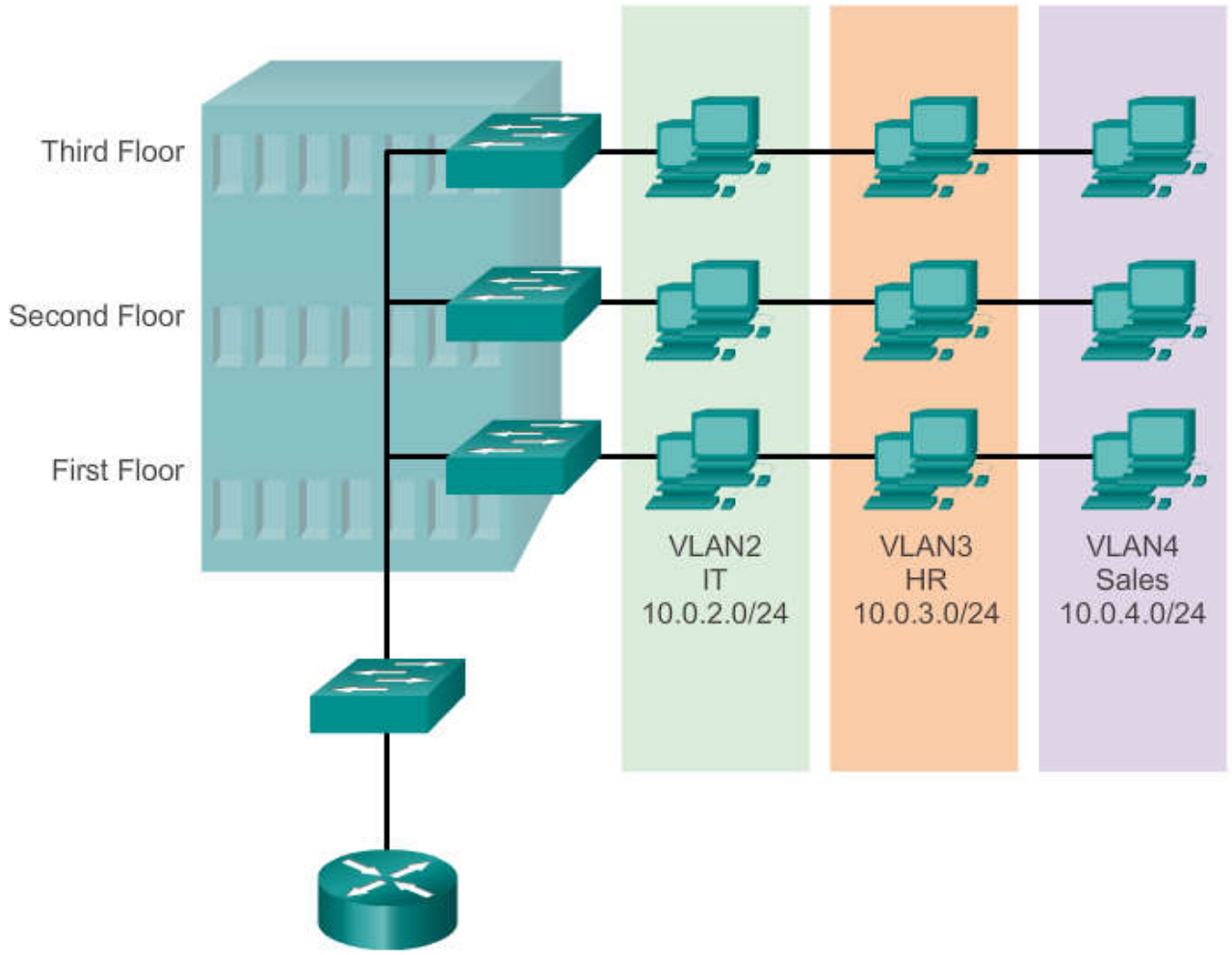
Virtual LAN (VLAN)

ความหมายของ VLAN

- VLAN คือ การแบ่งกลุ่มของสวิตซ์ภายในเลเยอร์ 2 ที่ไม่ขึ้นกับ ลักษณะทางกายภาพใดๆ
- เราไม่จำเป็นที่จะต้องนำสวิตซ์มาต่อกันเป็น ทอดๆ เพื่อจัดกลุ่มของสวิตซ์ว่าสวิตซ์กลุ่มนี้คือกลุ่มเดียวกัน
- แต่เราสามารถที่จะจัดกลุ่มให้ สวิตซ์ที่อยู่ห่างไกลกันออกไปนั้น เป็นสมาชิกของสวิตซ์อีกกลุ่มหนึ่งทางแนวตรรกกะ (Logical Design) ได้

VLAN Definitions



VLANs

- เป็นการแบ่งกลุ่มของสวิตซ์ในเชิงตรรกะ (Logical Design) ในกระบวนการทำงานของสวิตซ์เลเยอร์ 2
- แม้สวิตซ์จะสามารถลดปริมานของโดเมนปะทะ (Collision Domain) ให้เหลือเพียง 1 Collision Domain ต่อ 1 พอร์ทของสวิตซ์แล้วก็ตาม แต่ทุกพอร์ทของสวิตซ์ยังคงมีบรอดคาสท์โดเมน (Broadcast Domain) อยู่
- ซึ่งหากนำสวิตซ์มาต่อกันหลายๆ จุด และมีการใช้งานบรอดคาสท์โดเมนขึ้นมา นั่นหมายถึงว่ายังคงที่จะมีทราฟฟิก(Traffic) ที่เป็นส่วนเกินออกมาอยู่ดี ซึ่งจะทำให้ระบบเน็ตเวิร์กเกิดความล่าช้า และสิ้นเปลือง CPU ในการประมวลผลของอุปกรณ์ดีไวซ์ต่างๆ โดยไม่จำเป็น
- การทำ VLAN จะมาช่วยแก้ปัญหาตรงจุดนี้ได้ เนื่องจาก ในการทำVLAN นี้ จะเป็นการจำกัดวงของ บรอดคาสท์โดเมนให้อยู่ภายในพอร์ท หรือ ดีไวซ์ที่เรากำหนดเท่านั้น ซึ่งทราฟฟิกจะไม่ถูกส่งผ่านไปยังบรอดคาสท์โดเมนอื่นๆ

VLANs

- หากไม่มีการคอนฟิกใดๆ เพิ่มเติมและในทางการรักษาความปลอดภัยในระบบเครือข่ายนั้น ทุกๆพอร์ทของสวิตซ์ถือว่าเป็นบรอดคาส์ทโดเมนเดียวกัน
- ซึ่งทราฟฟิกที่วิ่งออกมาจากพอร์ทของสวิตซ์หนึ่งๆ ทุกๆ พอร์ทนั้น สามารถที่จะมองเห็นเฟรมข้อมูลนั้นๆ ได้ หากว่า มีใครสักคนหนึ่งทำตัวเป็น สนิฟเฟอร์โหมด (Sniffer Mode) เพื่อดักจับข้อมูลไปคงไม่ดีแน่
- แต่ถ้าทำ VLAN แล้ว เราสามารถที่จะควบคุมทราฟฟิกให้อยู่ในเฉพาะขอบเขตที่เราต้องการได้ เช่นเราต้องการให้ สวิตซ์พอร์ทที่ 1-5 ของสวิตซ์ 1 ซึ่งอยู่ชั้นที่ 1 เป็นสมาชิกเดียวกันกับ สวิตซ์พอร์ทที่ 6-8 ของสวิตซ์ 3 ที่อยู่ชั้นที่ 3 ก็เป็นได้
- โดยที่ ทราฟฟิกจะไม่ถูกส่งออกไปยังพอร์ทอื่นๆ ของสวิตซ์ตัวมันเอง และสวิตซ์ตัวอื่นๆ อีก ซึ่งเป็นมาตรการในการรักษาความปลอดภัยเบื้องต้นของระบบเน็ตเวิร์กได้

VLANs

- การคอนฟิก VLAN นั้น สามารถกระทำได้ภายใน ตัว IOS ของสวิตซ์ได้โดยตรง และการคอนฟิก VLAN ไม่จำเป็นที่จะต้องมีการย้ายสายเคเบิลใดๆ เพื่อจัดกลุ่มของสวิตซ์
- ไม่ต้องการตั้งค่าใดๆ ที่ตัว Client เลย นอกจากหมายเลข IP Address ของ Client ที่จะต้องจัดสรรใหม่ให้แก่ Client ในกรณีที่ต้องการให้ Client ไปอยู่ในต่างซับเน็ตเท่านั้น
- หากต้องการให้ VLAN นั้น สามารถที่จะติดต่อสื่อสารระหว่างกัน หรือที่เรียกว่า Inter VLANs นั้น เราจำเป็นที่จะต้องมีอุปกรณ์ในเลเยอร์ 3 เช่น เราเตอร์ หรือ สวิตซ์เลเยอร์ 3 มาช่วยในการ เราท์ทราฟฟิกระหว่าง VLANs กัน

