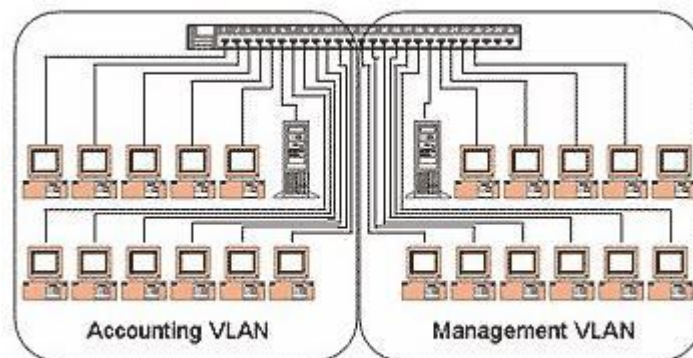


การ Configuration VLAN on switch Cisco เบื้องต้น ตอนที่ 1

VLAN คืออะไร

VLAN (Virtual Area Network) เป็นการจัดแยกการเชื่อมต่อเครือข่ายในรูปแบบที่เรียกว่า Domain ซึ่งจุดประสงค์ของการแยกออกเป็น Domain นี้ ก็เพื่อให้เครื่องคอมพิวเตอร์ที่อยู่ต่าง Domain ไม่สามารถสื่อสารกัน ได้ทั้งนี้เพื่อความปลอดภัยของเครือข่าย รวมทั้งสามารถเพิ่มประสิทธิภาพการทำงานของเครือข่ายอีกด้วย ในหนึ่งเครือข่ายอาจประกอบด้วย Switching Hub หลาย ๆ ตัว และใน Switching Hub หนึ่งตัวอาจประกอบด้วย VLAN หลาย ๆ Domain หรือหลาย VLAN ก็เป็นได้ การแบ่ง VLAN จะทำให้เครื่องคอมพิวเตอร์แม้จะเชื่อมต่อกันใน Switches Hub เดียวกัน แต่อยู่ต่าง VLAN กัน ไม่สามารถสื่อสารกันได้ รวมทั้งไม่สามารถมองเห็นกันได้ด้วยซ้ำไป (รูปที่ 1) และที่แน่นอน หนึ่ง VLAN สามารถกระจายไปตาม Switches Hub ต่าง ๆ ได้ เช่นกัน ภายใต้ Switches Hub ของ Cisco 1 ตัว สามารถติดตั้ง VLAN ได้มากถึง 64 VLAN และทั้งระบบสามารถมี VLAN ได้มากถึง 1024 VLAN



รูปที่ 1 แสดงการแบ่ง VLAN ออกเป็น 2 ชุด ภายใน Switches เดียว

ประโยชน์ที่จะได้รับจากการทำ VLAN

- จำกัดการแพร่กระจายของ Broadcast traffic ไม่ให้ส่งผลกระทบต่อประสิทธิภาพโดยรวมของ Network หรือเรียกว่า 1 VLAN คือ 1 Broadcast Domain นั่นเอง
- สามารถสร้างกลไกด้านความปลอดภัยได้ง่ายขึ้น เช่น การสร้าง Access Control List บนอุปกรณ์ Layer 3 และลดความเสี่ยงเกี่ยวกับการดักจับข้อมูล (Sniffing)
- ผู้ใช้สามารถที่จะเคลื่อนย้ายไปยัง VLAN (Subnet) อื่น ๆ ได้โดยเพียงแค่การเปลี่ยน config ของ switch และ IP Address ของ Client เพียงนิดเดียว ไม่จำเป็นต้องมีการย้าย switch หรือ สายใด ๆ
- สามารถรองรับการขยายตัวของระบบ Network ที่จะเพิ่มขึ้นในอนาคตได้ง่าย เนื่องจากการวางแผนเกี่ยวกับการทำ subnet และการ design ระบบที่ไม่ยึดติดกับทางกายภาพอีกต่อไป

