์ตเป็นช่วงกว้างมากเกินไป

ตารางที่ 4-2 จำนวน VLAN ที่สูญหายของแต่ละพื้นที่

| ลำดับ | POP | VLAN ทั้งหมด | VLAN สูญหาย | คิดเป็นร้อยละ |
|-------|-----|--------------|-------------|---------------|
| 1 | CBI | 941 | 366 | 38.89 |
| 2 | LBG | 265 | 146 | 55.09 |
| 3 | PTY | 1239 | 315 | 25.42 |

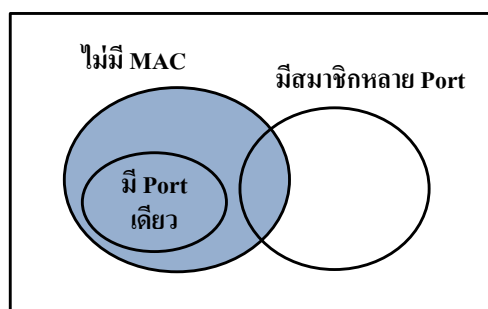
จากรายงานนี้ทำให้ผู้ดูแลเครือข่ายทราบว่า มี VLAN จำนวนมากที่ถูกตั้งค่าไว้ที่พอร์ตของสวิตช์ด้านบน (Upstream switch) แต่ VLAN เหล่านั้นไม่มีผู้ใช้งานอยู่จริง (สังเกตได้จากสวิตช์ปลายทางไม่มีการตั้งค่า VLAN ไว้) จึงควรแก้ไขโดยลบ VLAN ที่พอร์ตเหล่านั้นออก เพื่อช่วยปรับปรุงความถูกต้องของเส้นทาง

2. VLAN ที่ไม่จำเป็น

การตรวจสอบ VLAN ที่ไม่จำเป็นต่อการใช้งาน นอกจากเป็นการลดปริมาณข้อมูล (Traffic) ที่ไม่เกี่ยวข้องไม่ให้เข้ามายังสวิตช์แล้ว ยังช่วยลดการใช้หน่วยความจำ หน่วยประมวลผลของสวิตช์ เช่น โพรโทคอล Spanning tree สวิตช์ต้องคำนวณทุก VLAN (Spanning แบบ PVST รับได้สูงสุด 128 VLAN) หากสามารถลดจำนวน VLAN ที่ไม่จำเป็นลงจะทำให้สวิตช์มีประสิทธิภาพทำงานที่ดีขึ้น ซึ่งการค้นพบ VLAN ที่ไม่จำเป็น ระบบใช้วิธีตรวจสอบตามเงื่อนไข 3 รูปแบบคือ

- 1) VLAN ที่มีสมาชิกเพียงพอร์ตเดียว
- 2) VLAN ที่ไม่มี MAC
- 3) VLAN ที่มีพอร์ตสมาชิกมากเกินไป

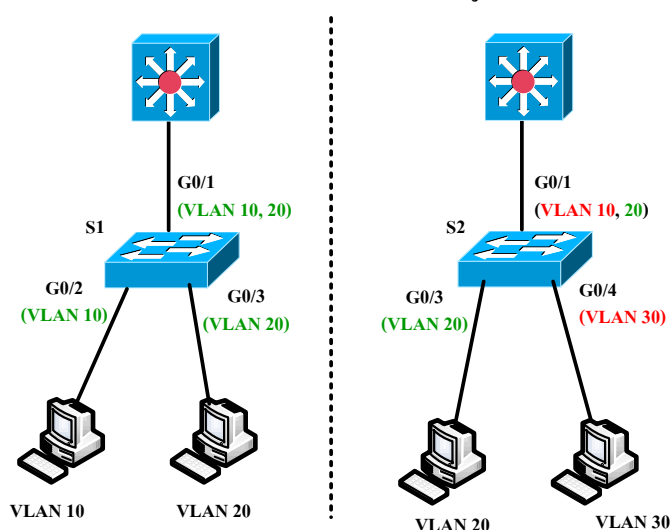
หากอธิบายด้วยแผนภาพเวนน์ (ดังภาพที่ 4-71) แสดงความเกี่ยวเนื่องกันระหว่างเงื่อนไข 3 แบบ สำหรับตรวจสอบ VLAN ที่ไม่จำเป็น