ทำไมต้องใช้ VLAN

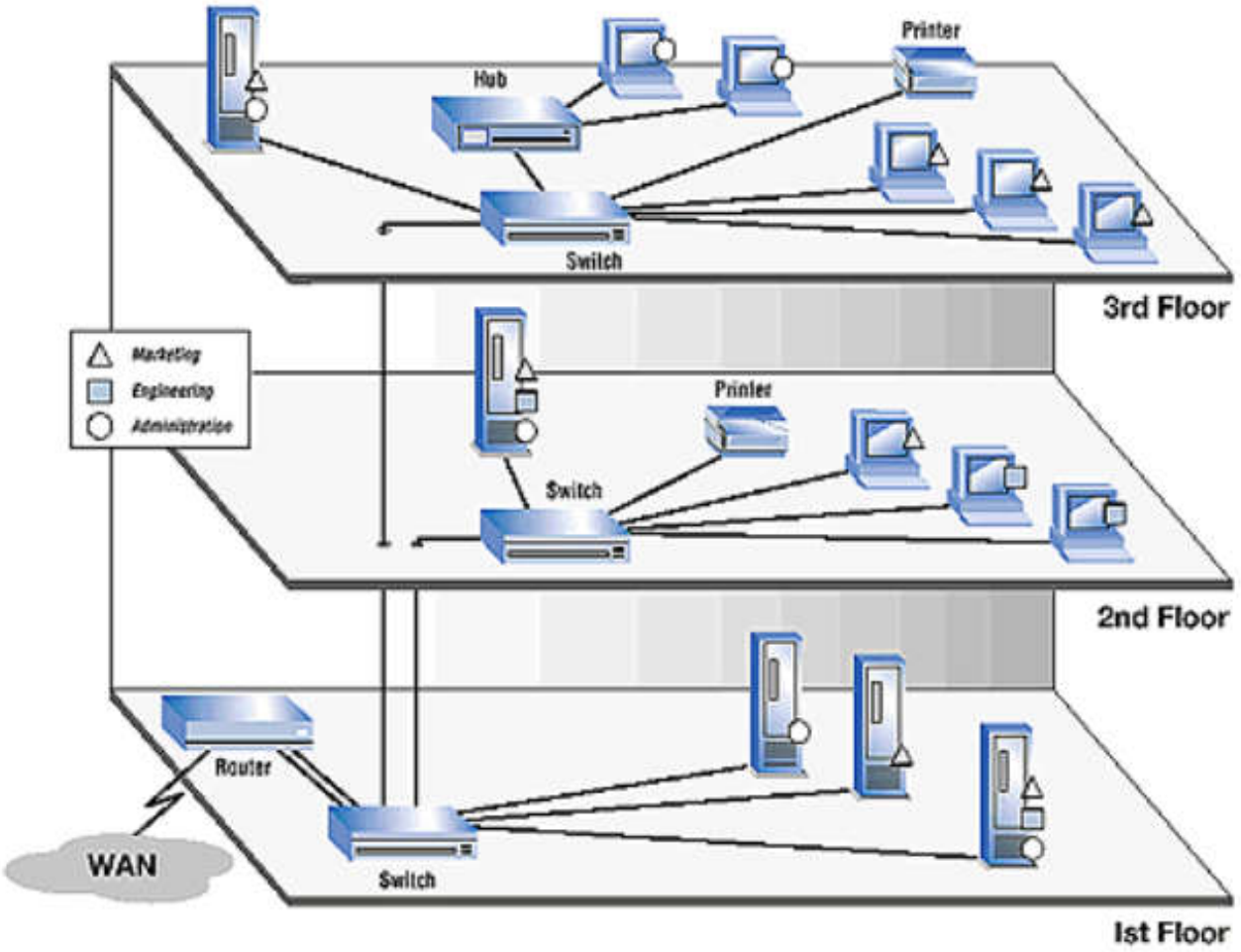
- **เพิ่มประสิทธิภาพของเครือข่าย** ในเครือข่ายปกติจะมีการส่ง Broadcast จำนวนมาก ทำให้เกิด Congestion และ VLAN สามารถช่วยเพิ่มประสิทธิภาพของเครือข่ายได้ โดยจำกัดให้ส่งข้อมูล Broadcast ไปยังผู้ที่อยู่ใน VLAN เดียวกันเท่านั้น
- **ง่ายต่อการบริหารการใช้งาน** VLAN อำนวยความสะดวกในการบริหารจัดการโครงสร้างของระบบเครือข่ายให้ง่าย มีความยืดหยุ่น และเสียค่าใช้จ่ายน้อย โดยเพียงเปลี่ยนโครงสร้างทาง Logical เท่านั้น ไม่จำเป็นต้องเปลี่ยนโครงสร้างทางกายภาพ
- **เพิ่มการรักษาความปลอดภัยมากขึ้น** เนื่องจากการติดต่อระหว่างอุปกรณ์เครือข่ายจะสามารถทำได้ภายใน VLAN เดียวกันเท่านั้น ถ้าต้องการที่จะติดต่อข้าม VLAN ต้องติดต่อผ่านอุปกรณ์ค้นหาเส้นทางหรือสวิตช์เลเยอร์ 3

แบบ Portbase และ Tagbase

- VLAN คือการจัดพอร์ตที่มีอยู่ในเน็ตเวิร์ค มาแบ่งกลุ่มกัน เพื่อจำกัดขอบเขตของการรับและส่งข้อมูล ข้อมูลสามารถจะไหลจากพอร์ตหนึ่งไปยังอีกพอร์ตหนึ่งได้ ถ้าพอร์ตปลายทางนั้นอยู่ในสมาชิก VLAN เดียวกับพอร์ตต้นทาง ไม่ว่าเฟรมข้อมูลนั้นจะเป็น Broadcast, Multicast หรือ Unicast ก็เป็นไปตามข้อกำหนดนี้
- พอร์ตใดพอร์ตหนึ่ง สามารถเป็นสมาชิกของ VLAN ใดก็ได้ แล้วแต่กำหนดและยังสามารถเป็นสมาชิกของหลาย ๆ VLAN ได้ด้วย เช่นเราต้องการแบ่งเน็ตเวิร์คออกเป็น 3 กลุ่ม กลุ่มละ 5 เครื่อง สามารถจะจัด VLAN ได้ว่า
  - VLAN 1 ประกอบด้วยสมาชิกได้แก่ พอร์ต 1 ถึงพอร์ต 5 และพอร์ต 16
  - VLAN 2 ได้แก่พอร์ต 6 ถึงพอร์ต 10 และพอร์ต 16
  - VLAN กลุ่มสุดท้ายก็จะมีพอร์ต 11 ถึงพอร์ต 15 และพอร์ต 16

  จะเห็นว่าพอร์ต 16 เป็นสมาชิกของทั้ง 3 VLAN หมายความว่าพอร์ต 16 จะถูกนำไปเสียบกับเซิร์ฟเวอร์นั่นเอง

The VLAN Solution



แบบ Portbase และ Tagbase

- ถ้า VLAN กลุ่มไหนมีเครื่อง 5 เครื่องวิธีคงสภาพของ VLAN ไว้ แต่ถ้าจำนวนเครื่องมากขึ้น เราจะใช้วิธีการขยายพอร์ตโดยการ Uplink เช่น ถ้ากลุ่ม 2 มีเครื่องมากขึ้น เราก็จะใช้พอร์ต 6 มา Uplink ไปหาสวิตช์ธรรมดาก็ได้ ลักษณะการเชื่อมต่อ VLAN แบบนี้เข้าใจง่าย จัดง่าย ไม่ยุ่งยาก และดูแลง่าย ซึ่งเราเรียกว่าเป็น VLAN แบบ Port base คือใช้พอร์ตเป็นตัวกำหนดว่าจะเป็นสมาชิกของ VLAN ใด

แบบ Portbase และ Tagbase

- VLAN แบบ Port base ก็มีข้อจำกัด เช่น เมื่อเราจะต้องจัดเน็ตเวิร์คขนาดใหญ่ เช่น เราต้องการจะให้เครื่องจำนวน 50 เครื่องอยู่ใน VLAN เดียวกัน และแยกออกจากเครื่องอีก 50 เครื่อง ให้เป็นอีก VLAN หนึ่ง เราต้องเอาสวิตช์หลายตัว มาพ่วงหรือ Uplink กันเป็นให้เกิดเป็น VLAN ขนาดใหญ่หลาย ๆ วง ซึ่ง VLAN แบบ Port base นั้นไม่สามารถรองรับได้แน่ จะต้องไปใช้ VLAN แบบ Tag base แทน
- Tag แปลว่าป้าย หมายความว่าแพ็กเก็ตข้อมูลใดก็ตามที่จะถูกส่งจากพอร์ตหนึ่งไปยังอีกพอร์ตหนึ่ง จะต้องมีการ"แปะป้าย" เพื่อแจ้งว่าแพ็กเก็ตนั้นเป็นของ VLAN ใด (ถูกส่งออกจากพอร์ตต้นทางที่อยู่ในสังกัด VLAN ใด)
- พอร์ตใดก็ตามที่จะรับแพ็กเก็ตนั้นไว้หรือจะยอมให้แพ็กเก็ตนั้นวิ่งทะลุผ่านตัวเองหรือไม่ (เช่น พอร์ต Uplink) มันจะต้องตรวจดูด้วยว่า แพ็กเก็ตนั้นมีป้าย ระบุว่าเป็น VLAN เดียวกับตัวเองหรือไม่ ถ้าไม่ใช่ ก็ไม่ให้แพ็กเก็ตผ่านหรือไม่ให้วิ่งเข้ามาในพอร์ตได้

Tag Base VLAN

- ด้วยวิธีการ Tag หรือแปะป้ายลงไปในแพ็กเก็ตนี้ จะทำให้แพ็กเก็ตสามารถจะวิ่งจากสวิตช์ตัวหนึ่ง ทะลุผ่านพอร์ต Uplink ไปยังสวิตช์อีกตัวหนึ่งได้ จะทะลุต่อไปได้เรื่อย ๆ โดยไม่หลง VLAN โดยตลอดเส้นทางการวิ่งผ่านนั้น พอร์ตทุก ๆ พอร์ตจะต้องสังกัดสมาชิกเดียวกับ VLAN ของแพ็กเก็ตนั้น
- VLAN แบบ Tag base เป็นระบบที่จัดการไม่ง่ายนัก มีเงื่อนไขและรายละเอียดค่อนข้างมาก ถ้าเราศึกษาลึกลงไปใน VLAN แบบ Tag base เช่น Ingress port, Egress port, Forbidden port, Fix ID, GARP, GVRP ฯลฯ

รูปแบบการ Encapsulation ของ VLAN

- เนื่องจากเฟรมที่วิ่งผ่าน Trunk Port ระหว่างสวิตซ์นั้น มีโอกาสที่เฟรมนั้นๆ จะเป็นของ VLAN ใดๆ ก็ได้ ดังนั้นสวิตซ์แต่ละตัวจำเป็นที่จะต้องหาเทคนิคบางอย่างในการที่จะทำให้สวิตซ์ปลายทางสามารถจำแนกได้ว่าทราฟฟิกที่มันได้รับเข้ามานั้นเป็นของ VLAN ใด
- เทคนิคที่ว่านั้นคือ การเพิ่มฟิลด์ข้อมูลเข้าไปในเฟรมมาตรฐานของสวิตซ์เพื่อใช้ในการจำแนก (Identified) ว่าทราฟฟิกนี้เป็นของ VLAN ใด
- ซึ่งการเพิ่มฟิลด์เข้าไปในเฟรมนี้ ถือเป็นการ Encapsulation เพิ่มเติมเข้าไปในเฟรม ซึ่งเทคนิคในการ Encapsulation ของ VLAN นี้จะมีอยู่ด้วยกัน สองแบบ คือ 802.1Q และ ISI

