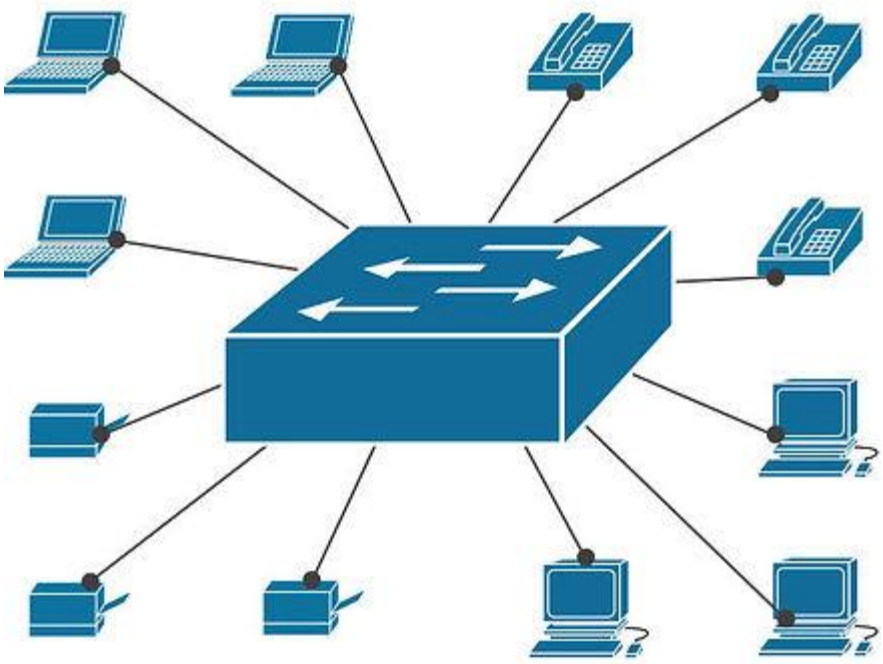
VLAN

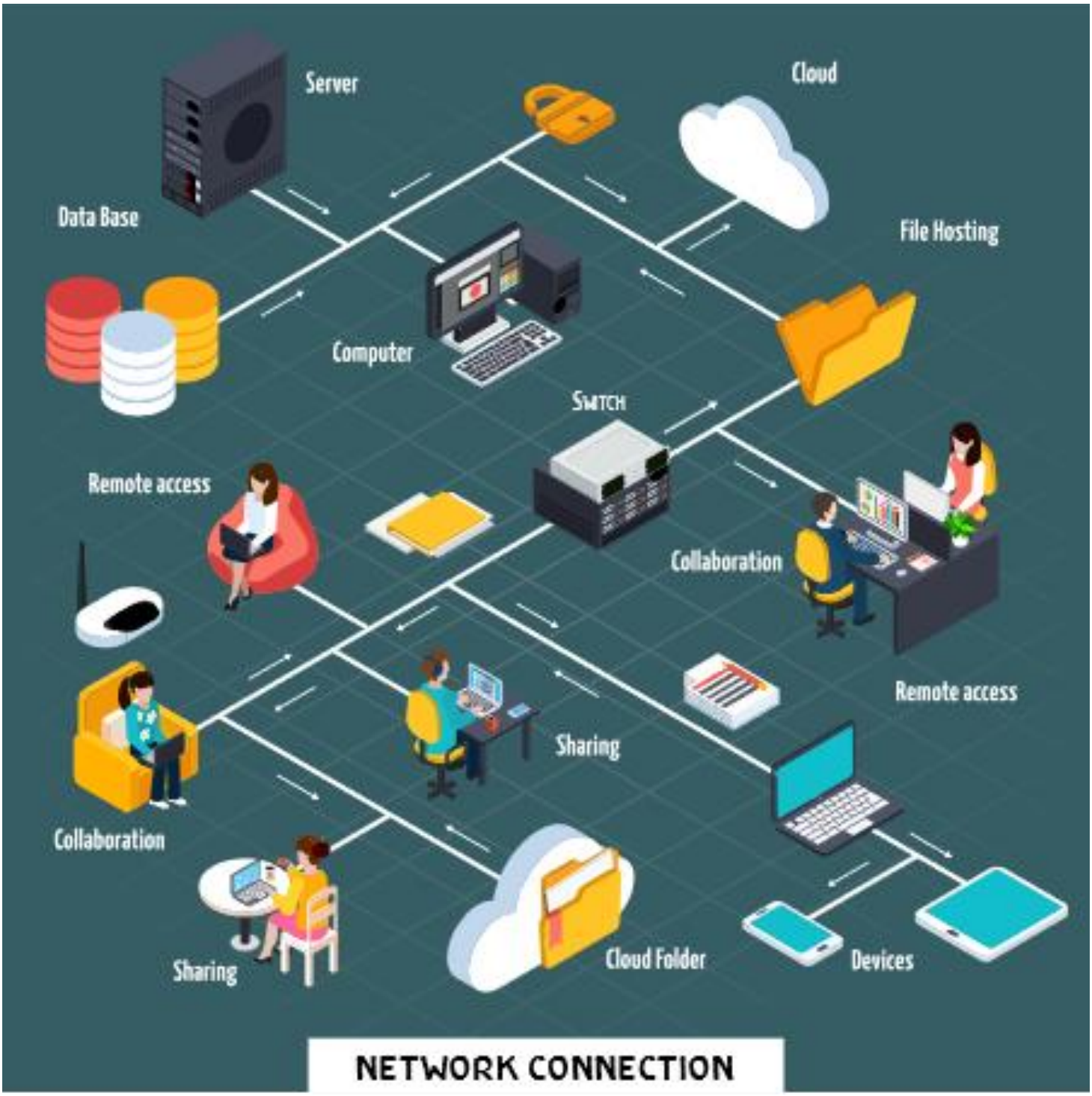
VLAN (Virtual Local Area Network) คือ ความสามารถในการจำกัด หรือแบ่งขอบเขตของการกระจายของสัญญาณภายในอุปกรณ์หรือภายในระบบ Networkออกเป็นกลุ่มๆ (ขอบเขตของการกระจายเรียกว่า Broadcast Domain) เพื่อไม่ให้สับสน ขออธิบายคำว่า LAN ก่อน เพราะ LAN เกิดมาก่อน พอระบบ Network มีขนาดใหญ่ขึ้นจึงเกิดคำว่า VLAN โดยที่ LAN เป็นการเชื่อมต่ออุปกรณ์ต่างๆ เช่น คอมพิวเตอร์ อุปกรณ์ Network เข้าด้วยกันในระยะไม่ไกลมากนัก อาจจะเชื่อมต่อด้วยอุปกรณ์ SWITCH, BRIDGE หรือ HUB เป็นต้น