ภาพที่ 4-71 แผนภาพเวนน์-ออยเลอร์แสดงความสัมพันธ์ของ VLAN ที่ไม่จำเป็น

2.1 VLAN ที่มีพอร์ตสมาชิกเพียงพอร์ตเดียว

เงื่อนไขนี้ เกิดจากแนวคิดที่ว่า พอร์ตที่เป็นสมาชิกของ VLAN จะต้องมียังน้อย 2 พอร์ต คือพอร์ต Uplink และพอร์ต Downlink หรือพอร์ตที่มีผู้ใช้งาน ตารางที่ 4-3 แสดงสวิตช์ที่ระบบพบว่ามีค่า VLAN พอร์ตเดียวสูงสุดในจำนวนนี้มีสวิตช์ cbi_pnn_02 และ cbi_pnn_04 ซึ่งพบ VLAN ไม่ใช้งานเกินกว่าร้อยละ 50 เมื่อตรวจสอบแล้วพบว่าสาเหตุคือการเปลี่ยนแปลงการเชื่อมต่อ (ย้ายสวิตช์บางตัวออกไปแต่ไม่ลบ VLAN ออกจากพอร์ต) โดยส่วนใหญ่จะเป็นพอร์ตด้าน Uplink เนื่องจากร้อยละ 50 ของ VLAN เหล่านี้ยังถูกใช้งานอยู่ เราจึงควรลบ VLAN ที่พอร์ตเหล่านี้ออกไปเพื่อป้องกันปริมาณข้อมูลที่ไม่จำเป็นวิ่งผ่านเข้ามายังสวิตช์



ภาพที่ 4-72 ตัวอย่าง VLAN ที่มีสมาชิกเพียงพอร์ตเดียว

ภาพที่ 4-72 (ซ้าย) แสดงตัวอย่าง VLAN ที่มีจำนวนพอร์ตสมาชิกอย่างน้อย 2 พอร์ต ที่สวิตช์ S1 VLAN 10 มีพอร์ต Gi0/1, Gi0/2 เป็นสมาชิกในขณะที่สวิตช์ S2 (ขวา) VLAN 10 มีเพียงพอร์ต Gi0/1 เป็นสมาชิกเนื่องจากไม่มีโฮสต์ใดใช้งานเลย เช่นเดียวกับ VLAN 30 ซึ่งมีพอร์ต Gi0/4 เป็นสมาชิกเพียงพอร์ตเดียวเช่นกัน ควรลบ VLAN 10 และ VLAN 30 ออกจากสวิตช์ S2

ตารางที่ 4-3 สวิตช์ที่พบ VLAN เพียงพอร์ตเดียวสูงสุด 5 อันดับ

| ลำดับ | ชื่อสวิตช์ | พอร์ต | VLAN ทั้งหมด | VLAN ที่พบปัญหา | คิดเป็นร้อยละ |
|-------|------------|---------|--------------|-----------------|---------------|
| 1 | lbg_lbg_01 | Gi0/1 | 210 | 82 | 39.04 |
| 2 | cbi_pnn_02 | Gi0/24 | 147 | 80 | 54.42 |
| 3 | cbi_pnn_04 | Gi0/16 | 132 | 74 | 56.06 |
| 4 | pty_pty_02 | Gi0/2 | 164 | 67 | 40.85 |
| 5 | pty_pty_01 | Gi1/0/2 | 258 | 67 | 25.97 |

