**VLAN คืออะไร**

VLAN ย่อมาจาก Virtual LAN เป็นเทคโนโลยีที่ใช้ในการจำลองสร้างเครือข่าย LAN แต่ไม่ขึ้นอยู่กับการต่อทางกายภาพเช่น สวิตช์หนึ่งตัวสามารถใช้จำลองเครือข่าย LAN ได้ห้าเครือข่าย หรือสามารถใช้สวิตช์สามตัวจำลองเครือข่าย LAN เพียงหนึ่งเครือข่าย เป็นต้น

ในการสร้าง VLAN โดยใช้อุปกรณ์เครือข่ายหลายตัว จะมีพอร์ตที่ทำหน้าที่เชื่อมต่อระหว่างอุปกรณ์เครือข่ายแต่ละตัว เรียก Trunk port ซึ่งเสมือนมีท่อเชื่อม หรือ Trunk เป็นตัวเชื่อมด้วย

เนื่องจาก VLAN เป็น LAN แบบจำลอง ถึงแม้ว่าจะต่อทางกายภาพอยู่บนอุปกรณ์เครือข่ายตัวเดียวกัน แต่การติดต่อกันนั้นจำเป็นต้องใช้อุปกรณ์ที่มีความสามารถในการค้นหาเส้นทาง เช่น เราเตอร์ หรือสวิตช์เลเยอร์สาม

**ลักษณะพิเศษของ VLAN ทั่วๆ ไปคือ**

1. VLAN แต่ละเครือข่ายที่ติดต่อกันนั้น จะมีลักษณะเหมือนกับต่อแยกกันด้วยบริดจ์
2. VLAN สามารถต่อข้ามสวิตช์หลายตัวได้
3. ท่อเชื่อม (Trunks) ต่างๆ จะรองรับทราฟฟิกที่คับคั่งของแต่ละ VLAN ได้

**ชนิดของ 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 ดังรูปที่ 1

|  |  |
| --- | --- |
| Port | VLAN |
| 1 | 1 |
| 2 | 1 |
| 3 | 2 |
| 4 | 1 |

**รูปที่ 1** แสดงการกำหนดพอร์ตให้กับ VLAN

1. Layer 2 VLAN : Membership by MAC Address

ใช้ MAC Address ในการแบ่ง VLAN โดยให้สวิตช์ตรวจหา MAC Address จากแต่ละ VLAN ดูรูปที่ 2

|  |  |
| --- | --- |
| MAC Address | VLAN |
| 1212354145121 | 1 |
| 2389234873743 | 2 |
| 3045834758445 | 2 |
| 5483573475843 | 1 |

**รูปที่ 2** แสดงการกำหนด MAC Address ให้กับ VLAN ต่างๆ

1. Layer 2 VLAN : Membership by Protocol types

แบ่ง VLAN โดยใช้ชนิดของ protocol ที่ปรากฎอยู่ในส่วนของ Layer 2 Header ดูรูปที่ 3

|  |  |
| --- | --- |
| Protocol | VLAN |
| IP | 1 |
| IPX | 2 |

**รูปที่ 3** แสดงการแบ่ง VLAN โดยใช้ชนิดของ protocol กำหนด

1. 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 |

**รูปที่ 4** แสดงการแบ่ง VLAN โดยใช้ IP Subnet

1. Higher Layer VLAN's

VLAN ทำได้โดยใช้โปรแกรมประยุกต์หรือ service แบ่ง VLAN เช่นการใช้โปรแกรม FTP สามารถใช้ได้ใน VLAN 1 เท่านั้น และถ้าจะใช้ Telnet สามารถเรียกใช้ได้ใน VLAN 2 เท่านั้น เป็นต้น

**ทำไมต้องใช้ VLAN**

1. เพิ่มประสิทธิภาพของเครือข่าย

ในระบบเครือข่ายทั่วไปจะมีการส่งข้อมูล Broadcast จำนวนมาก ทำให้เกิด Congestion และ VLAN มีความสามารถช่วยเพิ่มประสิทธิภาพของเครือข่ายได้เนื่องจาก VLAN จะจำกัดให้ส่งข้อมูล Broadcast ไปยังผู้ที่อยู่ใน VLAN เดียวกันเท่านั้น

1. ง่ายต่อการบริหารการใช้งาน

VLAN อำนวยความสะดวกในการบริหารจัดการโครงสร้างของระบบเครือข่ายให้ง่าย มีความยืดหยุ่น และเสียค่าใช้จ่ายน้อย โดยเพียงเปลี่ยนโครงสร้างทาง Logical เท่านั้น ไม่จำเป็นต้องเปลี่ยนโครงสร้างทางกายภาพ กล่าวคือ ถ้าต้องการเปลี่ยนโครงสร้างของ VLAN ก็ทำโดยการคอนฟิกที่อุปกรณ์เครือข่ายใหม่ ไม่จำเป็นเปลี่ยนรูปแบบทางกายภาพของการเชื่อมต่อเครือข่ายที่มีอยู่เดิม

1. เพิ่มการรักษาความปลอดภัยมากขึ้น

เนื่องจากการติดต่อระหว่างอุปกรณ์เครือข่ายจะสามารถทำได้ภายใน VLAN เดียวกันเท่านั้น ถ้าต้องการที่จะติดต่อข้าม VLAN ต้องติดต่อผ่านอุปกรณ์ค้นหาเส้นทางหรือสวิตช์เลเยอร์สาม