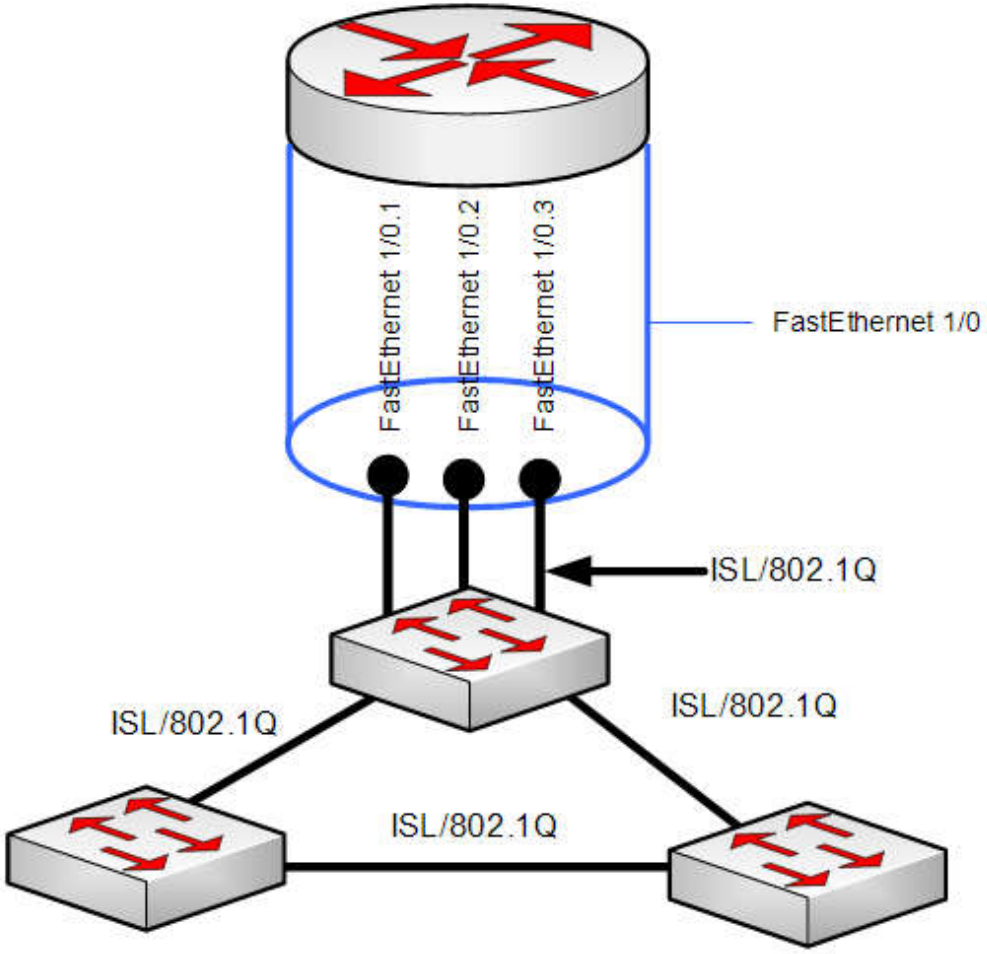
รูปแบบการ Encapsulation ของ VLAN

- **802.1Q (IEEE Standard)** เทคนิคของ IEEE 802.1Q จะใช้วิธีการเพิ่มฟิลด์พิเศษขนาด 4 Bytes เข้าไปแทรกระหว่างเฟรม และสามารถนำไปใช้ในเทคนิคของ Native VLAN ได้ (หมายถึง เฟรมที่ ตัดส่วนของ IEEE 802.1Q ออก เพื่อจำแนกให้มันเป็นทราฟฟิกพิเศษ เช่น การทำ Voice QoS)
- **ISL (Inter Switch Link: Cisco Proprietary)** ISL จะเพิ่มฟิลด์ขนาด 26 Bytes เข้าไปที่ด้านหน้าสุดของเฟรม และ ต่อท้ายจาก CRC (พูดอีกนัยหนึ่งคือ Encapsulation ห่อหุ้มเฟรมใหม่ทั้งหมดด้วย ISL Field)
- การ Encapsulation ทั้งสองแบบนี้จะกระทำที่ Egress Port (พอร์ท ขาออก) และสวิตซ์ที่จะพิจารณาเฟรมนี้ จะพิจารณาหลังจากที่รับเฟรมเข้ามาทางพอร์ทขาเข้า หรือ Ingress Port

มาตรฐานของ VLAN คือ 802.1Q

- เป็นมาตรฐานในการนำข้อมูลของ VLAN membership ใส่เข้าไปใน Ethernet Frame หรือที่เรียกว่า การ Tagging
- ถูกพัฒนาเพื่อแก้ปัญหาเรื่องการบริหารจัดการด้านเครือข่ายที่เพิ่มขึ้น เช่น การกระจายเครือข่ายใหญ่ๆ ให้เป็นส่วนย่อยๆ (Segment) ทำให้ไม่สูญเสียแบนวิธให้กับการ broadcast และ multicast มากเกินไป
- เป็นการรักษาความปลอดภัยระหว่างส่วนย่อยต่างๆ ภายในเครือข่ายให้สูงขึ้นอีกด้วย
- การต่อเติมเฟรม (tagging Frame) ด้วยมาตรฐาน 802.1Q นั้นจะทำในระดับ Data-Link layer
- การทำ VLAN Tagging นั้นจะเป็นการเปลี่ยนรูปแบบของ Ethernet Frame มาตรฐาน 802.3 ให้เป็นรูปแบบใหม่ที่เป็นมาตรฐาน 802.3 ac

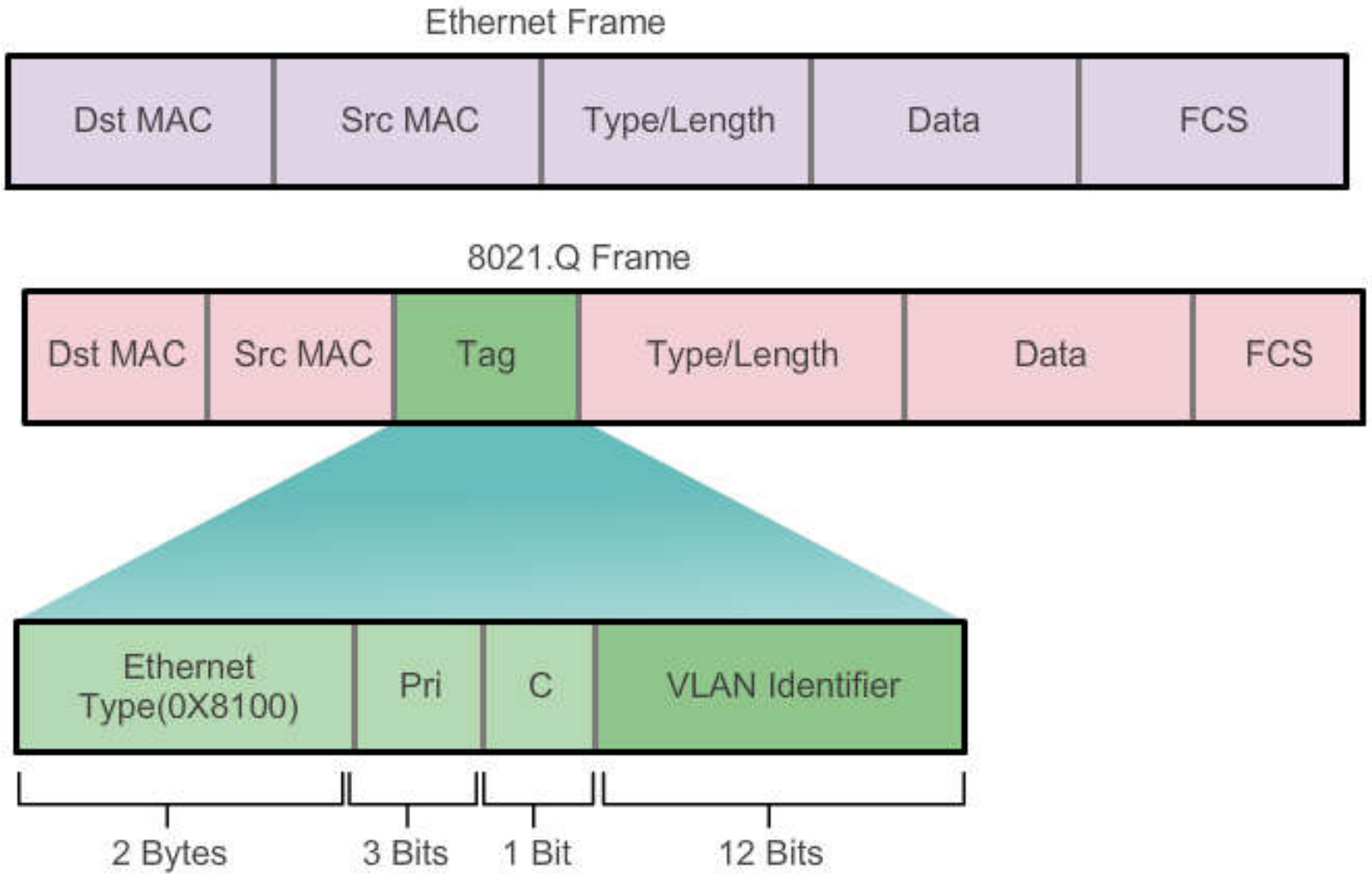
การ Encapsulation ของ VLAN



Tagging Ethernet Frames for VLAN Identification

- เฟรม tagging ใช้ในการส่งเฟรมข้าม VLAN ผ่านทาง Trunk Port
- Switches จะใช้ tag frames เพื่อใช้ระบุ VLAN ว่ามาจาก VLAN ใด มีโปรโตคอลที่ใช้ใน tagging ที่ต่างกัน IEEE 802.1q เป็นโปรโตคอลที่ได้รับความนิยมมาก
- โปรโตคอลใช้กำหนดโครงสร้างของ tagging header ที่เพิ่มไปยังเฟรม
- สวิทช์จะเพิ่ม VLAN tags ไปที่เฟรมก่อน frames ส่งไปที่ trunk links และเอา tags ออกก่อนจะส่งต่อไปยังพอร์ตที่ไม่ใช่ trunk ports
- อีกหนึ่งคุณสมบัติของ tagged คือเฟรมสามารถส่งผ่านสวิตช์ใดๆ ผ่านทาง trunk links และยังคงส่งต่อไปเรื่อยๆ จนถึง VLAN ปลายทางที่ถูกต้อง