2.2 VLAN ที่ไม่มี MAC address

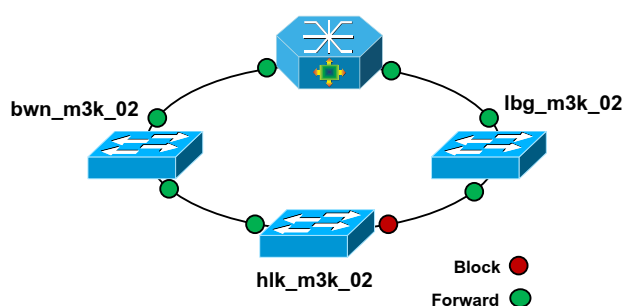
เราสรุปจำนวน VLAN ที่ไม่มีการใช้งาน โดยดูจากสถิติของจำนวน MAC address ในแต่ละ VLAN ที่ไม่เปลี่ยนแปลงหรือมีค่าเป็นศูนย์ แสดงดังในตารางที่ 4-4 ซึ่งประกอบด้วยชื่อสวิตช์และจำนวน VLAN ที่ไม่มี MAC address สูงสุด 5 อันดับ เมื่อพิจารณาแต่ละสวิตช์ พบว่า สวิตช์ลำดับที่ 1 และ 2 เป็นสวิตช์ที่ติดตั้งใช้งานมานาน มีจำนวน VLAN สะสมเกิดขึ้นปัญหาส่วนหนึ่งเกิดจากผู้ใช้ที่ยกเลิกใช้งานแล้วแต่ไม่ได้ลบ VLAN ออกจากสวิตช์ การลบ VLAN ที่ไม่สมบูรณ์ เช่นลบเฉพาะ VLAN ที่อยู่ใน Core switch แต่ไม่ตามลบที่สวิตช์ปลายทาง ทำให้เกิด VLAN ไม่ใช้งานค้างอยู่ในสวิตช์

ตารางที่ 4-4 สวิตช์ที่ไม่มี VLAN ใช้งานและจำนวน VLAN ที่ไม่ได้เรียนรู้ที่อยู่ MAC

| ลำดับ | ชื่อสวิตช์ | VLAN ทั้งหมด | VLAN ไม่มี MAC | คิดเป็นร้อยละ |
|-------|----------------|--------------|----------------|---------------|
| 1 | pty_c3k_01_nec | 275 | 162 | 58.90 |
| 2 | lbg_lbg_01 | 210 | 142 | 67.62 |
| 3 | nmd2_m3k_02 | 145 | 128 | 88.28 |
| 4 | lbg_m3k_02 | 223 | 121 | 54.26 |
| 5 | nmd3_m3k_02 | 140 | 76 | 54.28 |

ส่วนสวิตช์ nmd2_m3k_02 พบ VLAN ไม่มี MAC address สูงถึง 88.28 % เมื่อตรวจสอบพบว่าเป็นการนำสวิตช์ที่เคยใช้งานจากที่อื่นกลับมาใช้ใหม่แต่ไม่ลบ VLAN เดิมออกจากฐานข้อมูลของสวิตช์จึงพบ VLAN ไม่ใช้งานสูงกว่าสวิตช์ตัวอื่น

กรณีสวิตช์บางตัวมีเส้นทางที่เชื่อมต่อกันแบบวงแหวน (Ring topology) เพื่อทำเป็นเส้นทางสำรองตามกฎของ Spanning tree บางพอร์ตจะอยู่ในสถานะเตรียมพร้อมไม่มีการรับส่งข้อมูลทำให้ไม่พบ MAC address ในบาง VLAN ดังนั้นสวิตช์ที่ต่อในลักษณะครบรูป เช่น สวิตช์ lbg_m3k_02 มีการต่อกันดังแสดงในภาพที่ 4-72 การคำนวณของ Spanning tree พอร์ตของสวิตช์ hlk_m3k_02 ที่ต่อกับ lbg_m3k_02 อยู่ในสถานะ block จึงไม่มี MAC address ของ VLAN ที่มาจากสวิตช์ bwn_m3k_02 และสวิตช์ hlk_m3k_02 วิ่งมาถึงสวิตช์ lbg_m3k_02 ได้ จึงเสมือนว่ามี VLAN ที่ไม่มี MAC อยู่จำนวนมาก (ผู้ดูแลไม่ครบรูป VLAN ในกรณีนี้ออก)



