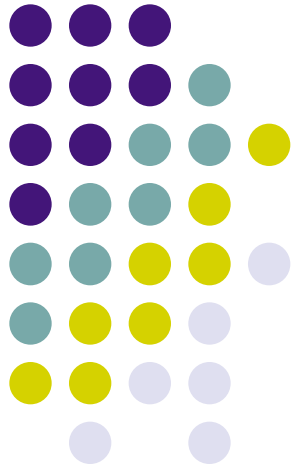
Network Security

Basic Computer Network

Mr.Jantapong Boodluck

Electronic Computer Technology

King Mongkut's University of Technology North Bangkok

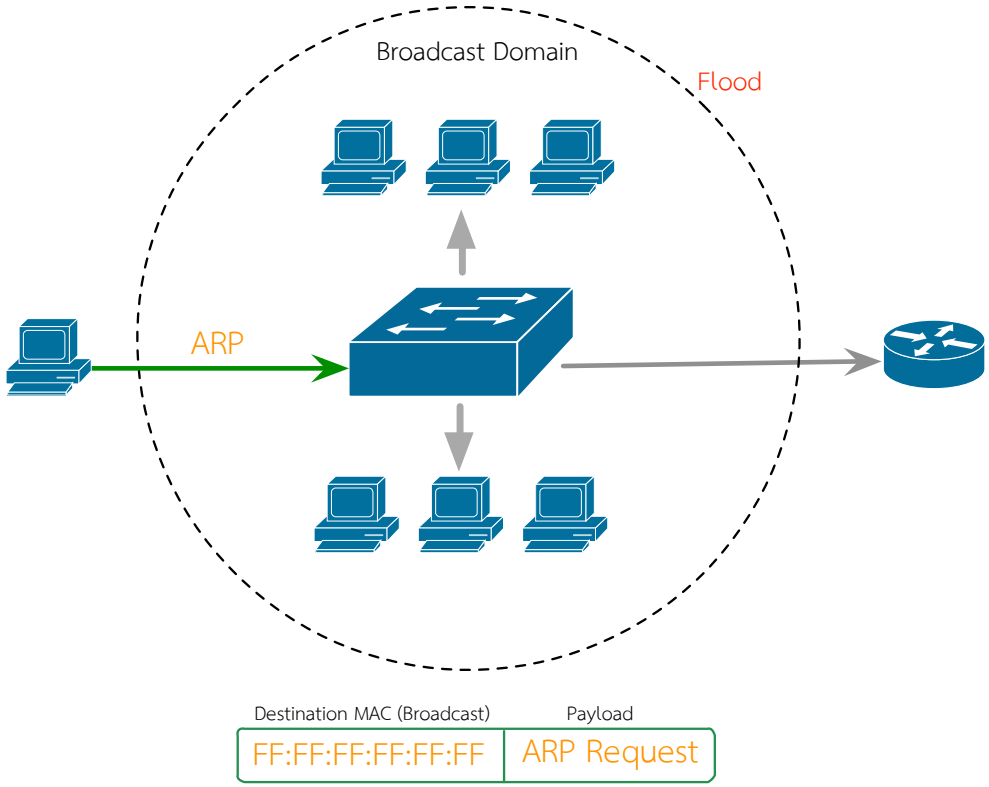


Outline

- Broadcast Domain
- VLAN (Virtual LAN)
- Trunk
- Inter-VLAN Routing

VLAN & Trunk

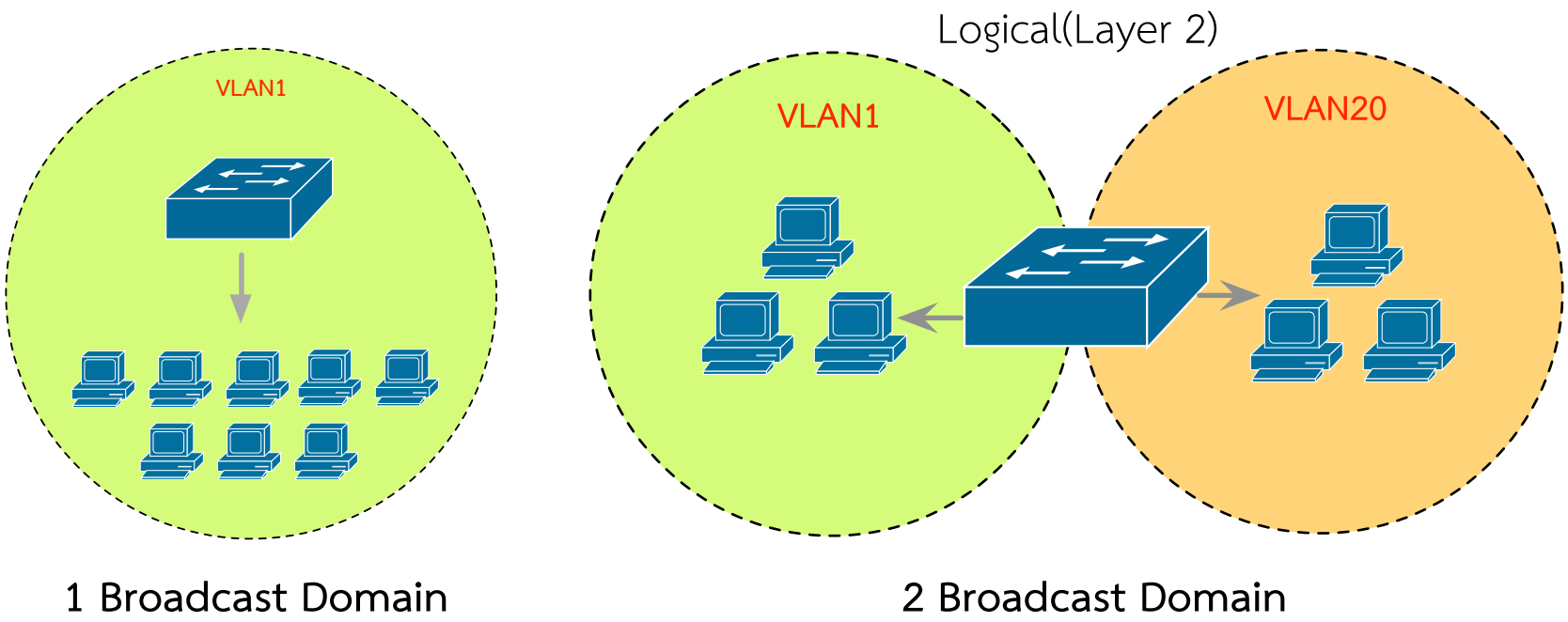
Broadcast Domain



- Broadcast Domain = LAN = VLAN = Subnet
- Broadcast Frame ยิ่งกระจายมาก Bandwidth ก็จะสิ้นเปลือง

VLAN & Trunk

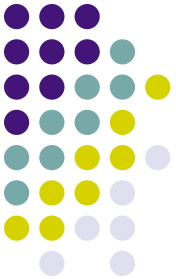
VLAN



1 Broadcast Domain

2 Broadcast Domain