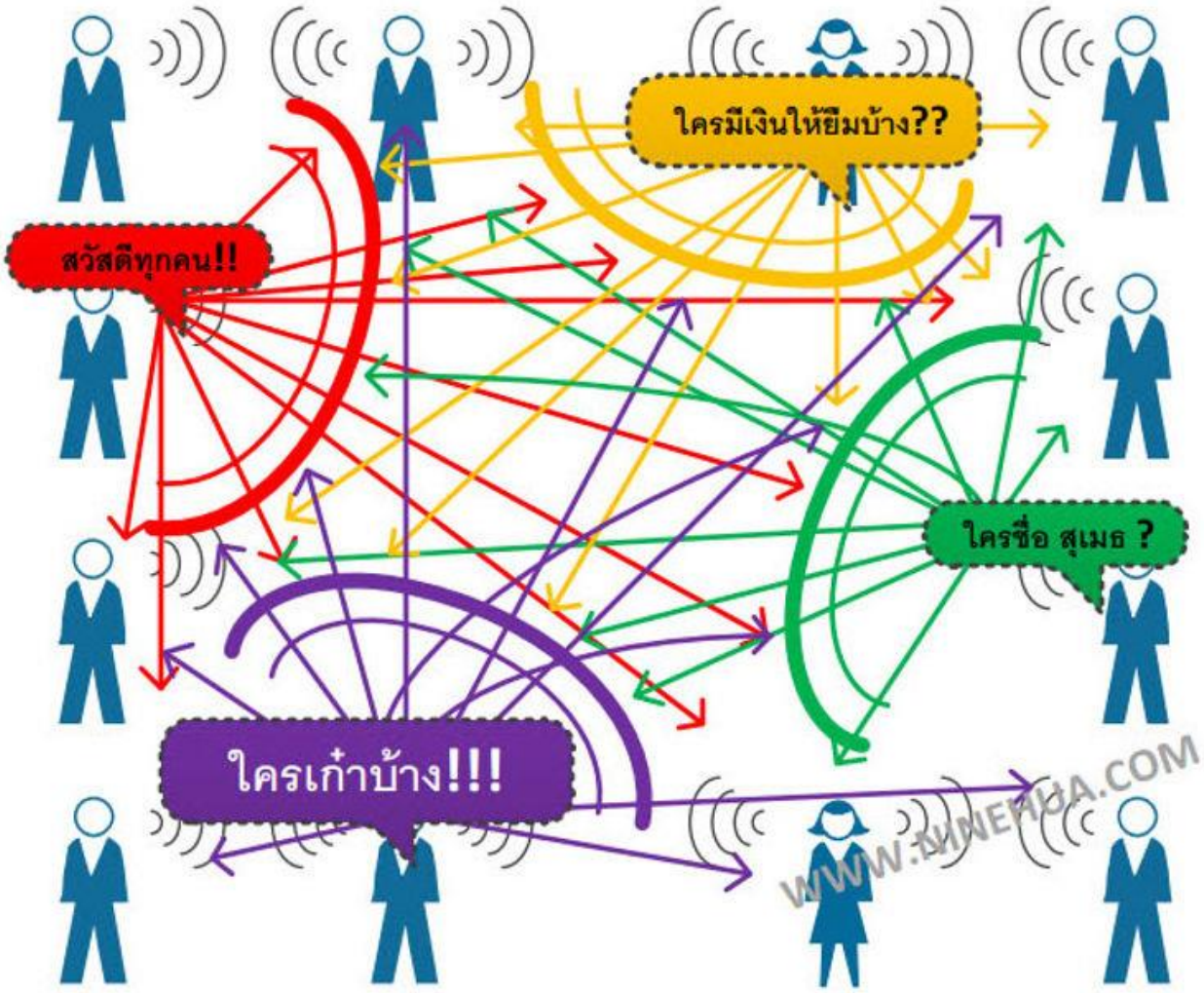


จากภาพนี้ถือว่านี่คือตัวอย่างของระบบ LAN ซึ่งเป็นการนำ SWITCH มาเป็นตัวกลางในการเชื่อมต่อ Notebook, PC, IP Phone และ Printer เข้าด้วยกัน การเชื่อมต่อ LAN ในลักษณะนี้ หากอุปกรณ์น้อยๆก็ไม่มีปัญหาอะไร แต่ถ้าหากอุปกรณ์ที่มาเชื่อมต่อมีเยอะๆขึ้น “มีปัญหาแน่ๆครับ”

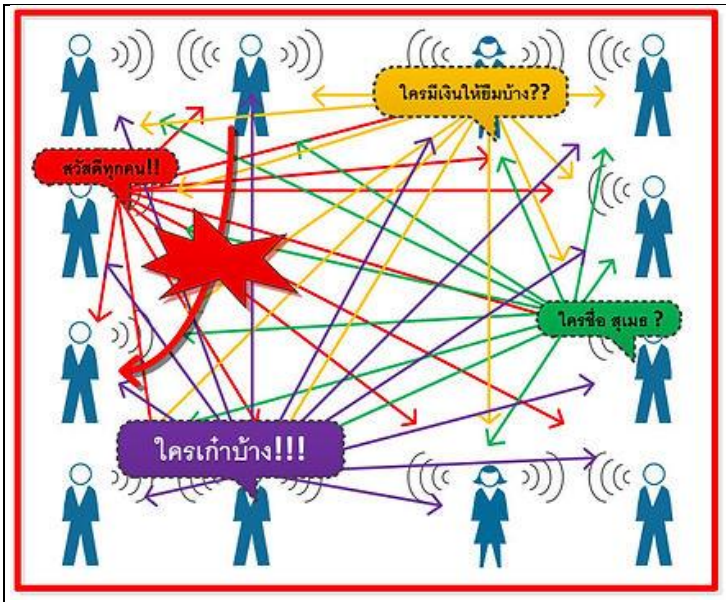
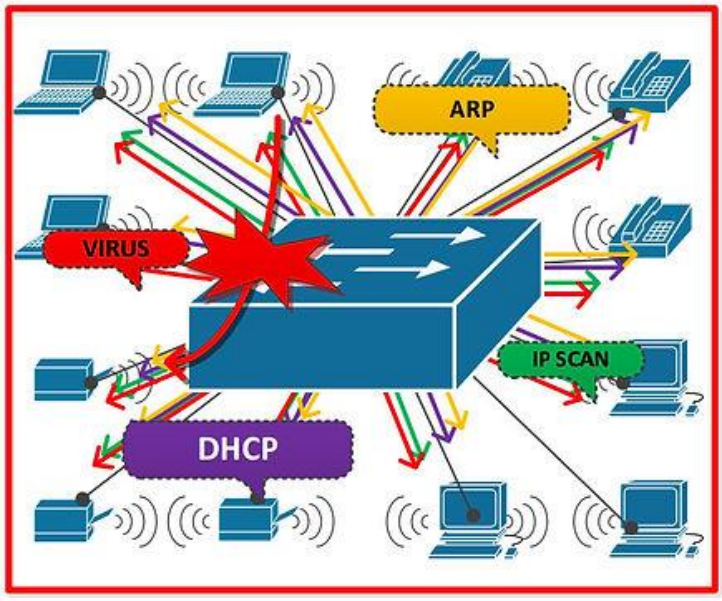
ปัญหาของระบบ LAN ที่ใหญ่เป็นอย่างไร

หากในระบบ LAN 1 วง มีการเชื่อมต่ออุปกรณ์ที่มากขึ้นเรื่อยๆ มีผลเกิดให้ระบบทำงานช้า จนถึงบางครั้งก็ทำงานไม่ได้เลย สาเหตุหลักๆเกิดจากพฤติกรรมการส่งข้อมูลแบบ Broadcast ของอุปกรณ์ (Broadcast เป็นการส่งให้อุปกรณ์ทุกๆเครื่องในวง LAN เดียวกันได้รับ)


Server
Cloud
Data Base
File Hosting
Computer
Switch
Remote access
Collaboration
Remote access
Sharing
Collaboration
Sharing
Cloud Folder
Devices
NETWORK CONNECTION

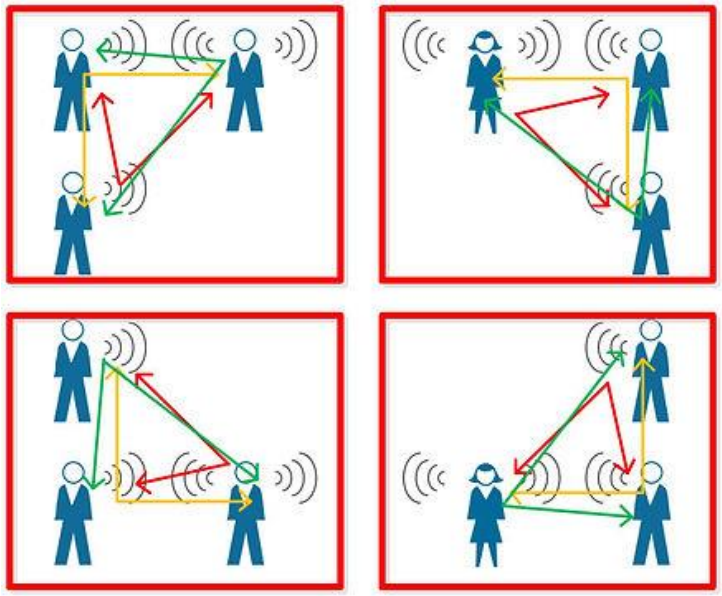
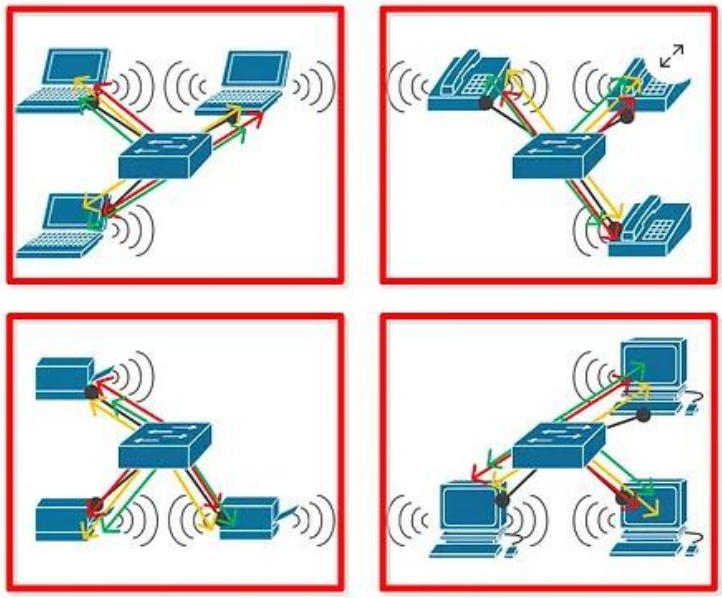


จากภาพนี้ เปรียบเสมือนทุกคนอยู่ในห้องเดียวกัน อยู่ในวง LAN เดียวกัน การ Broadcast ของสัญญาณก็เหมือนการที่ต่างคนต่างตะโกนเรียกหากัน ต่างคนต่างคุยกันเสียงดัง (ทุกคนได้รับเสียง ได้ยินเสียง) เกิดการ Broadcast หรือ กระจายของสัญญาณเสียง แน่นอนพอคนเยอะมากๆในห้อง ย่อมรบกวนกัน ทำให้หลายๆครั้งก็สื่อสารกันไม่รู้เรื่อง หรือ หากใครคนใดคนหนึ่งป่วย (เปรียบเสมือน Computer ติดไวรัส) ก็มีโอกาสแพร่เชื้อกระจายกระทบไปทั้งห้อง