ภาพที่ 4-73 การต่อเป็นวงแหวนของสวิตช์ lbg_m3k_02

2.3 VLAN ที่มีเส้นทางหรือพอร์ตที่เป็นสมาชิกมากเกินไป

รายงาน VLAN ที่มีพอร์ตที่เป็นสมาชิกเกินกว่าความต้องการ เป็นวิธีการหนึ่งที่จะตรวจสอบการแพร่กระจาย VLAN ซึ่งอาจไม่มีผู้ใช้ที่สวิตช์ปลายทาง ยกตัวอย่างการใช้งาน VLAN ของบริษัทที่โอที บริการในกลุ่มลูกค้า IP-VPN มีลักษณะใช้หนึ่ง VLAN ต่อหนึ่งลูกค้า ดังนั้น VLAN ในกลุ่มดังกล่าวจะมีพอร์ตที่เป็นสมาชิก ออกจาก Core switch เพียงพอร์ตเดียวเท่านั้น (อาจมีมากกว่าหนึ่งพอร์ตกรณีสวิตช์นั้นมีเส้นทางสำรอง) ข้อมูลที่ได้จากรายงานนี้จึงเสมือนเป็นการแสดงให้เห็นผู้ดูแลระบบเห็นว่ามี VLAN ใดบ้างที่กระจายออกไปตามพอร์ตต่าง ๆ โดยเริ่มจาก Core switch เพื่อให้สามารถกำจัดหรือจัดเส้นทาง VLAN ให้มีทิศทางที่ถูกต้องตามที่มีการใช้งานจริง

3. VLAN ที่ไม่สอดคล้อง

ผลของรายงาน VLAN ที่ไม่สอดคล้องระหว่างพอร์ตกับฐานข้อมูล VLAN ของสวิตช์ (VLAN database) อาจไม่มีส่วนช่วยในด้านการปรับปรุงประสิทธิภาพการทำงานของสวิตช์ แต่เป็นการตรวจสอบความถูกต้องของพอร์ตสวิตช์ให้มีเฉพาะ VLAN ที่มีอยู่จริงในสวิตช์ ลดความสับสน

เมื่อต้องแก้ปัญหาที่อาจเกิดขึ้น ช่วยให้อ่านค่าพอร์ตสวิตช์เข้าใจง่ายเมื่อตัด VLAN ที่ไม่เกี่ยวข้อง ออก จำนวนสวิตช์และจำนวน VLAN ที่พบในรายงานนี้แสดงให้เห็นถึงการปฏิบัติที่ผิดวิธี ในขั้นตอนการลบ VLAN โดยเฉพาะในสวิตช์ Cisco เมื่อต้องการลบ VLAN ออกจากสวิตช์จะมี 2 ขั้นตอนคือ 1) ลบ VLAN ออกจากพอร์ตที่เป็นสมาชิกทั้งหมด 2) ลบ VLAN ที่อยู่ในฐานข้อมูล สวิตช์ ซึ่งผู้ปฏิบัติงานบางคนอาจไม่รู้หรือไม่ทำตามขั้นตอน ทำให้มี VLAN ตกค้างอยู่ที่พอร์ต ของสวิตช์

สรุปผลหลังดำเนินการตรวจสอบการตั้งค่า VLAN โดยระบบที่นำเสนอ

1. จำนวน VLAN ที่ลดลง

ตารางที่ 4-5 เปรียบเทียบจำนวน VLAN ก่อนและหลังนำระบบเข้าไปตรวจสอบ

| ลำดับ | ชื่อสวิตช์ | VLAN | | ลดลง (%) |
|-------|----------------|---------------|---------------|----------|
| | | ก่อนดำเนินการ | หลังดำเนินการ | |
| 1 | cbi_cbi_10 | 231 | 116 | 49.78 |
| 2 | cbi_pnn_02 | 147 | 51 | 65.31 |
| 3 | cbi_pnn_04 | 132 | 28 | 78.79 |
| 4 | cbi_bbg_zte1 | 150 | 98 | 65.33 |
| 5 | lbg_c3k_02 | 235 | 120 | 51.06 |
| 6 | lbg_lbg_01 | 210 | 120 | 42.85 |
| 7 | lbg_m3k_02 | 223 | 213 | 15.70 |
| 8 | pty_c3k_01_nec | 275 | 102 | 62.91 |
| 9 | pty_pty_01 | 258 | 73 | 71.70 |
| 10 | pty_pty_02 | 164 | 87 | 46.95 |