- สามารถวิเคราะห์ปัญหาที่เกิดขึ้นในระบบได้ง่ายขึ้น เช่น ในระบบมีการแบ่ง VLAN ไว้ 3 แพลก ได้แก่ sale , engineer และ server วันหนึ่ง user ของ sale โทรมาแจ้งปัญหาเกี่ยวกับ admin ว่าเล่น Internet ไม่ได้ เราเป็น Admin ควรจะถาม user กลับไปว่าคนอื่นในแพลกเป็นด้วยหรือไม่ ถ้าไม่ก็แสดงว่าเป็นที่เครื่องของ user คนนั้นคนเดียว แต่ถ้าหากเป็นทั้งแพลก ก็ต้องโทรเช็คกับแพลก engineer ด้วยว่าเป็นเหมือนกันหรือไม่ ถ้าไม่เป็น แสดงว่าเป็นที่แพลก sale แพลกเดียว ดังนั้นก็ทำการตรวจเช็คปัญหาที่แพลก sale อย่างเดียว เห็นมั๊ยคะ การวิเคราะห์ปัญหาที่ง่ายขึ้นมากและการขอบเขตในการวิเคราะห์ปัญหาก็แคบลง ที่สำคัญตอนการแก้ปัญหาที่ควรนำหลักการ OSI Layer เข้ามาช่วยนะคะ จะทำให้หาสาเหตุได้เร็วขึ้นคะ

ในการสร้าง VLAN นั้น port ของ switch นั้นจะทำหน้าที่อยู่ 2 ประเภท คือ Access port และ Trunk port ซึ่งจะมีหน้าที่ในการทำงานต่าง ๆ กันไปตามที่ System Administrator จะเป็นคนกำหนดไว้ ซึ่งหน้าที่หลัก ๆ ของทั้งสองแบบนี้คือ

Access Port

เป็น Port ที่ทำหน้าที่เชื่อมต่อระหว่าง switch จาก Client ไปยัง switch ซึ่งเราจะใช้สาย Lan แบบสายตรง (Straight Through) ในการเชื่อมต่อ และ port ที่ถูก set เป็น Access Port นี้จะมี traffic ของ VLAN เพียง VLAN เดียวที่วิ่งผ่านออกมาถึง port นี้ หรือ port นี้จะต่อกับอุปกรณ์ที่มีค่า mac address เพียงค่าเดียวนั่นเอง เช่น

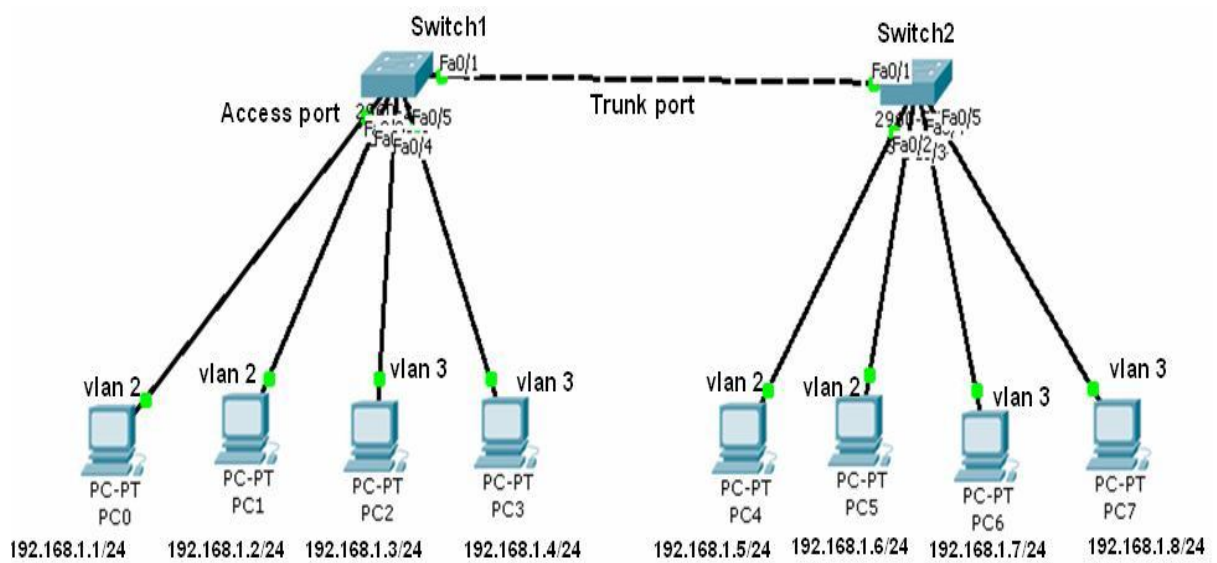
- port ที่ set ระหว่าง switch และ Client
- port ที่ set ระหว่าง switch และ Server
- port ที่ set ระหว่าง switch และ Router (มีชื่อแม้ว่า Router ที่เชื่อมต่อนั้น จะต้องไม่ใช่ Router ที่ทำหน้าที่ในการ Route Traffic ของ Inter VLAN)