VLAN ย่อมาจาก Virtual LAN เป็นเทคโนโลยีที่ใช้ในการจำลองสร้างเครือข่าย LAN แต่ไม่ขึ้นอยู่กับการเชื่อมต่อทางกายภาพ

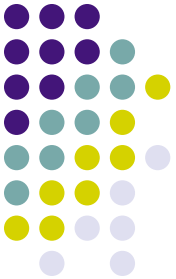


ลักษณะพิเศษของ VLAN ทั่วๆ ไปคือ

- VLAN แต่ละเครือข่ายที่ติดต่อกันนั้น จะมีลักษณะเหมือนกับต่อแยกกันด้วยบริดจ์
- VLAN สามารถต่อข้ามสวิตช์หลายตัวได้

ประโยชน์ของการแบ่ง VLAN

- *ใช้แบนด์วิธคุ้มค่า* โดยลดความหนาแน่นของ Broadcast Frame
- *เพิ่มความปลอดภัย* โดยจำกัดการเข้าถึงข้าม VLAN ด้วยฟีเจอร์ Layer3 เช่น ACL
- *จำกัดความเสียหายแค่ VLAN เดียว* เช่น ผลของ Layer 2 Loop หรือแอพพลิเคชั่นที่ใช้การสื่อสารแบบ Broadcast มีปัญหา