ข้อมูลจากตารางที่ 4-5 แสดงร้อยละของจำนวน VLAN ที่เหลือหลังจากที่ใช้ระบบเข้าไป ตรวจสอบการตั้งค่า VLAN และกำจัด VLAN ที่ไม่จำเป็นหรือตั้งค่าไม่ถูกต้องออกจากสวิตช์ เห็นได้ว่าสวิตช์บางตัวสามารถลด VLAN ได้ถึง 78% เนื่องจากการเปลี่ยนแปลงเครือข่าย และย้ายการเชื่อมต่อสวิตช์แล้วไม่เคยจัดการลบ VLAN ที่ไม่ใช้งานออก

2. ตัวอย่างปริมาณบรอดคาสต์

ข้อมูลในตารางที่ 4-5 แสดงสถิติการวัดปริมาณการจราจรข้อมูลประเภทยูนิคาสต์และบรอดคาสต์ที่ Core switch 3 แห่งโดยเลือกพอร์ตที่มีการใช้งานและมีจำนวน VLAN ก่อนข้างสูงเก็บข้อมูลในช่วงเดือนธันวาคม พ.ศ. 2557 จนถึงเดือนพฤษภาคม พ.ศ. 2558 ซึ่งมีการลบ VLAN ที่ไม่ถูกต้องในช่วงเดือนเมษายนถึงเดือนพฤษภาคม ผลที่ได้คือสวิตช์ cbi_m7k_01 ที่พอร์ต Gi3/7 ปริมาณบรอดคาสต์มีแนวโน้มลดลงเล็กน้อยเมื่อเทียบกับข้อมูลแบบยูนิคาสต์ ในขณะที่สวิตช์ pty_m7k_01 ที่พอร์ต Gi3/20 ปริมาณบรอดคาสต์มีแนวโน้มค่อย ๆ ลดลง ในขณะที่ปริมาณข้อมูลแบบยูนิคาสต์กลับเพิ่มขึ้น แสดงให้เห็นว่าการจัดการ VLAN ที่สวิตช์ pty_m7k_01 ส่งผลที่ดีขึ้น แต่ที่สวิตช์ lbg_pe_03 การจัดการ VLAN ไม่ส่งผลต่อการลดจำนวนบรอดคาสต์ลดลงได้

ตารางที่ 4-6 ตัวอย่างปริมาณบรอดคาสต์

| | cbi_m7k_01 | | lbg_pe_01 | | pty_m7k_01 | |
|----------|------------|-----------|-----------|-----------|------------|-----------|
| | (Gi3/ 17) | | (Po44) | | (Gi3/ 20) | |
| | Unicast | Broadcast | Unicast | Broadcast | Unicast | Broadcast |
| ธ.ค. 57 | 33340 | 25.75 | 55540 | 6.89 | 34700 | 9.80 |
| ม.ค. 58 | 32770 | 19.74 | 54560 | 7.02 | 35460 | 10.24 |
| ก.พ. 58 | 35120 | 19.34 | 56690 | 7.12 | 36540 | 11.56 |
| มี.ค. 58 | 35610 | 18.93 | 62860 | 7.35 | 37850 | 11.80 |
| เม.ย. 58 | 34570 | 18.65 | 63780 | 10.00 | 38980 | 9.34 |
| พ.ค. 58 | 34130 | 18.82 | 64470 | 10.00 | 39280 | 6.37 |

หมายเหตุ หน่วยเป็นแพ็กเกตต่อวินาที (pps)