Tagging Ethernet Frames for VLAN Identification



Native VLAN

- Native VLAN เป็น VLAN ที่ใช้สำหรับบริหารจัดการหรือติดต่อสื่อสารกันระหว่างอุปกณ์ (ในที่นี้หมายถึง Switch)
- การทำ trunk port นั้น จะมีการ encapsulate ของหมายเลข vlan นั้นๆ และติด tag header ไปกับ frame ด้วยและอุปกรณ์ปลายทาง (Switch) จะทราบว่าเป็นแพ็กเก็จจาก VLAN ใด แต่ Native VLAN จะไม่มีการ encapsulate อุปกรณ์ปลายทางหากไม่พบ tag header ก็จะเข้าใจว่าเป็น Native VLAN
- ปกติหากไม่มีการกำหนดหมายเลข Native VLAN อุปกรณ์จะกำหนดให้ VLAN 1 เป็น Native VLAN โดยอัตโนมัติ แต่เพื่อความปลอดภัยควรเปลี่ยนเป็นหมายเลข VLAN อื่น

Native VLANs and 802.1q Tagging

- เฟรมที่เป็น native VLAN จะไม่ถูกเพิ่มแท็ก
- เฟรมที่ได้รับมาไม่มีแท็กและกลายเป็น native VLAN เมื่อส่งต่อ
- หากมีพอร์ตไม่ใช่ native VLAN และไม่ได้เชื่อมต่อกับ Trunk เฟรมที่มีแท็กจะถูกดรอปทิ้ง
- ในสวิทช์ของซิสโก้ native VLAN จะเป็น VLAN 1 โดยค่าเริ่มต้น

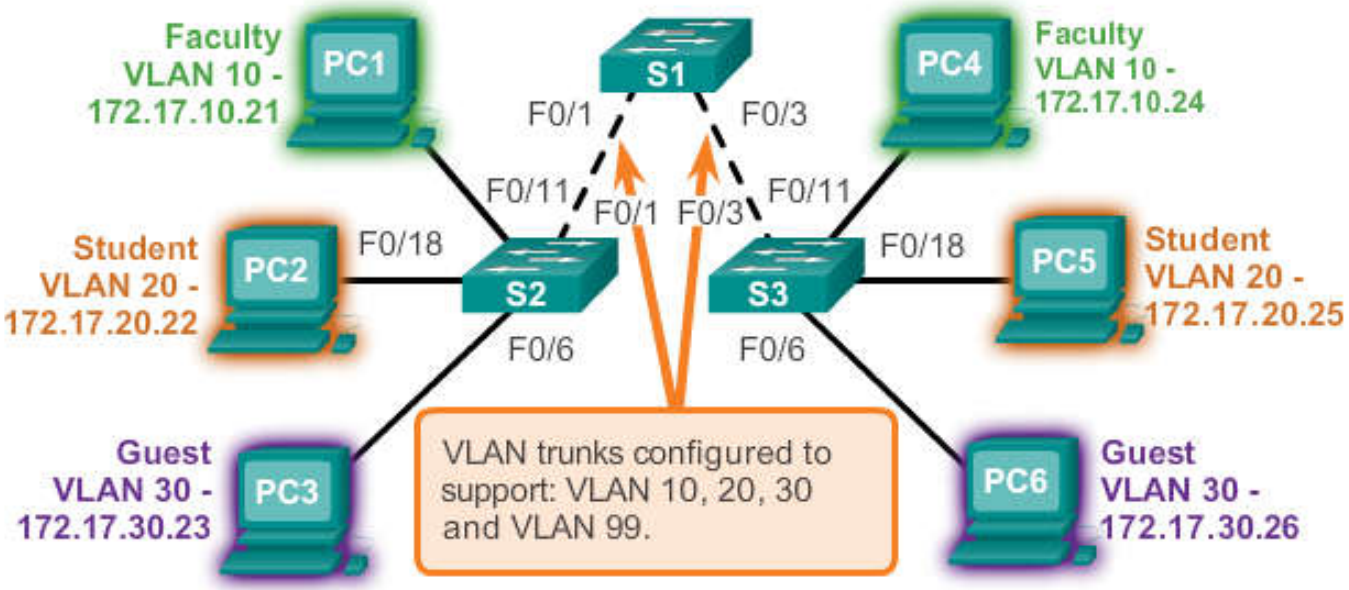
Trunking

- การเชื่อมต่อระหว่างสวิตช์โดยใช้สายเพียงแค่ 1 เส้นหรือที่เราเรียกกันว่า Uplink นั้น เป็นเรื่องที่มีกันมานานแล้ว แล้วก็ใช้งานกันมาจนถึงปัจจุบัน
- ซึ่ง IEEE ก็ได้สร้างมาตรฐานขึ้นมาใหม่ที่เราเรียกว่า IEEE 802.3ad หรือเรียกเป็นภาษาเทคนิคว่า Aggregate Link หรือเรียกเป็นภาษาทางการตลาดว่า Trunking
- Trunking ไม่ใช่การเพิ่มความเร็ว แต่เป็นการลดเวลา เพราะกลุ่มของพอร์ตของสวิตช์ตัวหนึ่งจำเป็นจะต้องสื่อสารกับกลุ่มของพอร์ตของสวิตช์อีกตัวหนึ่ง การสื่อสารก็คือการส่งข้อมูลแลกเปลี่ยนข้ามฝั่งกันไปมา เหมือนกับฝั่งธนฯกับฝั่งพระนคร แต่มีสะพานแค่อันเดียวมาเชื่อม ซึ่งรถก็จะติดเป็นขบวนเพราะต้อง“ เข้าคิว “
- ดังนั้นการวัดความเร็วของข้อมูลแต่ละชิ้นที่วิ่งข้ามแต่ละสะพานก็ทำไม่ได้แล้ว แต่เราจะวัดจากจำนวนของข้อมูลทั้งหมดที่สามารถวิ่งข้ามสะพานทั้งหมดได้ใน 1 วินาที ซึ่งในทางเทคนิคจะไม่เรียกว่าเป็นการวัด Speed แต่เป็นการวัดThroughput หรือความสามารถในการทะลุผ่าน

VLAN Trunks

VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24
VLAN 99 Management and Native - 172.17.99.0/24

F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.
F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.



ทฤษฎีของ Access Port และ Trunk Port

- ในการสร้าง VLAN นั้น พอร์ทของสวิตซ์นั้น จะทำหน้าที่อยู่ สองประเภท คือ ACCESS PORT และ TRUNK PORT
- ซึ่งจะมีหน้าที่ในการทำงานต่างๆ กันไปตามที่ System Administrator จะเป็นคนกำหนดไว้

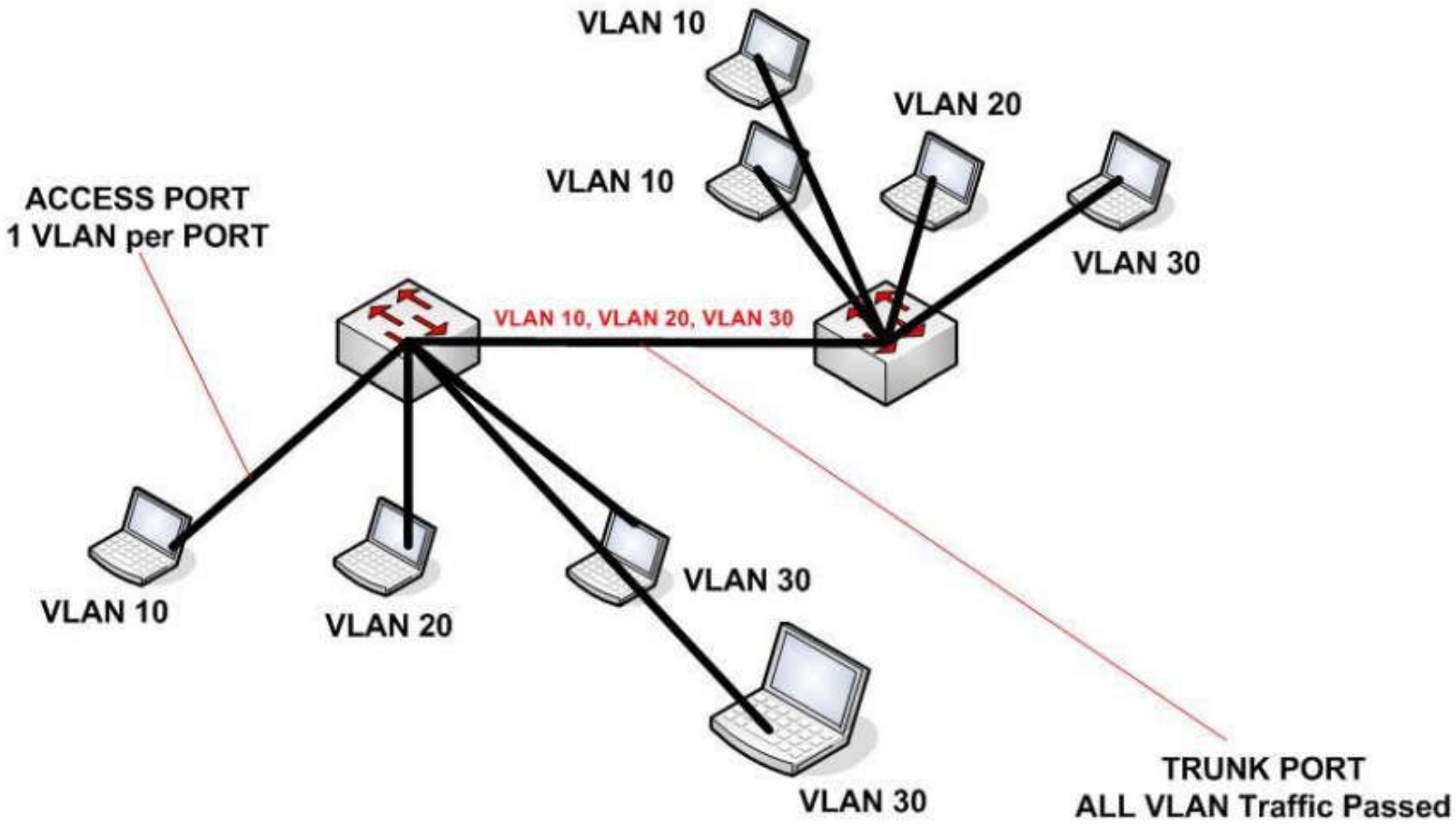
Access Port

- เป็นพอร์ทที่ทำหน้าที่เชื่อมต่อระหว่างสวิตซ์จาก Client ไปยังสวิตซ์ ซึ่งเราจะใช้สายแลนแบบสายตรง (Straight Through) ในการเชื่อมต่อ
- พอร์ทที่ถูกเซ็ตให้เป็น Access Port นี้ จะมีทราฟฟิกของ VLAN เพียง VLAN เดียว ที่วิ่งผ่านออกยังพอร์ทนี้ ซึ่งตัวอย่างในการเซตพอร์ทให้เป็น Access Port นี้คือ
  - พอร์ทที่ เซตระหว่างสวิตซ์ และ Client
  - พอร์ทที่ เซตระหว่างสวิตซ์ และ Server
  - พอร์ทที่ เซตระหว่าง สวิตซ์ และ เราเตอร์ (มีข้อแม้ว่า เราเตอร์ตัวที่เชื่อมต่อนั้นจะต้องไม่ใช่เราเตอร์ที่ทำหน้าที่ในการเราท์ทราฟฟิกของ Inter VLAN)