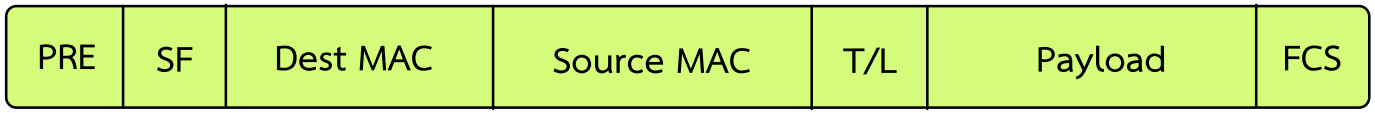
มาตรฐานของ VLAN คือ 802.1Q

มาตรฐาน IEEE 802.1Q นั้นเป็นมาตรฐานในการนำข้อมูลของ VLAN membership ใส่เข้าไปใน Ethernet Frame หรือที่เรียกว่า การ Tagging

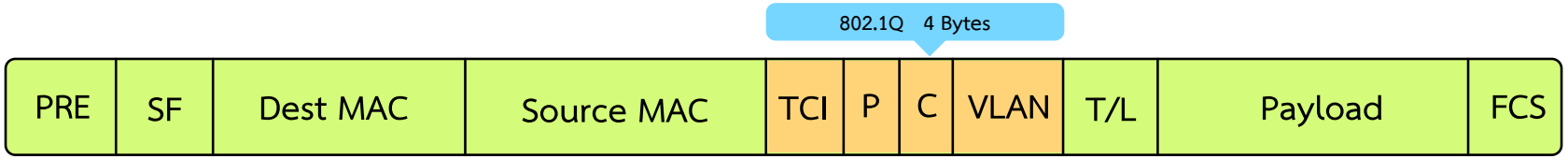
การต่อเติมเฟรม (Tagging Frame) ด้วยมาตรฐาน 802.1Q นั้นจะทำในระดับ Data-Link layer และการทำ VLAN Tagging นั้นจะเป็นการเปลี่ยนรูปแบบของ Ethernet Frame มาตรฐาน 802.3 ให้เป็นรูปแบบใหม่ที่เป็นมาตรฐาน 802.3 ac

VLAN & Trunk

VLAN



แสดงรูปแบบของเฟรม 802.3 ก่อนที่จะทำ VLAN Tagging



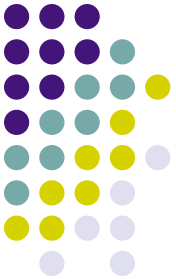
แสดงรูปแบบของเฟรม 802.3 ที่มีการ Tagging 802.1Q แล้ว

VLAN & Trunk

VLAN

Label	Field Name	Size	Description
PRE	Preamble	7 bytes	Used to synchronize traffic between nodes
SF	Start Frame Delimiter	1 bytes	Marks the beginning of the header
TCI	Tag Control Info	2 bytes	When set to “8100”, indicates this frame uses 802.1p and Q tags
P	Priority	3 Bit	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 Bit	Indicates if the MAC address are in canonical format Ethernet uses “0”
VLAN	VLAN Identifier (VID)	12 Bit	Indicates which VLAN this frame belongs to 0-4095
T/L	Type/Length Field	2 bytes	Ethernet II “type” or 802.3 “length” information
Payload	Payload	<=1500 bytes	User data or higher layer protocol information
FCS	Frame Check Sequence	4 bytes	Error checking on the frame’s contents-also known as “CRC”