ประเมินผลความถูกต้องของระบบ

จากรายงานในหัวข้อ VLAN สูญหาย, VLAN ที่มีพอร์ตสมาชิกเดียว และ VLAN ไม่มีที่อยู่ MAC เพื่อประเมินความถูกต้องของระบบ ผู้พัฒนาจึงใช้คำสั่งแบบ Command-line เปรียบเทียบการตั้งค่า VLAN กับข้อมูลในรายงานว่าให้ผลตรงกันหรือไม่ โดยข้อมูลการตั้งค่า VLAN ขณะที่ดำเนินการทดสอบมีจำนวนทั้งสิ้น 26,573 แถว ระยะเวลาที่ใช้ในการประมวลผลของแต่ละรายงานแสดงในตารางที่ 4-7

ตารางที่ 4-7 ค่าประสิทธิภาพความถูกต้องของระบบ

| ประเภทรายงาน | VLAN สูญหาย | VLAN มีพอร์ตสมาชิกเดียว | VLAN ไม่มี MAC |
|-----------------------|-------------|-------------------------|----------------|
| เวลาประมวลผล (วินาที) | 167 | 55 | 130 |
| % ความถูกต้อง | 94.083 % | 100 % | 96.561 % |
| % ความผิดพลาด | 5.907 % | 0 | 3.429 % |

จากตารางที่ 4-7 ความถูกต้องในด้านการค้นหา VLAN สูญหายมีค่าเป็น 94.083% ความผิดพลาดบางส่วนเกิดจากสวิตช์ที่ไม่สามารถสอบถามโดยใช้โปรโตคอล SNMP ต้องนำเข้าข้อมูล VLAN จากไฟล์คอนฟิกทำให้ข้อมูลบางส่วนไม่ถูกต้อง เช่น พอร์ต Gi0/23 และ Gi0/24 มีการรวมลิงก์แบบ port aggregation เพื่อเพิ่มแบนด์วิดท์ จะมีพอร์ตใหม่เกิดขึ้นเรียกว่า Portchannel (Po1) หากอ่านข้อมูลจากไฟล์คอนฟิกจะเก็บข้อมูลสมาชิก VLAN มาทั้ง 3 พอร์ต (Gi0/23, Gi0/24 และ Po1) ซึ่งตามจริงแล้วควรเป็นพอร์ตเดียวคือพอร์ต Po1 พอร์ตที่เกินมา (Gi0/23, Gi0/24) ระบบจึงเข้าใจผิดว่าเป็นพอร์ตที่มี VLAN สูญหาย

ตารางที่ 4-8 สรุปผลการทำงานของระบบ

| ฟังก์ชันการทำงาน | ผลลัพธ์ | | หมายเหตุ |
|---|---------|--------|-------------|
| | ได้ | ไม่ได้ | |
| 1. การเก็บจำนวน VLAN ในแต่ละสวิตช์ | ✓ | | |
| 2. การแสดง VLAN ที่เป็นสมาชิกของพอร์ตสวิตช์ | ✓ | | |
| 3. การแสดง MAC address ที่กำลังใช้งาน | ✓ | | เฉพาะ Cisco |
| 4. การแสดงผังภาพ VLAN | ✓ | | |
| 5. การสรุป VLAN ที่สูญหาย | ✓ | | |
| 6. ตรวจสอบ VLAN ที่ไม่ได้ใช้งาน | ✓ | | |
| 7. ตรวจสอบหมายเลข VLAN ที่ไม่สอดคล้อง | ✓ | | |
| 8. การแจ้งเตือน VLAN ที่มีผู้ใช้งานหนาแน่น | ✓ | | |

ตารางที่ 4-8 สรุปฟังก์ชันการทำงานของระบบค้นหาโครงสร้าง VLAN ที่สามารถ
ตอบสนองการทำงานต่อผู้ใช้งาน