	ภาพแสดงสัญญาณเสียงที่กระจาย หรือ Broadcast ออกไปหาทุกๆคน ทำให้บางครั้งคนสองคนจะคุยกันแต่ไม่สามารถที่จะสื่อสารกันได้ เพราะเกิดการรบกวน หรือ ให้นึกภาพเรากำลังโทรหาคุยกับใครอยู่ในห้องแต่ในห้องมีแต่คนตะโกนกันไปๆมาคุยกันเสียงดัง เราก็คุยกันไม่รู้เรื่อง
	ภาพแสดงในระบบ LAN ก็เช่นกัน เกิดการสื่อสารแบบ Broadcast ขึ้นมากมาย ไม่ว่าเป็นการทำงานของ Switch เอง หรือ จากอุปกรณ์ที่มาเชื่อมต่อ เช่น การทำงานของ ARP, DHCP, Programs ต่างๆ การทำงาน Switching FRAME ของ Switch เป็นต้น ปัญหาเช่น ส่งผลกระทบให้บางครั้ง Traffic เต็ม ไม่สามารถ Print เอกสารได้

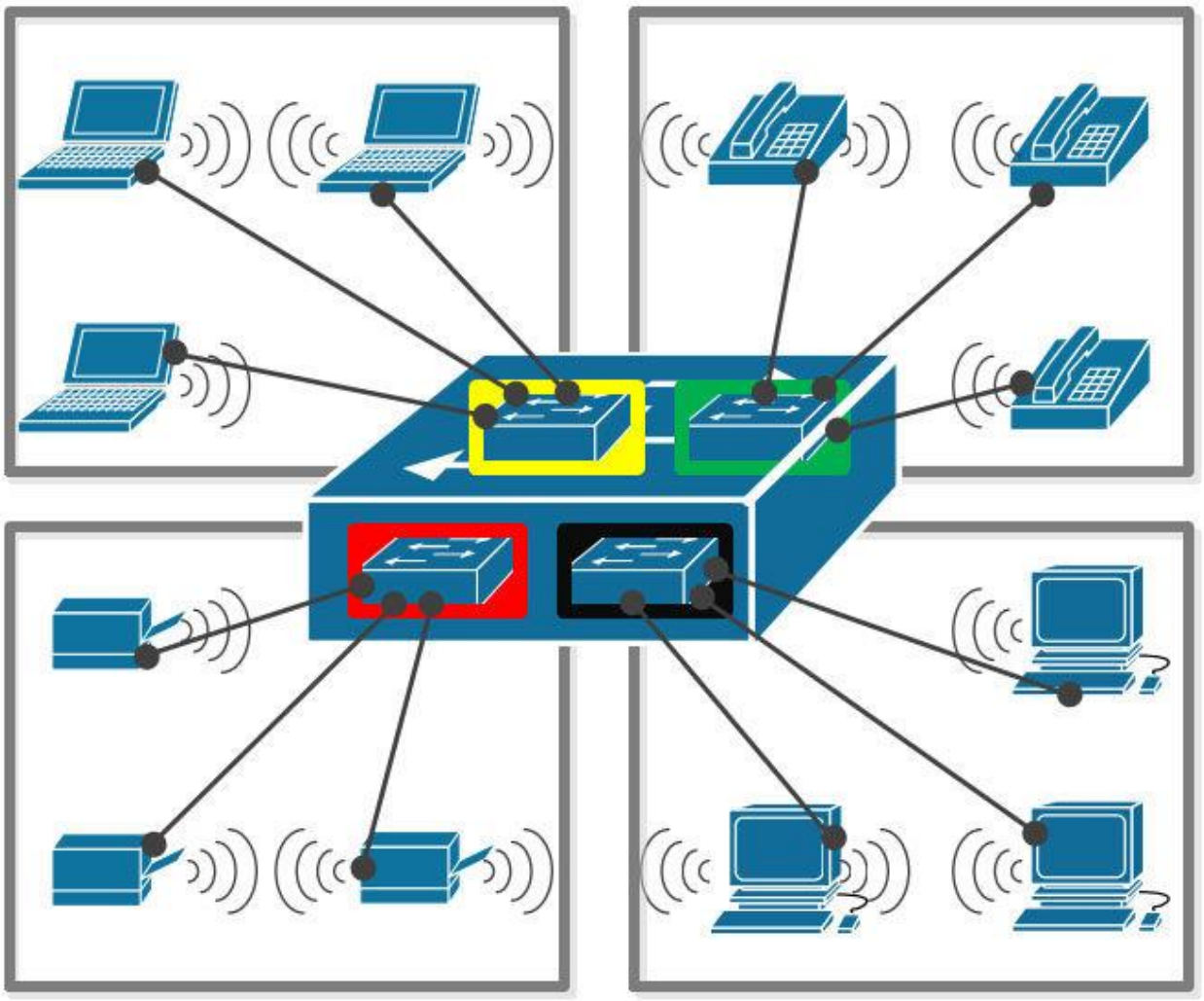
แล้วจะลดปัญหาเหล่านี้ได้อย่างไร ?

การแก้ปัญหาคือ เริ่มแรกต้องมีการออกแบบระบบ Network ที่ดี มีการจำกัดการ Broadcast ให้น้อยลง เปรียบเสมือนเราสร้างห้องแยกให้แต่ละกลุ่ม ก็จะทำให้เกิดการรบกวนกันน้อยลง สื่อสารกันรู้เรื่องขึ้น

	การแก้ปัญหาคือ จำกัด Broadcast ให้น้อยลง เปรียบเสมือนการสร้างห้องเพื่อแยกออกเป็นกลุ่มๆ การทำแบบนี้ก็จะทำให้เกิดการรบกวนน้อยลง สื่อสารกันได้รู้เรื่องขึ้นชัดเจนมากขึ้น
	การแก้ปัญหาจำกัดการขอบเขตของการกระจาย (Broadcast Domain) โดยการสร้างห้องเพิ่มก็เหมือนการซื้อ Switch มาเพิ่ม ยิ่งมีคนเยอะๆ อยากให้ไม่กวนกันมากก็ต้องสร้างห้องเพิ่มมากขึ้น หรือ ซื้อ Switch มากขึ้น และไม่ต้องต่อเข้าหากันตรงๆ (ถ้าจะเชื่อมต่อเข้าหากัน ให้คุยกันผ่านอุปกรณ์ Layer3 เช่น Router อีกที เพราะตัว Router เองก็จะกั้น Broadcast ไม่ให้ถึงกัน)

วิธีการจำกัดขอบเขตของการกระจายแบบนี้ก็ได้ผลดี แต่อาจไม่คุ้มค่ากับการลงทุนสร้างห้องหรือซื้อ Switch ใหม่หรือไม่ จากในภาพข้างต้นก็ต้องซื้อ Switch ใหม่ถึงสี่ตัว เพื่อแยกให้ Notebook, PC, Printer และ IP phone ไม่กวนกัน

ก่อกำเนิด VLAN บางครั้งเราอยากแยก Traffic ของ Notebook , IP Phone, Printer หรือ PC แต่ละแผนกไม่ให้ Broadcast มารบกวนกัน และอยากใช้ Switch ตัวเดียวให้คุ้มค่ามากที่สุด(เพราะ port ของ Switch มีค่อนข้างเยอะ เช่น 24 port/ 48 port) ด้วยเหตุนี้ นี่ก็เลยเป็นเหตุผลหนึ่งที่เกิดคำว่า “VLAN” ขึ้นมา



VLAN เป็นการแบ่งขอบเขตของการกระจายของสัญญาณภายในอุปกรณ์ในทาง Logical เพราะเราไม่ได้แบ่งในทาง Physical เราจึงเรียกความสามารถนี้ว่า “Virtual” LAN (VLAN) จากภาพด้านบนเรานำ Switch มาแบ่งเป็น 4 VLAN ก็คล้ายๆกับเราสร้าง Switch แบบ Virtual ขึ้นมา 4 ตัว (เพื่อให้มองเห็นภาพได้ชัดเจนมากขึ้น เพราะแต่ vlan ก็ยังใช้ Resource อื่นๆร่วมกัน ไม่ได้แบ่ง Switch ออกเป็นชิ้นๆจริงๆ) อุปกรณ์ตัวไหนเกาะอยู่บน

VLAN เดียวกัน ก็เหมือนกับต่อกับ Switch เดียวกัน ในภาพจะเห็นว่า

กลุ่มของ Notebook ต่อกับ VLAN สีเหลือง

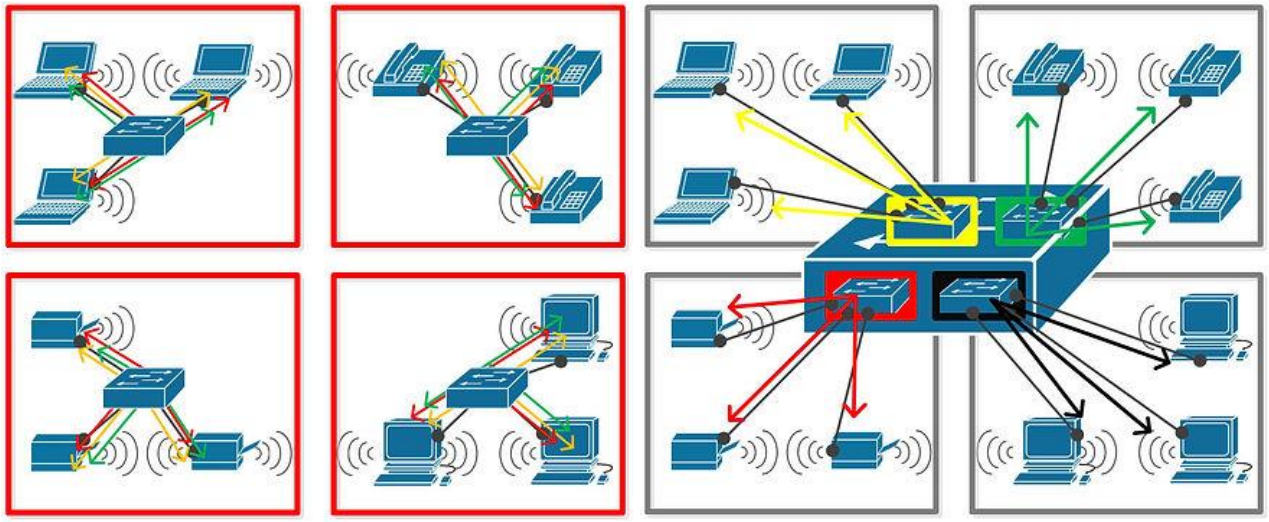
กลุ่มของ IP Phone ต่ออยู่กับ VLAN สีเขียว