แสดงคำอธิบายรูปแบบของเฟรม 802.1Q



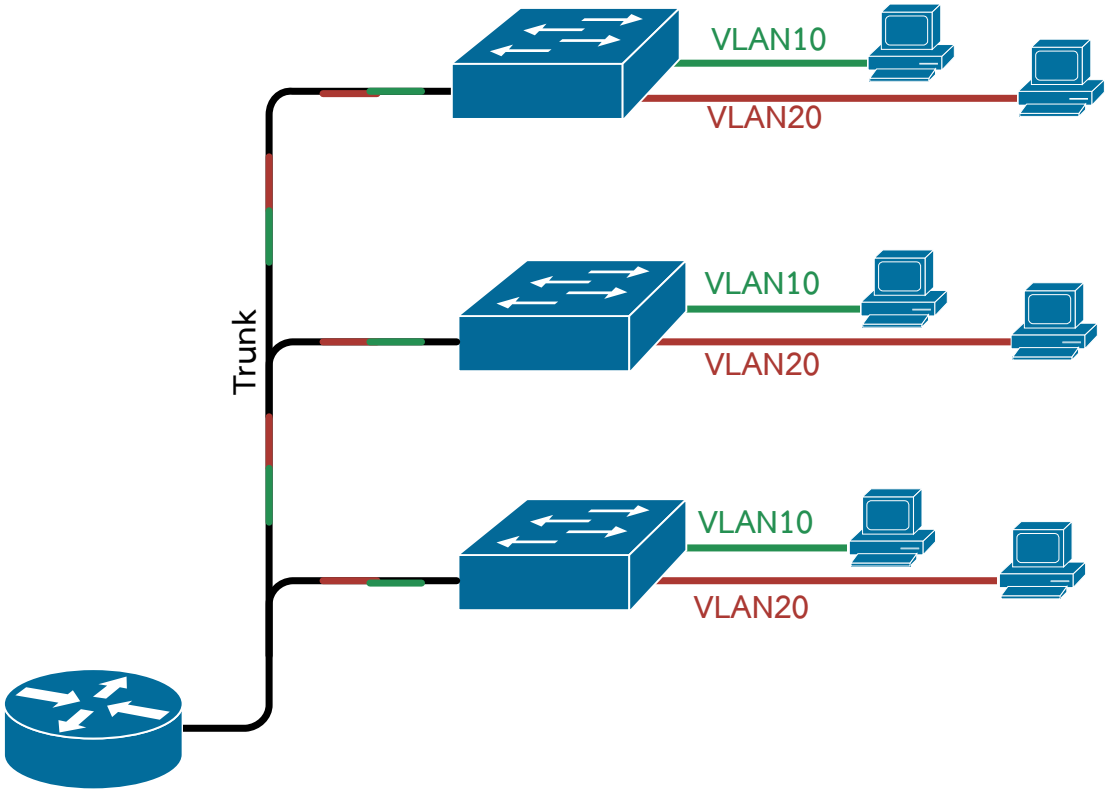
ช่องโหว่ VLAN

“การเบรค VLAN" ซึ่งช่องโหว่นี้เกิดจาก Trunking Protocol ของสวิตช์บางรุ่น

วิธีการทดสอบคือ ทำการส่งข้อมูลตัวอย่างจาก VLAN หนึ่งไปยัง VLAN อื่น ที่อยู่บนสวิตช์คนละตัวและข้อมูลที่ส่งนั้นให้ทำการสร้าง Ethernet Frame ที่มี Tag 802.1Q และเปลี่ยนค่าของหมายเลข VLAN ให้เป็นค่าของหมายเลข VLAN ปลายทางที่ต้องการเบรคการทดสอบดังกล่างจะสามารถทำการเบรค VLAN ได้

VLAN & Trunk

VLAN



Trunk Port ใช้สำหรับส่งผ่านทราฟฟิกของ VLAN เช่น การเชื่อมต่อสวิตซ์ดังรูปจะทำให้เครื่อง Client ถึงจะอยู่คนละสวิตซ์แต่ก็ยังอยู่ใน VLAN เดียวกัน

Trunk

Access Port และ Trunk Port

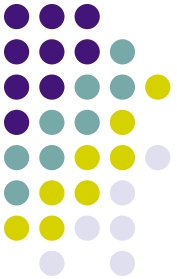
Access Port

- พอร์ตที่เชื่อมต่อระหว่างสวิตซ์ และ Client
- พอร์ตที่เชื่อมต่อระหว่างสวิตซ์ และ Server
- พอร์ตที่เชื่อมต่อระหว่าง สวิตซ์ และ เราเตอร์ (ไม่ใช่เราเตอร์เราท์ทราฟฟิก Inter VLAN)

Trunk Port

- พอร์ตที่ทำหน้าที่เชื่อมต่อไปยังสวิตซ์ตัวอื่นๆ เช่น UPLINK PORT
- พอร์ตที่ทำหน้าที่เชื่อมต่อไปยังเราเตอร์ตัวที่ทำหน้าเราท์ทราฟฟิกระหว่าง VLAN