Trunk Port

- เป็นพอร์ททำหน้าที่ เชื่อมต่อสวิตซ์ตัวอื่นๆ ที่ต้องการให้เป็นสมาชิกของ VLAN ต่างๆกันมาอยู่ด้วยกัน
- ทำหน้าที่ส่งผ่านทราฟฟิกของ หลายๆ VLAN ให้ กระจายไปยังสวิตซ์ตัวอื่นๆ ที่มีพอร์ทที่ถูกกำหนดให้เป็น VLAN เดียวกันกับสวิตซ์ตัวต้นทางได้ หรือที่เรียกกันโดยทั่วไปว่า UPLINK PORT
- ตัวอย่างในการเซตพอร์ทให้เป็น Trunk Port นี้ คือ
  - พอร์ทที่ทำหน้าที่เชื่อมต่อไปยังสวิตซ์ตัวอื่นๆ เช่น UPLINK PORT
  - พอร์ทที่ทำหน้าที่เชื่อมไปยังเราเตอร์ตัวที่ทำหน้า เราท์ทราฟฟิกระหว่าง VLAN

Access Port และ Trunk Port



ประโยชน์ที่จะได้รับจากการทำ VLAN

- สร้างกลไกด้านความปลอดภัยได้ง่ายขึ้น เช่น การสร้าง Access Control List บนอุปกรณ์ Layer3 และลดความเสี่ยงการดักจับข้อมูล (Sniffing)
- จำกัดการแพร่กระจายของ Broadcast traffic ไม่ให้ส่งผลกระทบต่อประสิทธิภาพโดยรวม
- ผู้ใช้สามารถย้ายไปยัง VLAN (Subnet) อื่น ด้วยการเปลี่ยน config ของ switch และ IP Address ของ Client ไม่จำเป็นต้องมีการย้าย switch หรือ สายใด ๆ
- สามารถวิเคราะห์ ปัญหาที่เกิดขึ้นในระบบได้ง่ายขึ้น เช่น
  - ในระบบมีการแบ่ง VLAN ไว้ 3 แผนก ได้แก่ sale , engineer และ server วันหนึ่ง ผู้ใช้ของ sale โทรมาแจ้งปัญหากับ admin ว่าเล่น Internet ไม่ได้
  - Admin ควรจะถาม user กลับไปว่าคนอื่นในแผนกเป็นด้วยหรือไม่ ถ้าไม่ก็แสดงว่าเป็นที่เครื่องของ user คนนั้นคนเดียว
  - แต่ถ้าหากเป็นทั้งแผนก ก็ต้องโทรเช็คกับแผนก engineer ด้วยว่าเป็นเหมือนกันหรือไม่ ถ้าไม่เป็น แสดงว่าเป็นที่แผนก sale แผนกเดียว ดังนั้นก็ทำการตรวจเช็คปัญหาที่แผนก sale อย่างเดียว
- จะเห็นได้ว่าการวิเคราะห์ปัญหาง่ายขึ้นมากและการขอบเขตในการวิเคราะห์ปัญหาก็แคบลง ที่สำคัญตอนการแก้ปัญหาก็ควรนำหลักการ OSI Layer เข้ามาช่วยจะทำให้หาสาเหตุได้เร็วขึ้น

VLAN 1

- VLAN โดยค่าดีฟอล์ท (Default) ทุกๆ พอร์ทของสวิตซ์นั้น จะถูกจัดให้อยู่ใน VLAN 1 หรือ ที่เรียกกันว่า “Management VLAN”
- เราจะไม่สามารถลบ VLAN 1 นี้ได้ และ หมายเลข VLAN นี้ สามารถสร้างได้ตั้งแต่หมายเลข 1 – 1005