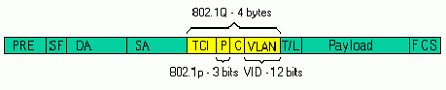
**มาตรฐานของ VLAN คือ 802.1Q**

มาตรฐาน IEEE 802.1Q นั้นเป็นมาตรฐานในการนำข้อมูลของ VLAN membership ใส่เข้าไปใน Ethernet Frame หรือที่เรียกว่า การ Tagging และโปรโตคอล 802.1Q นี้ถูกพัฒนาเพื่อแก้ปัญหาเรื่องการบริหารจัดการด้านเครือข่ายที่เพิ่มขึ้น เช่น การกระจายเครือข่ายใหญ่ๆ ให้เป็นส่วนย่อยๆ (Segment) ทำให้ไม่สูญเสียแบนวิธให้กับการ broadcast และ multicast มากเกินไป และยังเป็นการรักษาความปลอดภัยระหว่างส่วนย่อยต่างๆ ภายในเครือข่ายให้สูงขึ้นอีกด้วย

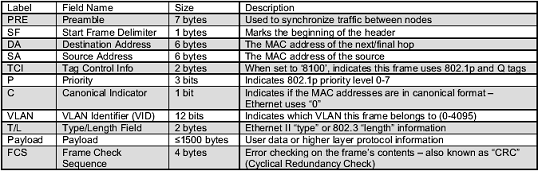
การต่อเติมเฟรม (tagging Frame) ด้วยมาตรฐาน 802.1Q นั้นจะทำในระดับ Data-Link layer และการทำ VLAN Tagging นั้นจะเป็นการเปลี่ยนรูปแบบของ Ethernet Frame มาตรฐาน 802.3 ให้เป็นรูปแบบใหม่ที่เป็นมาตรฐาน 802.3 ac ซึ่งมีไดอะแกรมของเฟรมมาตรฐาน 802.3 ดังรูปที่ 5 และไดอะแกรมของมาตรฐาน 802.3 ac ดังรูปที่ 6 ( ส่วนสีเหลืองแทนส่วนของ tag 802.1Q )

http://thaicert.nectec.or.th/paper/basic/vlan/8023beforetag.gif

**รูปที่ 5** แสดงรูปแบบของเฟรม 802.3 ก่อนที่จะทำ VLAN Tagging



**รูปที่ 6** แสดงรูปแบบของเฟรม 802.3 ที่มีการ tagging 802.1Q แล้ว



**รูปที่ 7** แสดงตารางของคำอธิบายส่วนต่างๆ ของมาตรฐาน 802.3

**ช่องโหว่ของการใช้ VLAN**

โดยปกติแล้วจะไม่สามารถส่งข้อมูลข้าม VLAN ได้ถ้าไม่ใช้ เราเตอร์ สวิตช์เลเยอร์สาม หรือตัวกลางที่ช่วยค้นหาเส้นทางอื่นๆ แต่มีช่องโหว่ที่ทำให้ผู้ใช้สามารถส่งข้อมูลข้าม VLAN ได้โดยไม่ต้องอาศัยตัวกลาง เรียกว่า " การเบรค VLAN " ซึ่งช่องโหว่นี้เกิดจาก Trunking protocol ของสวิตช์บางรุ่น และวิธีการทดสอบคือทำการส่งข้อมูลตัวอย่างจาก VLAN หนึ่งไปยัง VLAN อื่น ที่อยู่บนสวิตช์คนละตัว และข้อมูลที่ส่งนั้นให้ทำการสร้าง ethernet Frame ที่มี Tag 802.1Q และเปลี่ยนค่าของหมายเลข VLAN ให้เป็นค่าของหมายเลข VLAN ปลายทางที่ต้องการเบรค เฟรมที่ถูกสร้างขึ้นใหม่นั้นจะมีลักษณะดังรูปที่ 6 และค่าของ Tag 802.1Q จะมีรูปแบบ "81 00 0n nn" โดยที่ nnn คือหมายเลขของ VLAN ซึ่งผลจากการทดสอบดังกล่างจะสามารถทำการเบรค VLAN ได้

**สถานการณ์ต่อไปนี้จะทำให้เกิดช่องโหว่ของ VLAN**

* 1. เมื่อผู้บุกรุกสามารถที่จะเข้าถึงพอร์ตในสวิตช์ที่เป็น VLAN เดียวกันกับ VLAN ของ Trunk port
  2. เครื่องเป้าหมายอยู่บนสวิตช์ต่างกันแต่มีกลุ่ม trunk เดียวกัน
  3. ผู้บุกรุกทราบถึง MAC address ของเครื่องเป้าหมาย
  4. Layer 3 device สามารถสร้าง Connection จาก VLAN เป้าหมายกลับไปยัง VLAN ที่เป็นต้นทางได้

**สรุป**

เนื่องจากช่องโหว่ที่พบนั้นเป็นช่องโหว่ที่อาจจะไม่สามารถจะป้องกันได้เพราะเป็นช่องโหว่ที่เกิดจากทางผู้พัฒนามาตรฐานและผู้ผลิตอุปกรณ์เครือข่าย ฉะนั้นขอแนะนำว่า ไม่ควรใช้ VLAN เพื่อจุดประสงค์ในการรักษาความปลอดภัยของข้อมูลที่ส่งผ่าน เพียงแต่คุณสมบัติที่ดีของ VLAN นั้นก็ทำให้เป็นทางเลือกอีกทางที่น่าใช้ คุณสมบัติดังกล่าวเช่นสามารถทำการแบ่งเครือข่ายง่าย ลดการ broadcast และ ลดความคับคั่ง ( Collision ) เป็นต้น  
แต่ถ้าจำเป็นต้องใช้ VLAN นั้นให้พยายามเลี่ยงการใช้สวิตช์หลายตัว หรือกล่าวอีกนัยหนึ่งคือไม่ควรที่จะใช้ Trunk port