VLAN & Trunk
Inter-VLAN Routing



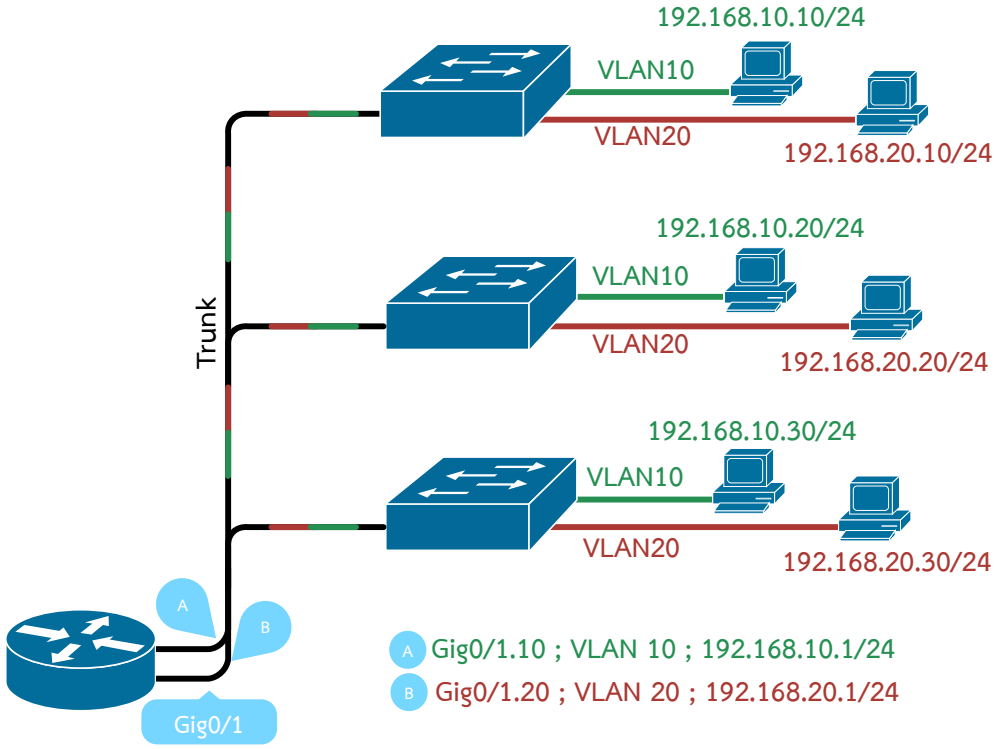
การเราท์ทราฟฟิกระหว่าง VLAN (Inter-VLAN Routing)

ในการเราท์ทราฟฟิกระหว่าง VLAN นั้น เราจำเป็นที่จะต้องมีอุปกรณ์ในเลเยอร์ 3 เช่น เราเตอร์หรือสวิตซ์เลเยอร์ 3 เข้ามาช่วยในการเราท์ทราฟฟิกที่อยู่ต่าง VLAN

หากใช้ Router ต้องมีพอร์ตอย่างน้อย 1 พอร์ต (ทำ Sub Interface)

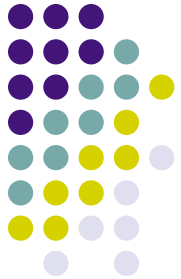
VLAN & Trunk

Inter-VLAN Routing



หากใช้ Router ต้องมีพอร์ตอย่างน้อย 1 พอร์ต (ทำ Sub Interface) จากรูป Router มี 1 Physical Interface Gig0/1 แล้วทำการสร้าง Sub Interface Gig0/1.10, Gig0/1.20 เพื่อทำหน้าที่เป็น Gateway ให้กับ Network ของ VLAN10 และ VLAN20 ตามลำดับ

Resources



- เอกสิทธิ์ วิริยจารี. เรียนรู้ระบบเน็ตเวิร์กจากอุปกรณ์ของ Cisco ภาคปฏิบัติ. พิมพ์ครั้งที่ 5. กรุงเทพฯ: ซีเอ็ดยูเคชั่น, 2549.
- จักกริช พฤษการ. การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์. กรุงเทพฯ: ท้อป. 2549.