VLAN 1

VLAN 1

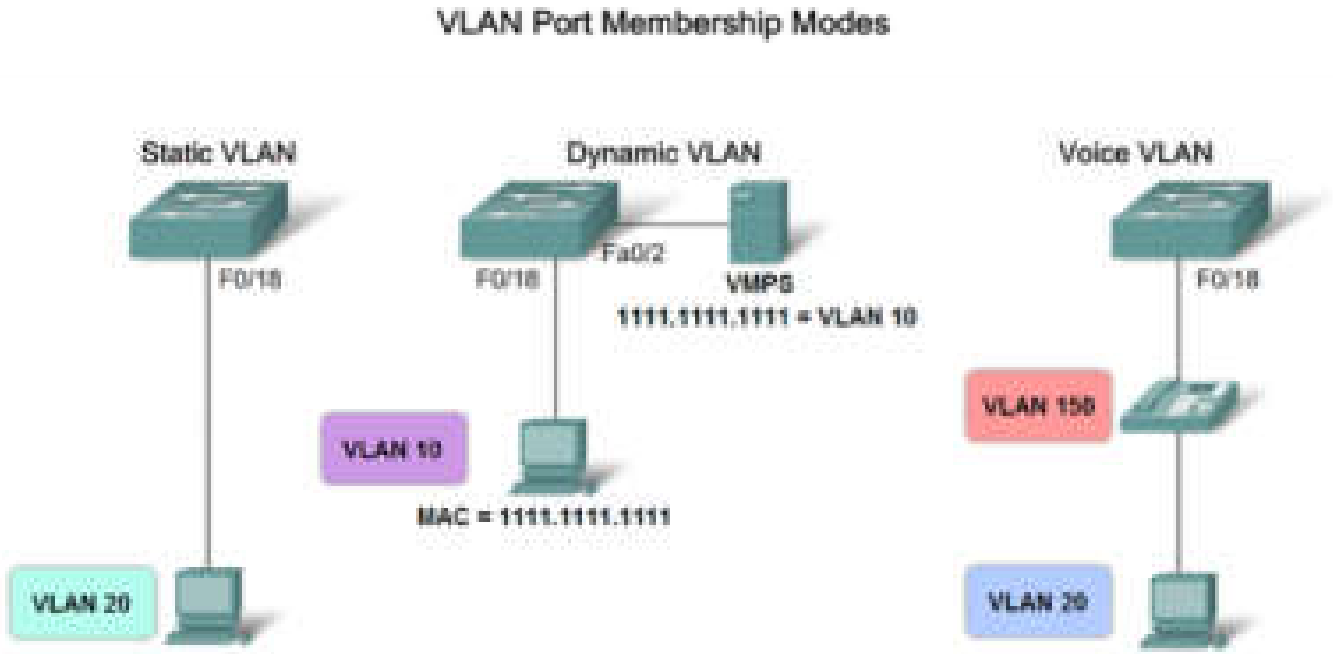
```
Switch# show vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------
1    default             active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                   Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                   Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                   Gi0/1,  Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

- All ports assigned to VLAN 1 to forward data by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.
- VLAN 1 cannot be renamed or deleted.

ชนิดของ VLAN มี 2 ชนิด

1. Static VLAN เลือกตามเลขพอร์ต

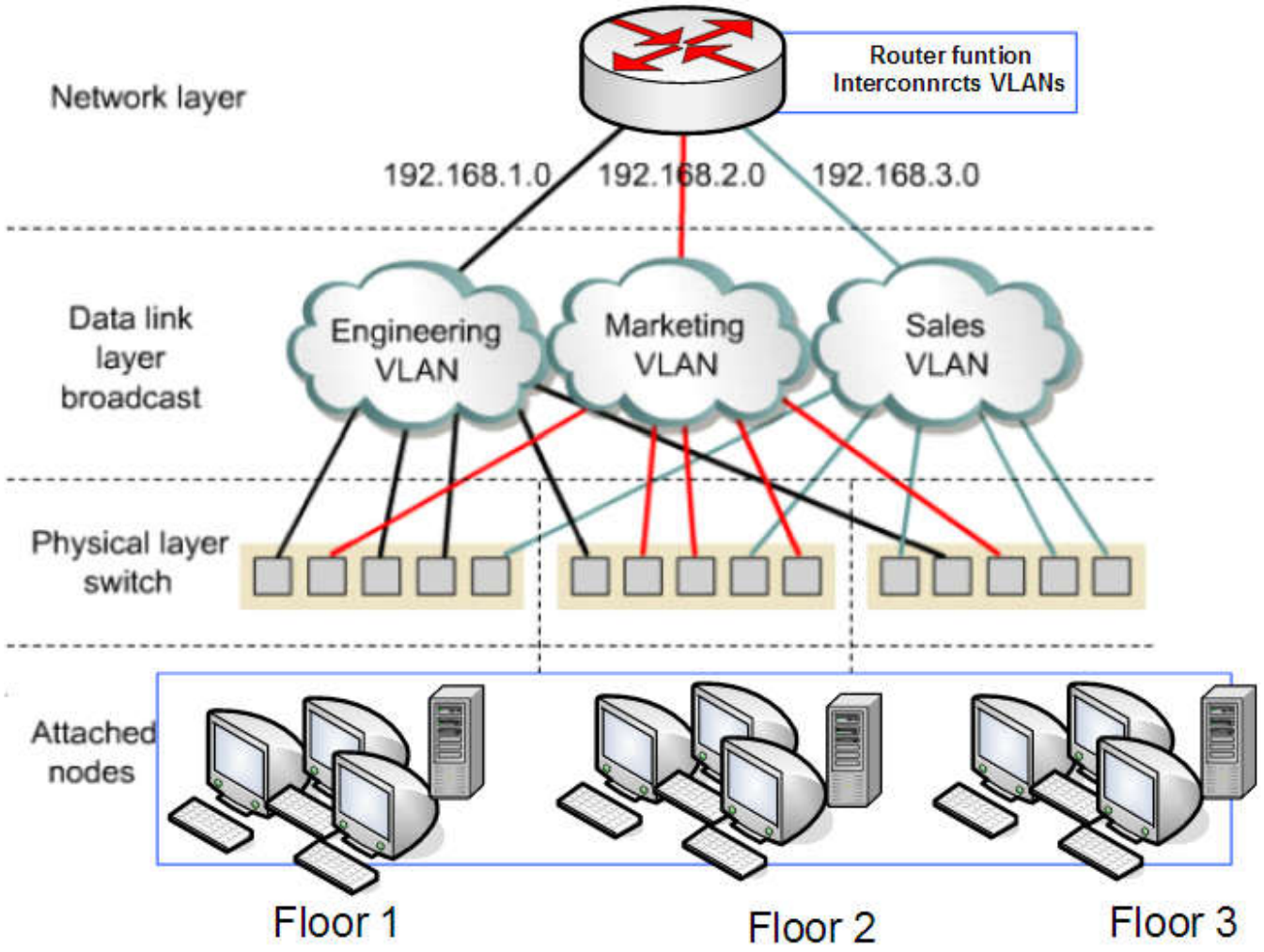
2. Dynamic VLAN คือการเลือกสมาชิกVLAN โดยพิจารณาจาก MAC address ที่ต้องการ



Static VLAN

- Static VLAN หรือ อีกชื่อหนึ่งคือ Port-Based Membership จะเป็นการพิจารณาความเป็นสมาชิกของ VLAN หนึ่งๆ โดยดูจากพอร์ท
- ซึ่งพอร์ทของสวิตซ์ที่เชื่อมต่ออยู่กับ Client นั้น ถึงแม้ว่าจะเป็นพอร์ทของสวิตซ์เดียวกัน แต่หากพอร์ททั้งสองนั้นอยู่คนละ VLAN กัน ก็ไม่สามารถที่จะติดต่อกันได้ หากไม่มีอุปกรณ์ในเลเยอร์ 3 มาช่วยในการเราท์ทราฟฟิก
- ซึ่งการเซตพอร์ทแต่ละพอร์ทให้เป็นสมาชิกของ VLAN ใดๆ นั้น จะถูกกระทำแบบ Manual จาก System Administrator

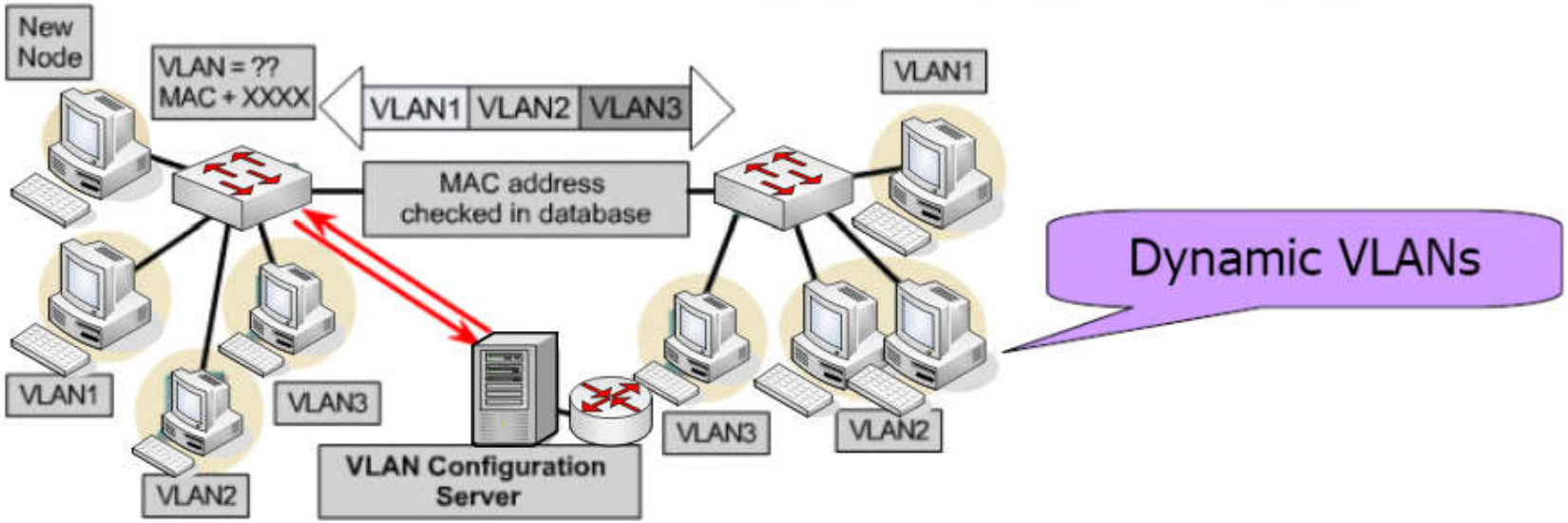
Static VLAN


Network layer
Router funtion
Interconnrcts VLANs
192.168.1.0
192.168.2.0
192.168.3.0
Data link
layer
broadcast
Engineering
VLAN
Marketing
VLAN
Sales
VLAN
Physical layer
switch
Attached
nodes
Floor 1
Floor 2
Floor 3

Dynamic VLAN

- Dynamic VLAN เป็นการกำหนด VLAN ให้กับเครื่อง Client โดยพิจารณาจากหมายเลข MAC Address ของ Client
- เมื่อ Client ทำการเชื่อมต่อไปยังสวิตซ์ตัวใดๆ สวิตซ์ที่รัน Dynamic VLAN นี้ก็จะไปหาหมายเลข VLAN ที่ MAP กับ MAC Address นี้จาก Database ส่วนกลางมาให้
- ซึ่ง System Administrator สามารถที่จะเซตหมายเลข MAC Address ในการจับคู่กับ VLAN ได้ที่ VLAN Management Policy Server (VMPS)

Dynamic VLAN



รูปแบบอื่นๆ ของ VLAN

1. Layer 1 VLAN : Membership by ports ในการแบ่ง VLAN จะใช้พอร์ตบอกว่าเป็นของ VLAN ใด เช่นสมมุติว่าในสวิตช์ที่มี 4 พอร์ต กำหนดให้ พอร์ต 1, 2 และ 4 เป็นของ VLAN เบอร์ 1 และพอร์ตที่ 3 เป็นของ VLAN เบอร์ 2

Port	VLAN
1	1
2	1
3	2
4	1

2. Layer 2 VLAN : Membership by MAC Address ใช้ MAC Address ในการแบ่ง VLAN โดยให้สวิตช์ตรวจหา MAC Address จากแต่ละ VLAN

MAC Address	VLAN
1212354145121	1
2389234873743	2
3045834758445	2
5483573475843	1

3. Layer 2 VLAN : Membership by Protocol types แบ่ง VLAN โดยใช้ชนิดของ protocol ที่ปรากฏอยู่ในส่วนของ Layer 2 Header ดูรูปที่ 3

Protocol	VLAN
IP	1
IPX	2

4. Layer 3 VLAN : Membership by IP subnet Address แบ่ง VLAN โดยใช้ Layer 3 Header นั่นก็คือใช้ IP Subnet เป็นตัวแบ่ง

IP Subnet	VLAN
23.2.24	1
26.21.35	2

5. Higher Layer VLAN's ทำได้โดยใช้โปรแกรมประยุกต์หรือ service แบ่ง VLAN เช่นการใช้โปรแกรม FTP สามารถใช้ได้ใน VLAN 1 เท่านั้น และถ้าจะใช้ Telnet สามารถเรียกใช้ได้ใน VLAN 2 เท่านั้น เป็นต้น

Protocol	VLAN
FTP	1
Telnet	2

VLAN Ranges On Catalyst Switches

- Catalyst 2960 และ 3560 Series switches รองรับมากกว่า 4,000 VLANs แบ่งเป็น 2 กลุ่ม:
- Normal Range VLANs
  - VLAN numbers from 1 through 1005
  - Configurations stored in the vlan.dat (in the flash)
  - VTP can only learn and store normal range VLANs
- Extended Range VLANs
  - VLAN numbers from 1006 through 4096
  - Configurations stored in the running-config (in the NVRAM)
  - VTP does not learn extended range VLANs

Creating a VLAN

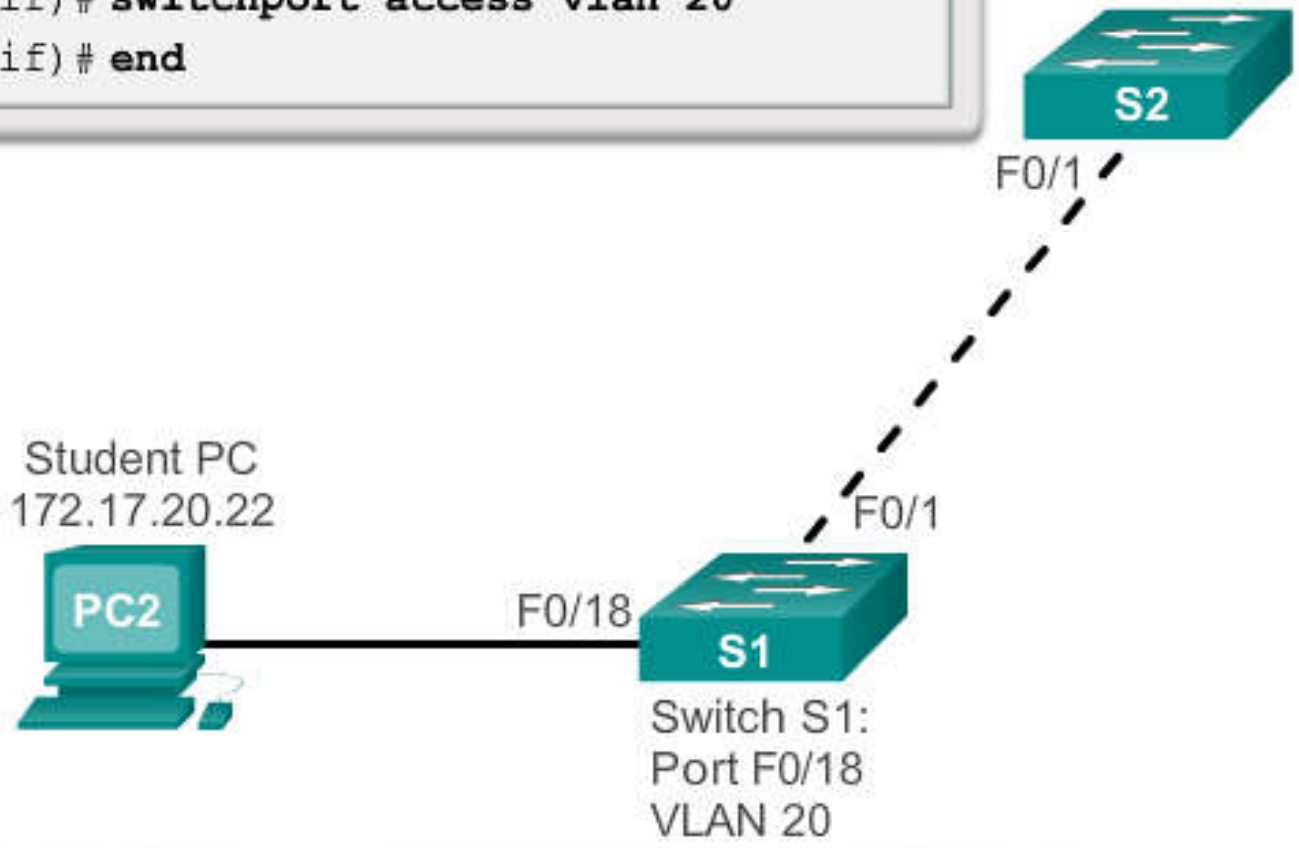
Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Create a VLAN with a valid id number.	`S1(config)# vlan vlan_id`
Specify a unique name to identify the VLAN.	`S1(config)# name vlan_name`
Return to the privileged EXEC mode.	`S1(config)# end`

Assigning Ports To VLANs

Cisco Switch IOS Commands	
Enter global configuration mode.	S1 # **configure terminal**
Enter interface configuration mode for the SVI.	S1(config) # **interface** *interface_id*
Configure the management interface IP address.	S1(config) # **ip address 172.17.99.11**
Set the port to access mode.	S1(config-if) # **switchport mode access**
Assign the port to a VLAN.	S1(config-if) # **switchport access vlan** *vlan_id*
Return to the privileged EXEC mode.	S1(config-if) # **end**

Assigning Ports To VLANs