Trunk Port

เป็น port ที่ทำหน้าที่ connect switch ตัวอื่น ๆ ที่ต้องการให้เป็นสมาชิกของ VLAN ต่าง ๆ กันมาอยู่ด้วยกัน และทำหน้าที่ส่งผ่าน traffic ของหลาย ๆ VLAN ให้กระจายไปยัง switch ตัวอื่น ๆ ที่มี port ที่ถูกกำหนดให้เป็น VLAN เดียวกันกับ switch ตัวต้นทางได้ หรือ ที่เรียกกันโดยทั่วไปว่า Uplink Port หรือง่าย ๆ ว่า Trunk port เป็น port ที่มีค่าหลายๆ ค่าวิ่งผ่าน เช่น VLAN หลายๆ VLAN หรือมีค่า Mac address หลายๆ ค่าวิ่งผ่าน นั่นเอง ตัวอย่างในการ set port ให้เป็น Trunk port ก็คือ

- port ที่ทำหน้าที่ connect ไปยัง switch ตัวอื่น ๆ เช่น Uplink Port
- port ที่ทำหน้าที่เชื่อม ไปยัง Router ตัวที่ทำหน้าที่ Route Traffic ระหว่าง VLAN

ผังรูป



ตัวอย่างการ Configuration บน Switch Cisco

Step

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
```

จากนั้นทำการกำหนด 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
Switch1 (config-if)#switchport trunk encapsulation dot1q
```

หมายเหตุ ค่า encapsulation ของ mode trunk มี 2 ประเภท คือ dot1q และ isl โดยส่วนใหญ่แล้วมักจะใช้เป็นค่ามาตรฐาน ที่ทุกๆ product สามารถรองรับได้คือ dot1q (IEEE802.1q) ส่วนค่า encapsulation แบบ ISL เป็นค่าเฉพาะของ product CISCO เท่านั้น

ในส่วนของการ config VLAN ที่ switch 2 รูปแบบ config เหมือนกันเลยคะ (เนื่องจากว่าต่อ diagram เหมือนกัน)

เพิ่มเติม เราสามารถ manage port หลาย port พร้อมกันได้ด้วย range นะคะ เช่น

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

หรือถ้า port ที่ set ไม่เรียงต่อกันก็ใช้ (,) ช่วยได้คะ เช่น

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

Switch 2

```
Switch2> enable
Switch2# configure terminal
Switch2(config)# vlan 2
Switch2(config-vlan)# name Admin
Switch2(config-vlan)# vlan 3
Switch2(config-vlan)# name User
```

จากนั้นทำการกำหนด interface ให้กับแต่ละ VLAN

```
Switch2> enable
Switch2# configure terminal
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
```

```
Switch2 (config)# interface range fa0/4 - 5
Switch2 (config-if-range)# switchport mode access
Switch2 (config-if-range)# switchport access vlan 3
Switch2 (config-if-range)# no shutdown
```

```
Switch2 (config)# interface fa0/1
Switch2 (config-if)# switchport mode trunk
Switch2 (config-if)#switchport trunk encapsulation dot1q
```

หมายเหตุ

เราสามารถดูสถานะของ interface และ VLAN ได้ด้วยคำสั่ง show vlan หรือ show vlan brief ที่ privilege mode ได้

จากนั้นลอง test ping ดูจะเห็นว่า จะ ping เฉพาะ VLAN ตัวเองเท่านั้น

เรียบเรียงโดย พัชรินทร์ ด้วงสิงคำ
[http:// www.jodoi.com](http://www.jodoi.com)