กลุ่มของ Printer ต่ออยู่กับ VLAN สีแดง

กลุ่มของ PC ต่ออยู่กับ VLAN สีดำ

แต่ยังมีอีกความสามารถที่มีความเป็น Virtual ที่มากกว่าการแบ่ง VLAN คือ เรื่อง “VDC” ซึ่งเป็นการแบ่ง Switch ออกเป็นชิ้นๆได้เกือบใกล้เคียงกับ Physical

ภาพแสดงการเปรียบเทียบระหว่าง LAN กับ VLAN



ก็จะเห็นได้ว่าการทำ VLAN จะช่วยให้ใช้ Bandwidth ได้คุ้มค่ามากขึ้น เพราะสามารถลดจำนวน broadcast traffics ลงมาได้ และก็ส่งผลให้ cpu ลดการประมวลผลในสิ่งที่ไม่จำเป็นลงมาได้ด้วย อีกทั้งยังมีความปลอดภัย ลดความเสี่ยงในการโดนโจมตีในรูปแบบต่างๆ แต่ถ้าจะให้อุปกรณ์ที่เชื่อมต่อแต่ละ vlan สามารถสื่อสารข้าม vlan กันได้ เราก็สามารถใช้อุปกรณ์ Layer3 เช่น Router หรือ L3 Switch มาช่วยได้ และที่สำคัญ VLAN ยังมีความยืดหยุ่นในการใช้งาน

การกำหนดค่าต่างๆ ของ Switch ใน Cisco Package Tracer เพื่อใช้งาน VLAN

เมื่อเข้าสู่ Command ของ Switch ตัวที่ต้องการกำหนดค่า คั่งที่ใช้ในการกำหนดค่ำหรับ VLAN มีดังนี้

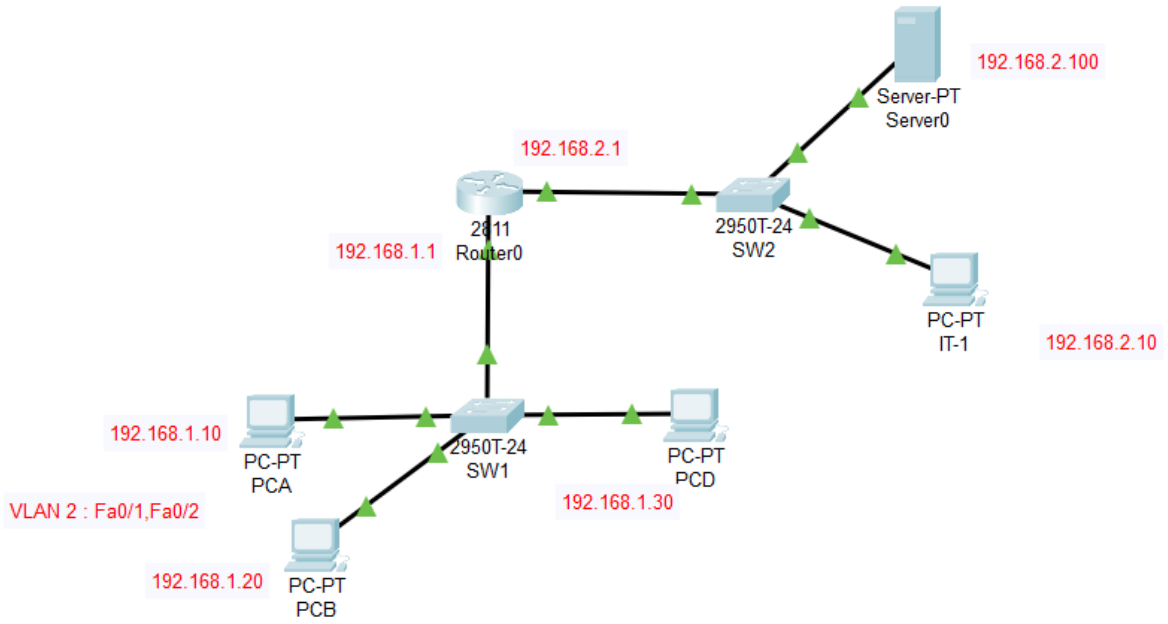
1. คำสั่งตรวจสอบ VLAN ของ Switch ว่าตั้งค่าอะไรไว้อย่างไร
2. การตั้งค่า VLAN 2 การกำหนด ชื่อ เป็น Account และกำหนด VLAN 3 เป็น Service ดังตัวอย่างด้านล่าง

```
Switch>enable

Switch#conf t

Switch(config)#vlan 2

Switch(config-vlan)#name Account

Switch(config-vlan)#vlan 3

Switch(config-vlan)#name Service

Switch(config-vlan)#end

Switch#show vlan
```

3. การกำหนด ว่า Port ไหนเป็น Vlan ตัวไหน

```
Switch#conf t

Switch(config)#int fa 0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 2

Switch(config-if)#exit
```

ตัวอย่างการตั้งค่า VLAN



VLAN2 แผนก IT วงนี้ประกอบด้วย PC IT-1,Server 0

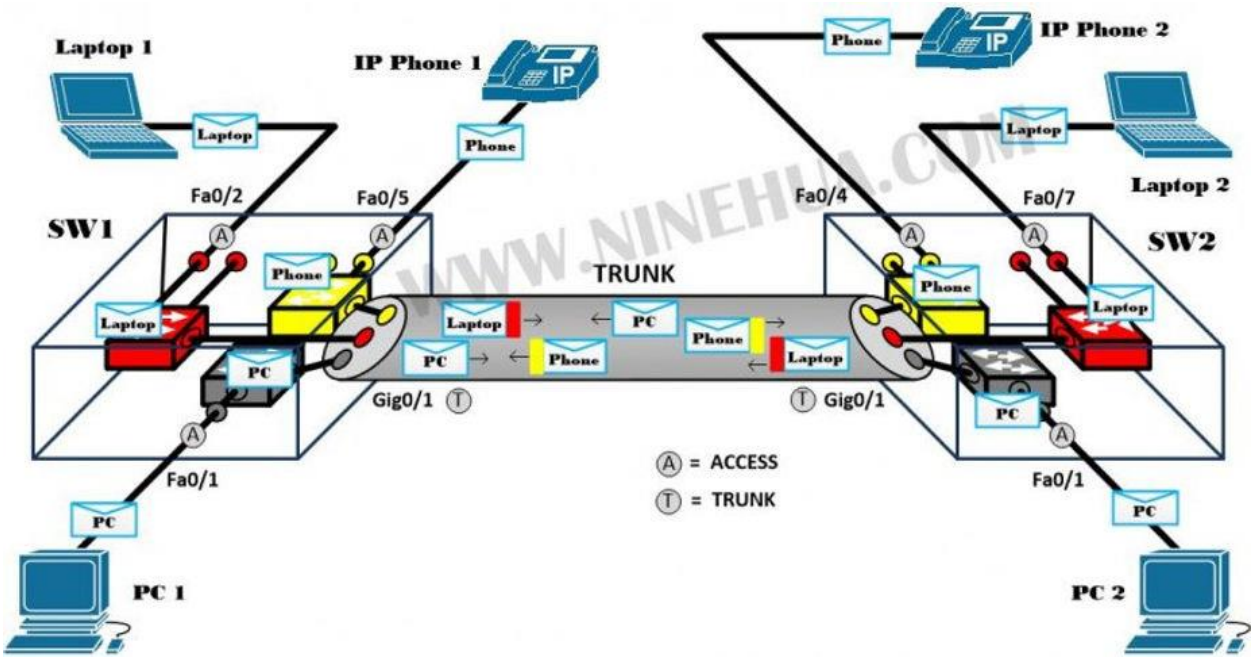
VLAN3 แผนก Account วงนี้ประกอบด้วย PCA,PCB