```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```



Changing VLAN Port Membership

```
S1(config)# int fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# show vlan brief

VLAN Name                Status    Ports
---- ----------------- ------- -------------------------------
1    default              active  Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                  Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                  Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                  Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                  Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                  Gi0/1, Gi0/2
20   student              active
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Changing VLAN Port Membership

```
S1# config t
S1(config)# int fa0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# show vlan brief

VLAN Name                 Status     Ports
---- -------------------- --------- -------------------------------
1    default              active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                     Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                     Fa0/9, Fa0/10, Fa0/12, Fa0/1
                                     Fa0/14, Fa0/15, Fa0/16, Fa0/
                                     Fa0/18, Fa0/19, Fa0/20, Fa0/
                                     Fa0/22, Fa0/23, Fa0/24, Gi0/
                                     Gi0/2
20   student              active     Fa0/11
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Deleting VLANs

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief

VLAN Name                Status    Ports
---- ----------------    --------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                   Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                   Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                   Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                   Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                   Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
S1#
```

Verifying VLAN Information

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, Fa0/18

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------

S1# show vlan summary
Number of existing VLANs              : 7
Number of existing VTP VLANs          : 7
Number of existing extended VLANS     : 0

S1#
```

Virtual Trunking Protocol (VTP)

- ในการที่เราจะสร้าง VLAN หนึ่งๆ ขึ้นมาใช้งานนั้น เราจำเป็นที่จะต้องสร้าง VLAN ที่ตัวสวิตซ์หนึ่งๆ (รวมถึงตั้งชื่อให้ VLAN ในบางกรณี)
- ซึ่งหากว่า ใน Infrastructures ของเรานั้น มีสวิตซ์หลายๆ ตัวอยู่ในระบบนั้น การที่จะสร้าง VLAN ทุกๆ VLAN ขึ้นมานั้น คงเป็นเรื่องที่เสียเวลามากเลยทีเดียว
- ดังนั้น ทางซิสโก้ จึงมีเทคนิคที่จะทำให้เราสามารถออกแบบ และ สร้างหมายเลข VLAN ที่จุดๆ เดียว และมีการกระจาย (Propagation) ไปยังสวิตซ์ตัวอื่นๆ ภายในเน็ตเวิร์กของเราได้

VTP Operation

- เมื่อเริ่มแรก ต้องโปรโมทสวิตซ์ตัวหนึ่งๆ ขึ้นมาทำหน้าที่เป็น VTP Server ให้กับสวิตซ์ทุกๆตัวในเน็ตเวิร์ก โดยการสร้าง VLAN ขึ้นที่สวิตซ์ตัวนี้
- เมื่อเรานำสวิตซ์ตัวอื่นๆ มาต่อกับมันด้วย (สวิตซ์ตัวแรก จะต้องถูกเซตให้เป็น VTP Server Mode และ สวิตซ์ตัวต่อๆ มา จะต้องถูกเซตเป็น VTP Client Mode และมีการเซตโดเมนเนมภายในสวิตซ์ให้เหมือนกัน (อย่างน้อยที่สุด ในครั้งแรกที่นำสวิตซ์ตัวอื่นๆ มาต่อกับ VTP Server สวิตซ์ตัวอื่นๆ จำเป็นที่จะต้องอยู่ในสถานะ Client Mode จนกระทั่งได้เรียนรู้ VLAN Number เรียบร้อยแล้ว)
- เมื่อเราเชื่อมต่อในลักษณะนี้แล้ว ทาง VTP Server นั้น จะเป็นตัวแพร่กระจายหมายเลข VLAN ให้แก่ Client Switch เอง เราเพียงแต่ทำหน้าที่เซตพอร์ทของสวิตซ์นั้นๆ ให้ว่ามันอยู่ใน VLAN ใด หรือพอร์ทใดที่ทำหน้าที่เป็น Access Port หรือ Trunk Port เท่านั้น

VTP Terminology

- VTP Domain เป็นการรวมกลุ่มของสวิตซ์ทั้งหมดที่มีการบริหารจัดการ VLAN เหมือนกัน มาอยู่ด้วยกัน และจะมี ดาต้าเบสของ VLAN เป็นชุดเดียวกัน และ สวิตซ์จะไม่แชร์ดาต้าเบสภายในโดเมนของตน ให้แก่ โดเมนอื่นๆ
- VTP Modes
  - Server: สวิตซ์โหมดนี้จะมีอิสระอย่างเต็มที่ในการเพิ่ม-ลบ VLAN นั้นๆ ได้
  - Client: สวิตซ์โหมดนี้ จะสามารถทำได้เพียงแค่ รับหมายเลข VLAN มาจาก VTP Server เท่านั้น
  - Transparent: สวิตซ์โหมดนี้ จะไม่เกี่ยวข้องในการอัพเดตหรือ รับรู้เกี่ยวกับ สวิตซ์ตัวอื่นๆ แต่จะส่งต่อเฟรมที่วิ่งผ่านตัวมันไปยังปลายทางได้ผ่านทางพอร์ท Trunk ของมัน จุดประสงค์ของ VTP Transparent Mode นี้ มักใช้ในการ Save Configurations ของสวิตซ์
- ในการประกาศ VLAN ของ VTP Server นั้น จะใช้วิธีการส่งหมายเลข VLAN และ หมายเลข VTP Advertisement ออกไปยัง VTP Client อื่นๆ โดยการส่งผ่าน Multicast IP Address ซึ่ง VTP Server ที่มี VTP Advertisement ที่มีค่าสูงสุด Client จะรับฟังและ Update ข้อมูลตาม VTP Server นั้นๆ