บทที่ 5

สรุปผล และข้อเสนอแนะ

สรุปผล

งานนิพนธ์ฉบับนี้นำเสนอการพัฒนากระบวนการค้นหาโครงสร้าง VLAN ในเครือข่าย เพื่อช่วยปรับปรุงประสิทธิภาพการให้บริการ โดยใช้วิธีรวบรวมข้อมูล VLAN ผ่านโพรโทคอล SNMP ซึ่งผู้พัฒนาแสดงการหาค่า OID ที่เกี่ยวกับการทำงานของ VLAN เช่น หมายเลข VLAN, พอร์ตที่เป็นสมาชิก VLAN และการเรียนรู้ที่อยู่ MAC โดยทดลองกับสวิตช์ 3 ยี่ห้อ คือ Cisco, Huawei และ ZTE (เนื่องจาก OID เกี่ยวกับ VLAN เป็นข้อมูลเฉพาะราย OID แต่ละยี่ห้อจะไม่เหมือนกัน) ค่า OID ที่ตอบกลับมาจากแต่ละยี่ห้อจะถูกนำมาใช้ในการวางแผนและออกแบบระบบ เพื่อนำข้อมูล VLAN มาวิเคราะห์การตั้งค่า VLAN ในเครือข่าย

การนำระบบค้นหาโครงสร้าง VLAN ไปทดลองใช้กับเครือข่ายของบริษัทที่โอที จำกัด (มหาชน) ในพื้นที่ให้บริการชลบุรี แหลมฉบัง และพัทฯ ซึ่งผลลัพธ์ที่ได้จากรายงานแสดงให้เห็นถึงปัญหาที่เกิดจากการตั้งค่า VLAN สามารถแบ่งออกได้ 3 ประเภทคือ

1. VLAN สูญหาย พบว่าส่วนใหญ่เกิดจากการตั้งค่าพอร์ตที่เป็นสมาชิก VLAN มากกว่าที่ใช้งานจริง โดยที่สวิตช์ปลายทางไม่มีการตั้งค่า VLAN นั้นไว้
2. VLAN ที่ไม่จำเป็น จากการทดลองพบว่ามี VLAN ที่ไม่ได้ใช้งานเป็นจำนวนมาก ซึ่งเกิดจากการยกเลิกการใช้งานหรือเปลี่ยนแปลงการเชื่อมต่อเครือข่าย ควรลบ VLAN เหล่านี้ ออกเพื่อช่วยลดปริมาณข้อมูลที่ไม่เกี่ยวข้องไม่ให้เข้ามายังสวิตช์
3. VLAN ที่ไม่สอดคล้อง เป็นการตรวจสอบความถูกต้องของพอร์ตสวิตช์ ช่วยรายงาน VLAN ที่ไม่เกี่ยวข้องและไม่ได้อยู่จริงในฐานข้อมูลสวิตช์

ระบบสามารถแสดงผังภาพการเชื่อมต่อ VLAN เพื่อใช้เป็นเครื่องมือสนับสนุนการทำงานให้แก่ผู้ดูแลเครือข่ายในการแก้ไขปัญหาที่อาจเกิดขึ้นในระดับเลเยอร์ 2 ช่วยอำนวยความสะดวกในการทำงาน สามารถเห็นภาพรวมการเชื่อมต่อได้ง่ายขึ้น

ข้อเสนอแนะ

1. ข้อมูล MIB ของสวิตช์บางยี่ห้อไม่มีเอกสารอธิบายวิธีการใช้ OID เพื่อสอบถามข้อมูล เกี่ยวข้องกับการตั้งค่า VLAN ทำให้ต้องใช้เวลาในการค้นหาและทดลองเปรียบเทียบกับที่ได้จาก คำสั่งแบบ Commanad-line

2. สวิตช์บางยี่ห้อ เช่น ZTE แม้จะเป็นรุ่นเดียวกันแต่เมื่อปรับปรุงซอฟต์แวร์ของอุปกรณ์ (Firmware) แล้ว ค่า OID ที่ใช้สอบถาม มีค่าไม่เหมือนกัน ทำให้ต้องมีเงื่อนไขในการตรวจสอบรุ่นซอฟต์แวร์ ก่อนการเก็บข้อมูล