VLAN4 แผนก Service วงนี้ประกอบด้วย PCD

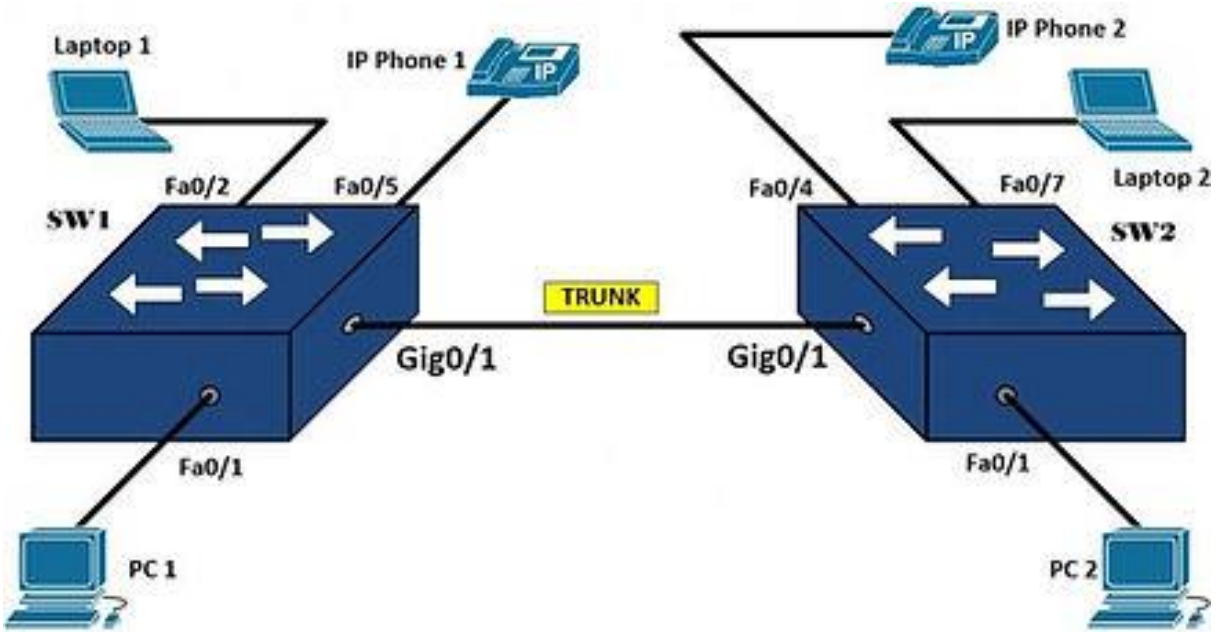
Trunk

Trunk Port คืออะไร

Trunk port เป็น Port ที่สามารถมี Traffic ของหลายๆ VLAN วิ่งผ่านได้ (Traffic จะมีการ Tag vlan หรือ อาจจะไม่ tag vlan ก็ได้) ตัวอย่างในการตั้งค่า Port ของ Switch ให้เป็น Trunk Port เช่น - Port ที่ทำหน้าที่เชื่อมต่อไปยัง Switch ตัวอื่น ๆ เช่น Uplink Port - Port ที่ทำหน้าที่เชื่อม ไปยัง Routerตัวที่ทำหน้าที่ Route Traffic ระหว่าง VLAN

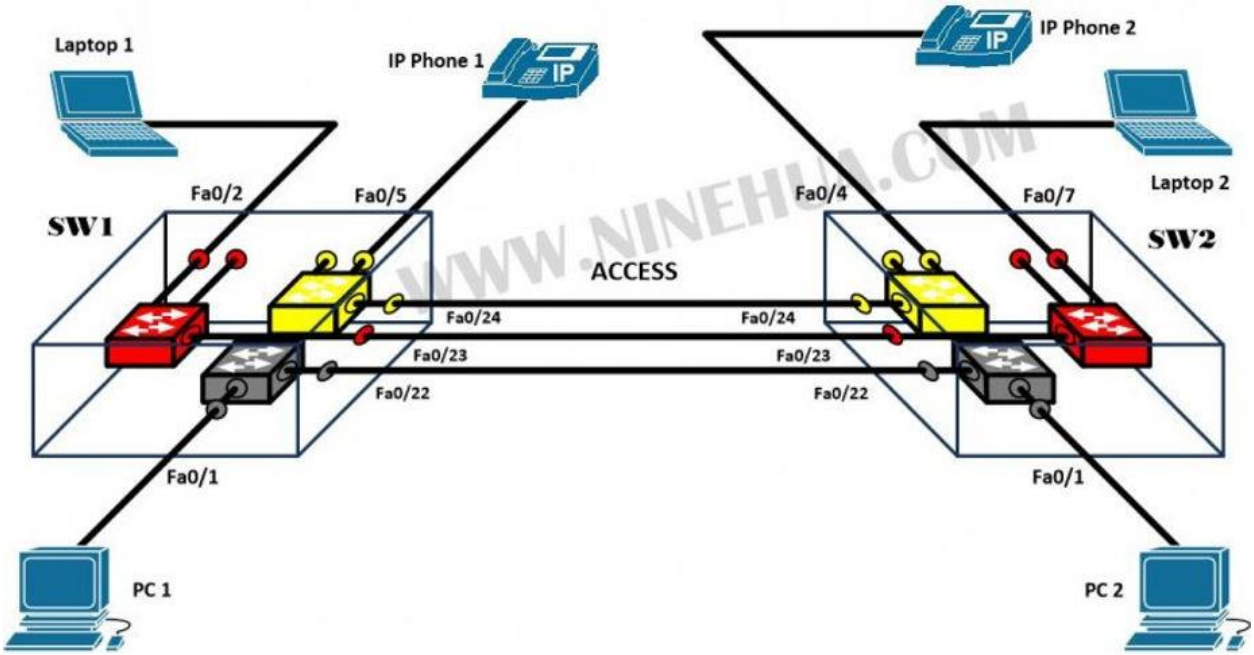


Trunk Port และ Access Port จะใช้ภาพ Network Diagram ด้านล่างนี้ในการอธิบายเรื่อง Trunk Port

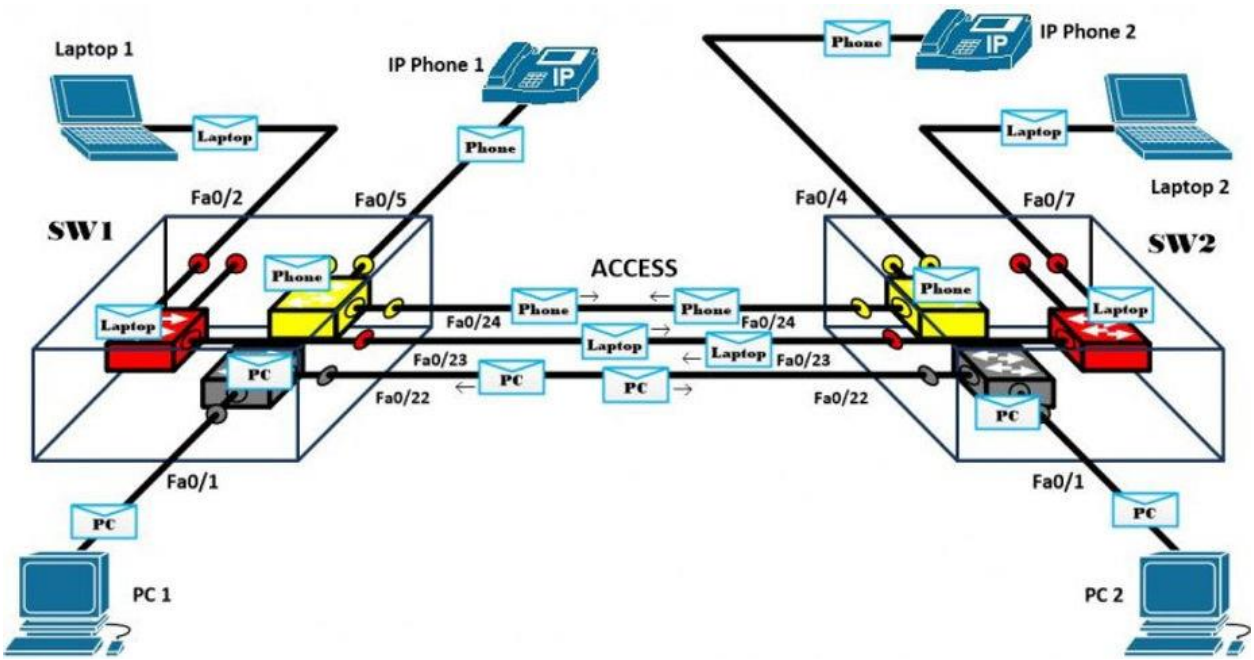


หากเราต้องการขยาย VLAN ให้ยืดยาวออกไป เช่น ใน SW1 มีการสร้าง VLAN ขึ้นมา 3 VLAN และเราต้องการยืดหรือขยาย VLAN ทั้ง 3 VLAN นี้ให้ไปอยู่ที่ SW2 อีกอาคารหนึ่ง (SW2 ก็ต้องมีการตั้งค่าให้มี 3 VLAN เช่นกัน) แน่นอนว่าเราก็ต้องหา Port มาเชื่อมต่อเพื่อเป็น Uplink ระหว่าง Switch ทั้ง 2 เข้าด้วยกัน