Configuration VTP

- VTP Sever

Switch# config terminal

Switch(config)# vtp mode server

Switch(config)# vtp domain eng_group

Switch(config)# vtp password mypass

Switch(config)# end

- VTP Client

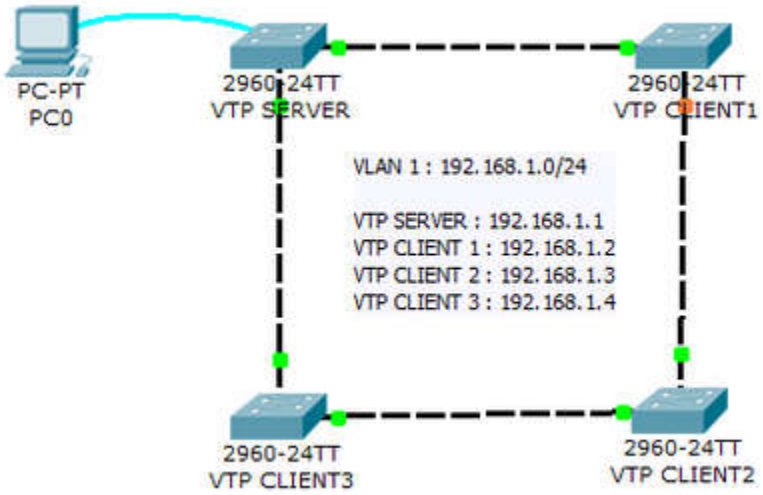
Switch# config terminal

Switch(config)# vtp mode client

Switch(config)# vtp domain eng_group

Switch(config)# vtp password mypass

Switch(config)# end

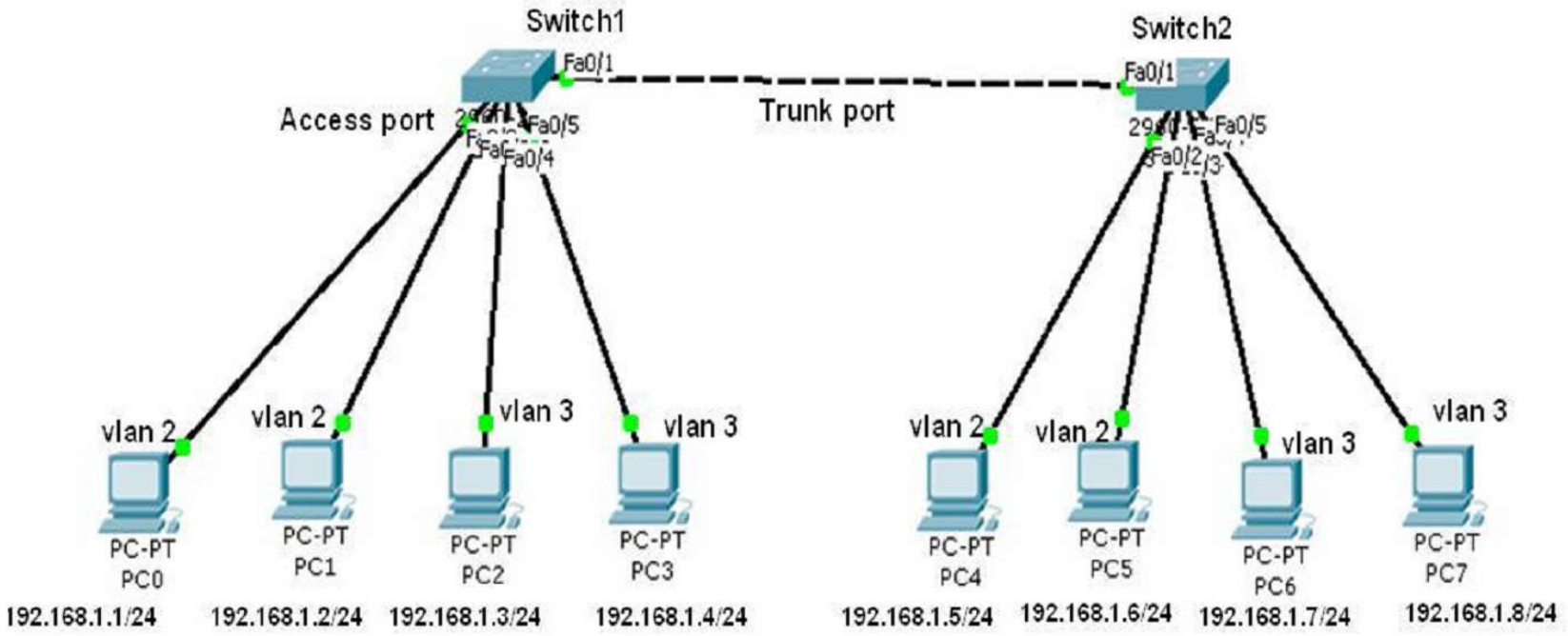


Inter-VLAN Routing

- การสื่อสารระหว่างต่าง VLANs ต้องใช้ Router หรือ Switch Layer 3
- ซึ่งเทคนิคการเอาเราเตอร์มาใช้ เรียกว่า “Routes on a stick” และเทคนิคการเอาสวิตซ์เลเยอร์ 3 มาใช้ เรียกว่า “Switch Virtual Interface (SVI)”
- รูปแบบในการเชื่อมต่อแบบ Routes on a stick นี้ เราเตอร์จะใช้เพียง Fast Ethernet อย่างน้อย 1 พอร์ทในการต่อเข้ากับสวิตซ์ และ มีการเซต Sub-Interface ที่รองรับ VLAN นั้นๆ เพื่อทำหน้าที่เราท์ทราฟฟิกระหว่าง VLAN
- ต้องเซตพอร์ตของสวิตซ์พอร์ตนั้นเป็น Trunk Port ด้วย และพอร์ตของเราเตอร์ จะต้องมีการเซต Encapsulation ในแบบที่ สวิตซ์ตัวนั้นๆ ยอมรับ

VLAN Basic LAB 1

1. สร้าง หมายเลข VLAN และ ชื่อของ VLAN ขึ้นมาก่อน
2. กำหนด port (interface) ที่ต้องการให้อยู่ VLAN นั้นๆ



การสร้าง VLAN

- **Switch 1**

Switch1 > enable

Switch1 # configure terminal

Switch1 (config)# vlan 2

Switch1 (config-vlan)# name Admin

Switch1 (config-vlan)# vlan 3

Switch1 (config-vlan)# name User

การกำหนด interface ให้กับแต่ละ VLAN

```
Switch1 > enable
Switch1 # configure terminal
Switch1 (config)# interface fa0/2
Switch1 (config-if)# switchport mode access
Switch1 (config-if)# switchport access vlan 2
Switch1 (config-if)# no shutdown

Switch1 (config)# interface fa0/3
Switch1 (config-if)# switchport mode access
Switch1 (config-if)# switchport access vlan 2
Switch1 (config-if)# no shutdown
```

```
Switch1 (config)# interface fa0/4
Switch1 (config-if)# switchport mode access
Switch1 (config-if)# switchport access vlan 3
Switch1 (config-if)# no shutdown

Switch1 (config)# interface fa0/5
Switch1 (config-if)# switchport mode access
Switch1 (config-if)# switchport access vlan 3
Switch1 (config-if)# no shutdown

Switch1 (config)# interface fa0/1
Switch1 (config-if)# switchport mode trunk
```

การกำหนด interface ให้กับแต่ละ VLAN

- การ config VLAN ที่ switch 2 รูปแบบ config เหมือนกัน
- สามารถ manage port หลาย port พร้อมกันได้ด้วย range เช่น

  Switch2 (config)# interface range fa0/2-3

  Switch2 (config-if-range)# switchport mode access

  Switch2 (config-if-range)# switchport access vlan 2

  Switch2 (config-if-range)# no shutdown
- ถ้า port ที่ set ไม่เรียงต่อกันใช้ **(,)** ช่วยได้ เช่น

  Switch1 (config)# interface range fa0/2 , fa0/5 , fa0/10 , fa0/20

การดูสถานะของ VLAN

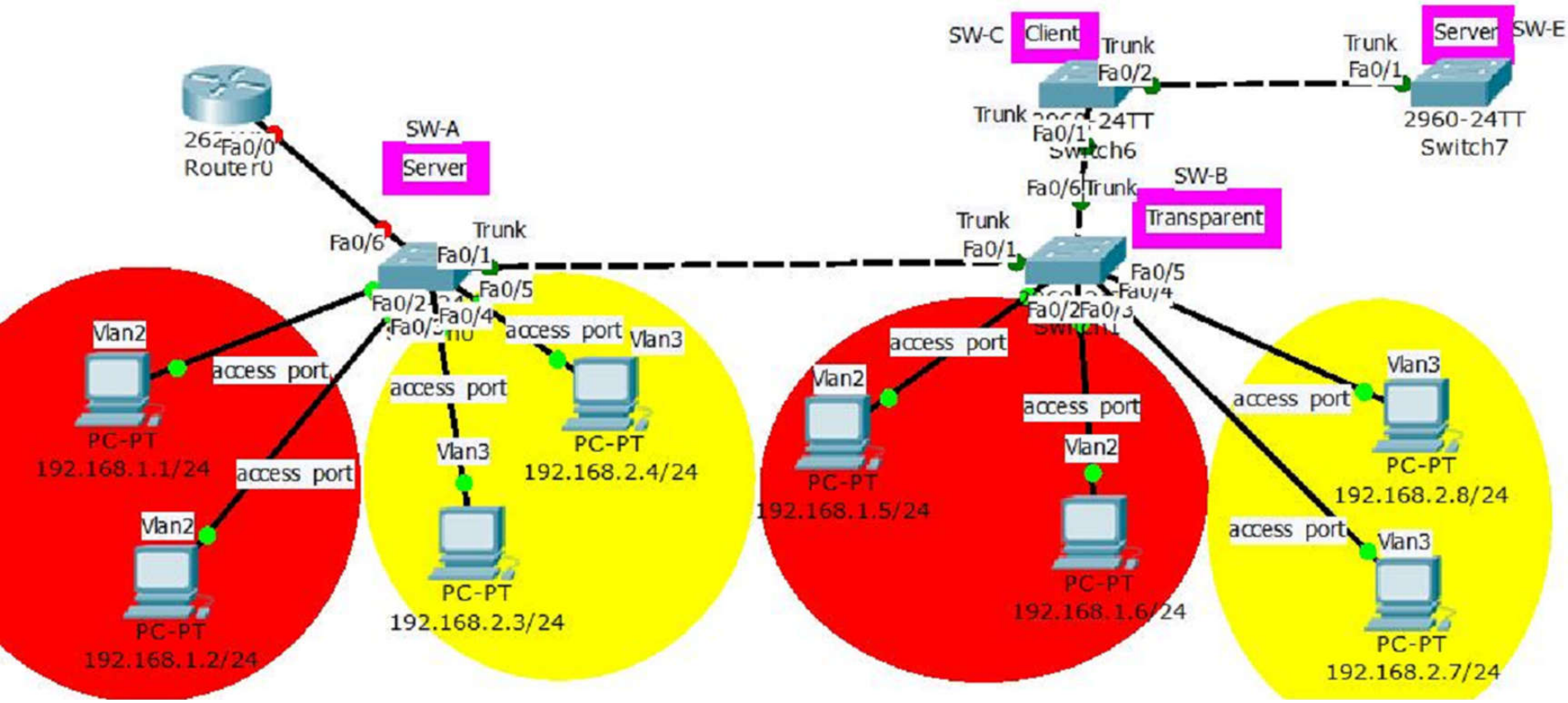
- สามารถดูสถานะของ interface และ VLAN ที่ privilege mode ได้ด้วยคำสั่ง
  - show vlan หรือ
  - show vlan brief
- จากนั้นลอง ping ดู จะ ping เจอเฉพาะ VLAN ตัวเองเท่านั้น

Lab 2 InterVLAN Routing

- InterVLAN Routing คือการติดต่อสื่อสารกันระหว่าง VLAN ทำให้ต่าง VLAN ติดต่อหรือแลกเปลี่ยนข้อมูลกันได้โดยมีอุปกรณ์ Layer 3 เป็นตัวเชื่อมหรือเป็น Gateway ให้นั่นเอง

- จงทำให้ VLAN 2 และ VLAN 3 ติดต่อกันได้ ด้วยการ Config Inter VLAN ที่ Router CISCO

Lab InterVlan Routing



กำหนด IP ของ PC ตามรูปด้านบน

VLAN 2 เป็น Network 192.168.1.0/24 Gateway คือ 192.168.1.254

VLAN 3 เป็น Network 192.168.2.0/24 Gateway คือ 192.168.2.254

รูปแบบ Config Inter VLAN บน Router CISCO

Router(config)#interface f0/0
Router(config-if)#no shutdown
Router(config)#interface f0/0.1
Router(config-subif)#encapsulation dot1Q VLAN ID
Router(config-subif)#ip address IP address subnet mask

เฉลย LAB Inter VLAN Routing

- Switch-A ที่ Fa0/6 ต้อง Set เป็ น Port trunk

```
SW-A(config)#interface fastEthernet 0/6
SW-A(config-if)#switchport mode trunk
```

- ที่ Router config

```
Router1(config)#interface fastEthernet 0/0
Router1(config-if)#no ip address
Router1(config-if)#no shutdown
```

- แบ่ง Sub Interface และ Show ip route ผลที่ได้ตามด้านล่าง

Router1(config)#interface fastEthernet 0/0.2

Router1(config-subif)#**encapsulation dot1q 2**

Router1(config-subif)#**ip address 192.168.1.254 255.255.255.0**

Router1(config)#interface fastEthernet 0/0.3

Router1(config-subif)#**encapsulation dot1q 3**

Router1(config-subif)#**ip address 192.168.2.254 255.255.255.0**

- ใช้คำสั่งเพื่อแสดง routing table

Router1# Show ip route

Summary

- Allows an administrator to logically group devices that act as their own network
- Are used to segment broadcast domains
- Some benefits of VLANs include Cost reduction, security, higher performance, better management
- Types of Traffic on a VLAN include
  - Data
  - Voice
  - Network protocol
  - Network management

- Trunks A common conduit used by multiple VLANS for intra-VLAN communication
- IEEE 802.1Q
  - The standard trunking protocol
  - Uses frame tagging to identify the VLAN to which a frame belongs
  - Does not tag native VLAN traffic