3. สวิตช์ที่เป็นรูทบริดจ์หรือ Core switch ในเครือข่ายที่ใช้ทดสอบไม่อนุญาตให้เครื่องแม่ข่ายสอบถามข้อมูล VLAN ผ่านทางโพรโทคอล SNMP เพราะอาจไปรบกวนการทำงานของอุปกรณ์ ทำให้ต้องแก้ปัญหาดังกล่าวด้วยการอ่านจากไฟล์การตั้งค่า ซึ่งอาจทำให้ได้ข้อมูลไม่สมบูรณ์

แนวทางการพัฒนาต่อ

1. พัฒนาระบบให้มีบริการทางเว็บ (Web service) สำหรับให้บริการส่วนงานอื่น ในองค์กรสามารถสอบถามข้อมูลต่าง ๆ เช่น เส้นทางการเชื่อมต่อของ VLAN, ข้อมูลสมาชิก VLAN, ข้อมูลการเรียนรู้ที่อยู่ MAC

2. ก่อนที่จะดำเนินการลบ VLAN (ที่ไม่มีการเรียนรู้ MAC เลยภายในระยะเวลาที่กำหนด) ออกจากสวิตช์ ต้องมีการตรวจสอบให้แน่ใจก่อนว่าเป็น VLAN ที่ยกเลิกใช้งานแล้วจริง ผู้ดูแลเครือข่ายต้องนำหมายเลขวงจรถูกค้า (ชื่อของ VLAN) มาตรวจสอบกับฐานข้อมูลใบแจ้งหนี้ลูกค้า ว่ายกเลิกใช้งานจริง เนื่องจากผู้ดูแลระบบต้องตรวจสอบด้วยตนเองที่หมายเลขทำให้เสียเวลามาก ผู้จัดทำงานนิพนธ์จึงเห็นว่าหากสามารถให้บริการข้อมูลใบแจ้งหนี้ลูกค้าในลักษณะ Web service ได้ ระบบจะสามารถแลกเปลี่ยนข้อมูลในลักษณะนี้ได้เป็นอย่างดี นอกจากนี้ Web service ยังอาจสามารถช่วยตรวจสอบข้อมูลการรั่วไหลของรายได้อีกช่องทางหนึ่ง (ในกรณีที่มีการใช้ VLAN แต่ไม่พบใบแจ้งหนี้)

บรรณานุกรม

- Garimella, P., Yu-Wei, S., Zhang, N., & Rao, S. (2007). Characterizing VLAN usage in an operational network. Retrieved from <http://docs.lib.purdue.edu/ecetr/362/>
- Gobjuka, H. (2010). *Topology discovery for virtual local area networks*. Retrieved from <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5462267>
- Hameed, A., & Mian, N. A. (2012). *Finding efficient VLAN topology for better broadcast containment*. Retrieved from http://www.researchgate.net/publication/269269012_Finding_efficient_VLAN_topology_for_better_broadcast_containment
- Krothapalli, D. S., Sun, X., Yu-Wei, E. S., Yeo, A. S., & Rao, G. S. (2009). *A toolkit for automating and visualizing VLAN configuration*. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.162.2071>
- Krothapalli, D. S., Sun, X., Yu-Wei, E. S., & Rao, G. S. (2010). *Systematic approach for evolving VLAN designs*. Retrieved from <http://dl.acm.org/citation.cfm?id=1833723>
- Li, D., Chen, M., Han, C., & Liu, Y. (2012). Heterogeneous network topology discovery algorithm base on VLAN. *CISME*, 2(7), 1-7.
- Qin, K., & Li, C. (2010). *Network topologic discovery base on SNMP*. Retrieved from <http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?reload=true&arnumber=5678177>
- Skaljo, E., Hadziahmetovic, N., & Akyel, C. (2010). *Impact of broadcast, multicast and unknow unicast at low speed DSL connections based at SHDSL*. Retrieved from <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5606112>
- Yu, M., Rexford, J., Sun, X., Rao, S. & Feamster, N. (2011). Survey of virtual LAN usage in campus network. *IEE Communication Magazine*, 49(7), 98-103.