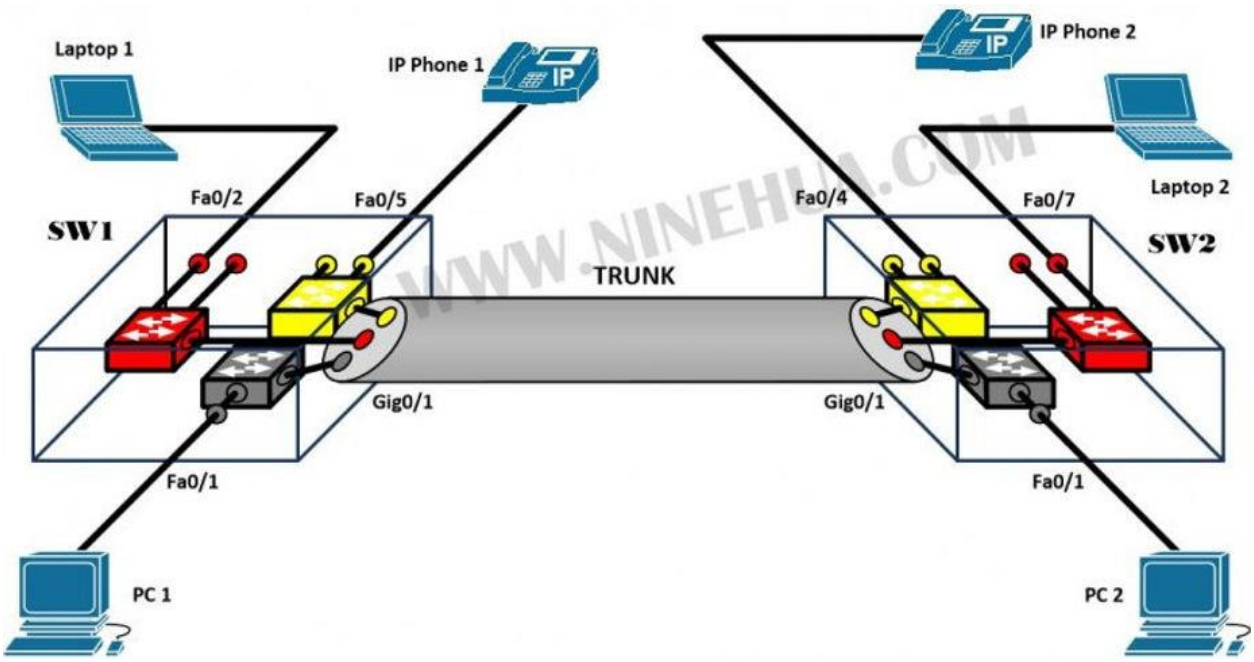
กรณีที่ 1 ใช้ Uplink เป็น Access Port หากเราตั้งค่า Uplink ให้เป็น Access Port แล้วเราจะขยาย VLAN ทั้ง 3 VLAN ออกไป เราก็จำเป็นต้องใช้ Uplink ถึง 3 Port ด้วยกัน เพราะว่า Access Port จะมี traffic ของ VLAN เพียง VLAN เดียวเท่านั้นที่วิ่งผ่านได้



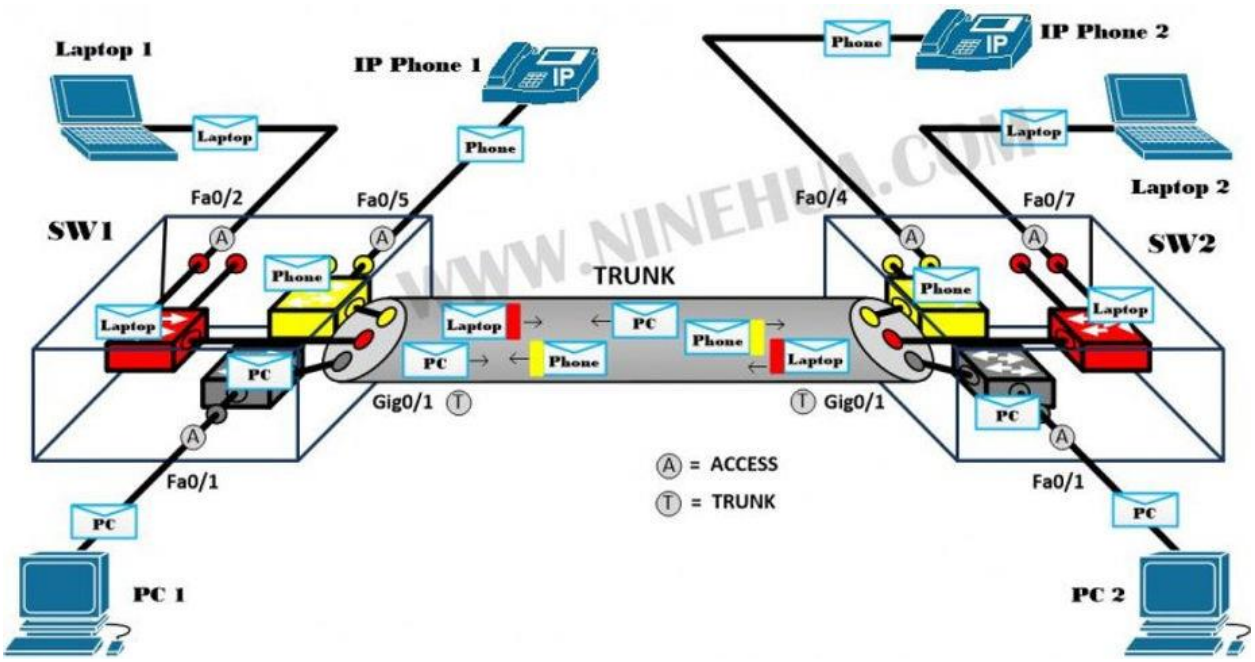
จากภาพตัวอย่างข้างต้น ที่ SW1 และ SW2 มีการสร้าง VLAN ไว้ 3 VLAN คือ VLAN RED, VLAN Yellow และ VLAN Black แล้วมีการยืด VLAN ทั้ง3นี้ จาก SW1 ไปยัง SW2 ผ่าน Uplink ที่เป็น Access Port เมื่อมี 3 VLAN ก็ต้องใช้ Uplink ถึง 3 Port (1 Uplink : 1 VLAN)



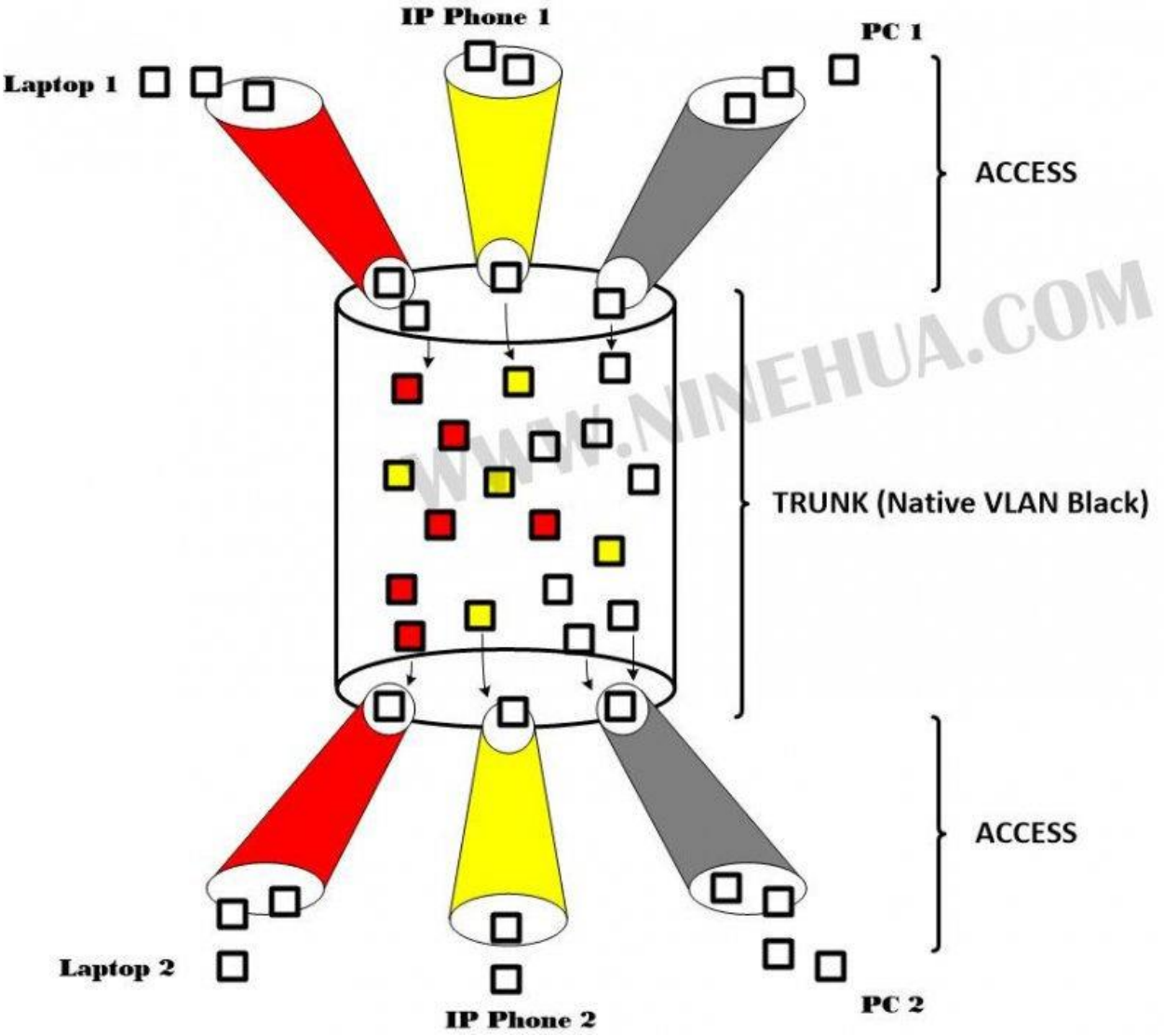
ผลจากการยืดขยาย VLAN ออกไป ทำให้ PC1 กับ PC2 เปรียบเสมือนต่ออยู่บน Switch ตัวเดียวกัน สามารถตั้งค่า IP Address ให้อยู่ในวงSubnet เดียวกันได้เลย ในส่วนของ Laptop และ IP Phone ก็เป็นไปตามกรณีเดียวกับ PC แต่อยากให้ลองนึกภาพตามนะครับ ถ้าหากเรามี VLAN จำนวนประมาณ 10 VLAN ที่ต้องยืดขยายออกไปยัง Switch ตัวอื่นๆ แล้วใช้ Access Port เป็น Uplink เราต้องเสีย Uplink ไปถึง 10 Port มันคงดูไม่เหมาะสมเท่าไหร่ที่เราจะใช้ Uplink มากมายขนาดนั้น กรณีที่ 2 ใช้ Uplink เป็น Trunk Port จากปัญหาข้างต้นของการใช้ Access Port เป็น Uplink เพื่อยืดขยาย VLAN ออกไป เราสามารถแก้ปัญหาดังกล่าวโดยการใช้ Trunk Port มาทดแทนได้ (การทำ Trunk Port เรียกได้อีกอย่างว่าการทำ Tagged)



หากเราใช้ Trunk Port มาเป็น Uplink เราจะทำการยืดขยายกี่ VLAN ก็ได้ไปยัง Switch ตัวอื่นๆ โดยใช้ Port แค่เพียง Port เดียว(จากภาพตัวอย่างด้านบนใช้ Port Gig0/1) เพราะว่า Trunk Port สามารถมี Traffic ของหลายๆ VLAN วิ่งผ่านได้ พอมีการตั้งค่า Uplink ให้เป็น Trunk Port ให้ทุกคนลองจินตนาการว่า Port Gig0/1 เสมือนไปเชื่อมต่อกับกล่อง VLAN ทุกๆกล่องนั่นเอง เมื่อมี Traffic ของหลายๆ VLAN วิ่งผ่านอยู่ใน Port เดียวกัน แล้วฝั่งต้นทาง(SW1)กับปลายทาง(SW2)จะแยกแยะและรู้ได้อย่างไร ว่า Traffic ไหนเป็นของ VLAN อะไร คำตอบคือจำเป็นต้องมีเทคนิคอะไรบางอย่างเพิ่มเติมสำหรับการแยกแยะ Traffic ของ VLAN ซึ่งเทคนิคที่ว่านี่เป็นการเพิ่มหรือระบุ VLAN เข้าไปใน Traffic นั้นๆ



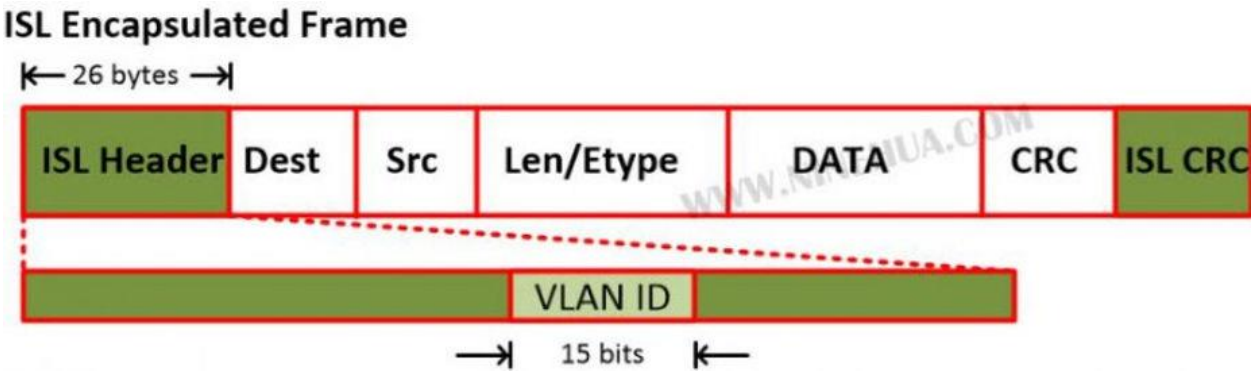
ให้ลองมองดูภาพด้านล่าง เพื่อจะได้เข้าใจเทคนิคการเพิ่มฟิลด์ของ VLAN เข้าไป



กล่องสี่เหลี่ยมที่แสดง เปรียบเสมือนว่าเป็นข้อมูลที่สร้างขึ้นจาก Laptop, IP Phone และ PC เมื่อข้อมูลวิ่งอยู่ใน Access Port ก็จะเป็น Frame ข้อมูลปกติ ซึ่งTraffic แต่ละ VLAN ก็จะไม่ปะปนกัน เพราะ Access Port มี Traffic ของ VLAN เดียววิ่งผ่านอยู่แล้ว จึงไม่มีการเพิ่มฟิลด์ VLAN ในข้อมูลหรือ Frame บน Access Port แต่เวลา Frame ข้อมูลวิ่งเข้าสู่ Trunk Port จะต้องมีการเพิ่มฟิลด์ของ VLAN เข้าไป ยกตัวอย่าง ข้อมูลที่ส่งจาก Laptop 1 เมื่อวิ่งเข้าสู่ Trunk Port ตัว Frame ข้อมูลจะถูกเพิ่มฟิลด์ VLAN เข้าไป เพื่อสื่อว่าเป็น VLAN RED และเมื่อ Frame เดินทางออกจาก Trunk Port ก็จะถูกเอาฟิลด์ VLAN ออก แล้วส่ง Traffic ไปยังปลายทางที่เป็น Access Port ของ VLAN RED ต่อไป ข้อมูลที่ส่งจาก IP Phone 1 เมื่อวิ่งเข้าสู่ Trunk Port ข้อมูลจะถูกเพิ่มฟิลด์ VLAN เข้าไป เพื่อสื่อว่าเป็น VLAN YELLOW และเมื่อ Frame เดินทางออกจาก Trunk Port ก็จะถูกเอาฟิลด์ VLAN ออก แล้วส่งไปยังปลายทางที่เป็น Access Port ของ VLAN YELLOW ต่อไป ข้อมูลที่ส่งจาก PC 1 เมื่อวิ่งเข้าสู่ Trunk Port ตัว Frame ข้อมูลจะ”ไม่”ถูกเพิ่มฟิลด์ VLAN เข้าไป “ถ้าหาก VLAN นี้เป็น Native VLAN”

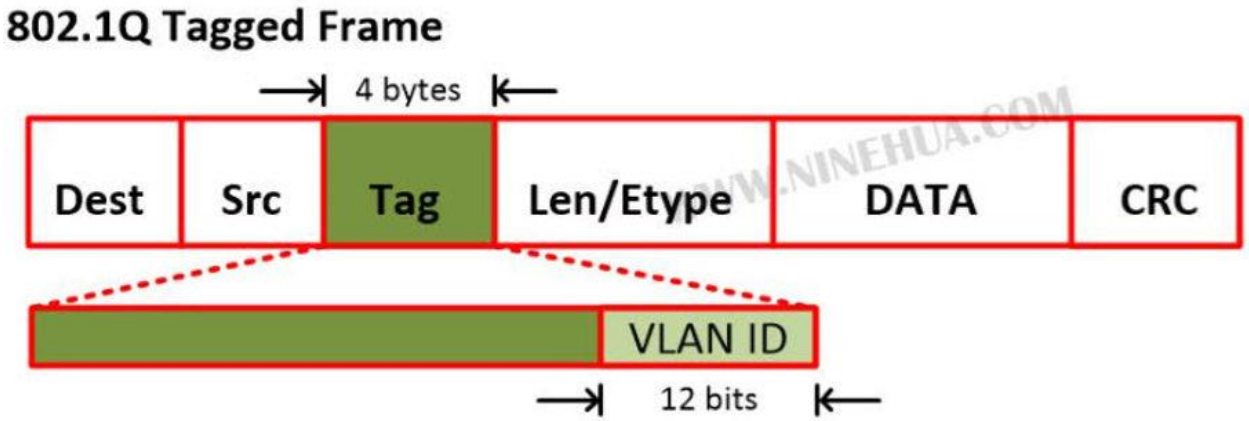
และเมื่อ Frame เดินทางออกจาก Trunk Port ก็จะถูกเอาส่งไปยังปลายทางที่เป็น Access Port ของ Native VLAN นั้นๆต่อไป หมายเหตุ : สำหรับ IEEE 802.1Q (จะอธิบายในหัวข้อถัดไป) ใน 1 Trunk Port จะมี Native ได้แค่ 1 VLAN เท่านั้น ซึ่ง Frame ที่อยู่ใน VLAN ที่เป็น Native VLAN จะไม่ถูกเพิ่มฟิลด์ของ VLAN เมื่อถูกส่งอยู่ภายใน Trunk Port เรื่อง Native จะขออธิบายเพิ่มเติมในบทความต่อๆไปนะครับ **เทคนิคการเพิ่มฟิลด์ VLAN ใน Trunk Port มีอยู่ 2 วิธี คือ** 1 แบบ Inter Switch Link (ISL) โดยปกติ Frame ข้อมูลที่อยู่ใน Access Port จะเป็น Frame ข้อมูลที่เรียกว่า “Untagged Ethernet Frame” ตามภาพด้านล่างนี้

วิธีการเพิ่มฟิลด์ VLAN แบบ ISLนี้ใช้ได้กับอุปกรณ์ของยี่ห้อ Cisco เท่านั้น (Cisco Proprietary) ซึ่งจะทำการเพิ่ม ISL Header (26 bytes) และ CRC (4 bytes) รวม 30 bytes เข้าไปตามภาพด้านล่าง โดยภายใน ISL Header ก็จะมีในส่วนของ VLAN อยู่ภายในอีกที ดังนั้นวิธีการนี้ถือได้ว่าเป็นการ Encapsulation Frame เดิมทั้งหมด และก็มีการสร้าง Headerใหม่ขึ้นมา

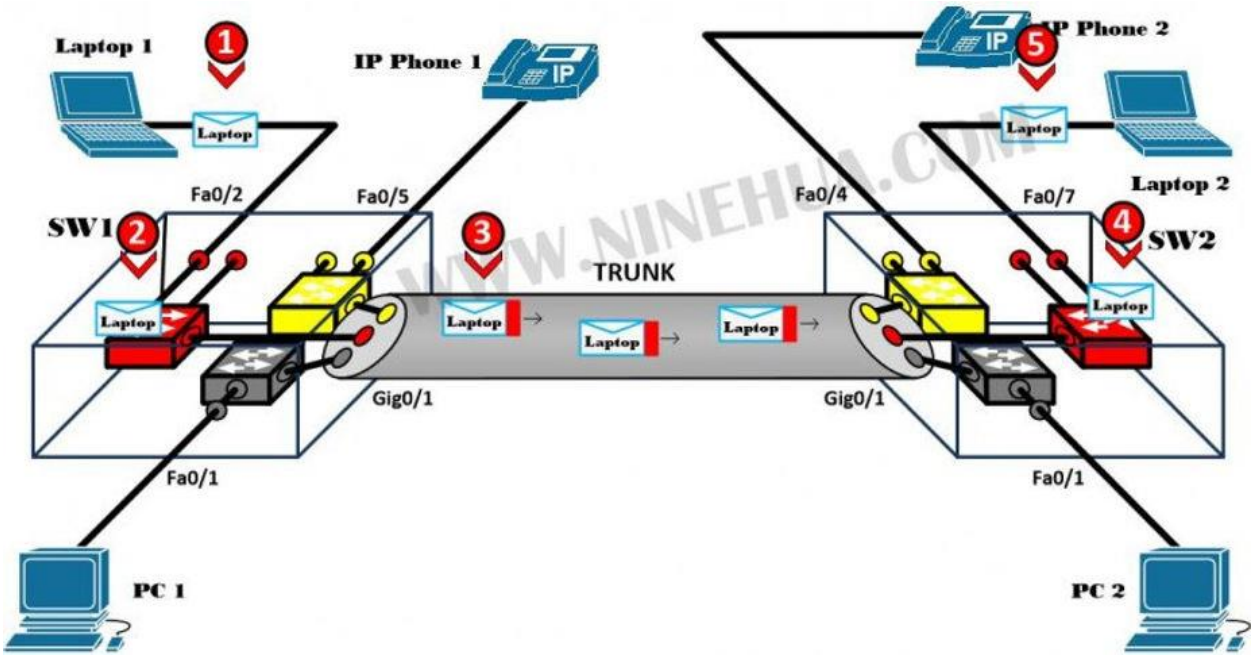


2 แบบ IEEE 802.1Q

วิธีนี้จะเพิ่มฟิลด์ Tag ขนาด 4 bytes เข้าไประหว่าง Frameเดิมตามรูปด้านล่าง และภายในฟิลด์ Tag ที่เพิ่มเข้าไปจะมีในส่วนของ VLAN ขนาด 12 bits ประกอบอยู่ด้วย ซึ่งวิธีนี้เป็นมาตรฐานกลางของ IEEE และเป็นวิธีที่นิยมนำมาใช้งานมากที่สุดในปัจจุบัน (วิธีนี้รองรับการใช้งาน Native VLAN)



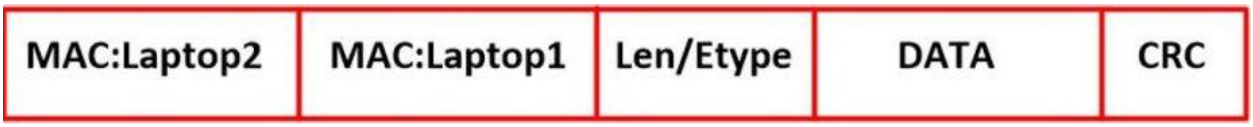
ตัวอย่างการส่งข้อมูลผ่าน Access Port และ Trunk Port (802.1Q) VLAN BLACK = VLAN 1 VLAN RED = VLAN 2 VLAN YELLOW = VLAN 3



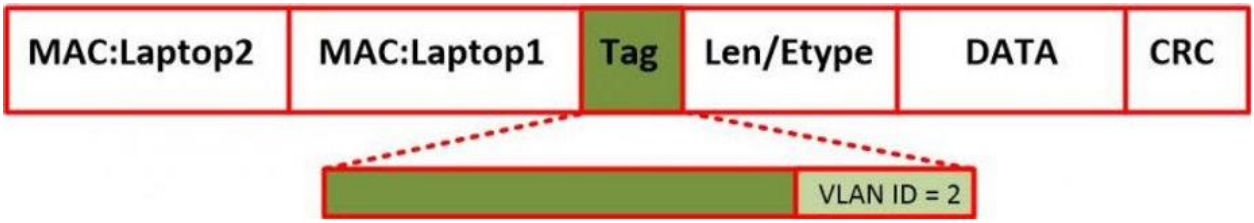
จากภาพขอยักตัวอย่างการส่งข้อมูลจาก Laptop 1 ไปยัง Laptop 2 ซึ่งทั้ง 2 เครื่องอยู่ใน VLAN RED (การยกตังอย่างนี้ไม่ได้ลงรายละเอียดถึงการเรียนรู้ MAC Address และการทำงาน Switching ของ Switch นะครับ แต่

ต้องการให้เข้าใจเรื่องการ Tagging VLAN) จุดที่ 1 ข้อมูลถูกสร้างจาก Laptop 1 และต้องการส่งไปยังผู้รับคือ Laptop 2

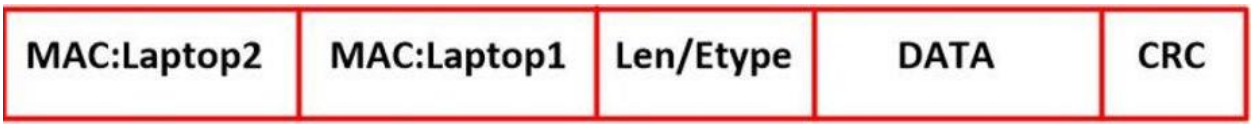
จุดที่ 2 ข้อมูลวิ่งเข้าสู่ Access Port (Interface Fa0/2) ของ SW1 ซึ่ง Portนี้ เป็นสมาชิกของ VLAN RED ซึ่งมี VLAN ID = 2 ข้อมูลก็จะยังคงเหมือนเดิมไม่มีการ Tag อะไรเข้าไป



จุดที่ 3 เมื่อ Frame ข้อมูลถูกส่งต่อไปยัง Uplink Port ของ SW1 ที่เป็น Trunk Port (Interface Gig0/1) ตัว Frame ข้อมูลจะต้องถูก Tag VLAN เข้าไป เพื่อให้ SW2 ที่เป็นปลายทางแยกแยะได้ว่า Traffic ที่ได้รับมานั้นเป็น Traffic ของ VLAN ใด ฉะนั้นเมื่อข้อมูลที่รับมาเป็นของ VLAN RED ซึ่งมี VLAN ID = 2 ผลที่ได้จึงแสดงตามภาพด้านล่างนี้



จุดที่ 4 เมื่อข้อมูลไปถึง Trunk Port ปลายทางอีกฝั่ง(Interface Gig0/1)ของตัว SW2 ตัว SW2 ก็จะรู้ได้ทันทีว่า Traffic นี้เป็นของ VLAN 2 (เพราะมีการ Tag VLAN 2 มา) และ SW2 ก็จะส่งต่อข้อมูลนี้ให้ Laptop 2 (Laptop 2 ต่ออยู่กับ Interface Fa0/7 ซึ่งเป็น Access Port) SW2 จึงทำการถอด Tag ออก แล้วส่งออกไปยัง Port Fa0/7ดังกล่าว



จุดที่ 5 ข้อมูลที่ Laptop 2 ได้รับ จึงเป็นข้อมูลที่ไม่ได้ถูก Tag อะไรเข้าไป