แผนบริหารการสอนประจำบท
บทที่ 6 การอิมพลีเมนต์ VLAN ในเน็ตเวิร์ก

วัตถุประสงค์

1. อธิบายประโยชน์ของ VLAN ได้
2. บอกถึงกระบวนการทำงานของ VLAN ได้
3. นำ VLAN ไปประยุกต์ใช้กับเครือข่ายจริงได้

เนื้อหา

1. ความหมายของ VLAN (Virtual LAN)
2. ความสัมพันธ์ระหว่าง VLAN กับโพรโทคอล TCP/IP
3. ความสัมพันธ์ระหว่าง VLAN กันมุมมองของเครื่องคอมพิวเตอร์ที่ผู้ใช้ใช้งานอยู่
4. ประโยชน์ที่ได้รับจากการสร้างและแบ่ง VLAN
5. การสร้าง VLAN และการเข้าเป็นสมาชิกของ VLAN
6. ความหมายของ Access Port และ Trunk Port
7. โพรโทคอลที่ช่วยให้ง่ายต่อการอิมพลีเมนต์ VLAN ในสวิตช์เน็ตเวิร์ก

กิจกรรมการเรียนการสอน

1. ผู้สอนอธิบายวัตถุประสงค์ ความคิดรวบยอด ขอบเขตเนื้อหา วิธีการเรียน และกิจกรรมการเรียนการสอนประจำบทเรียน
2. ผู้สอนใช้สไลน์และเอกสารประกอบการสอนในรูปแบบไฟล์อิเล็กทรอนิกส์ประเภท PPT ประกอบการบรรยายเนื้อหาประเด็นสำคัญ
3. ผู้สอนบรรยายสรุปเนื้อหาและประเด็นสำคัญประจำบทเรียน
4. ผู้เรียนทำแบบฝึกหัด เพื่อเป็นการทำทวนความรู้ความเข้าใจเนื้อหาประจำบท และประเมินผลเป็นคะแนนระหว่างเรียน
5. ผู้เรียนทำงานตามที่ได้รับมอบหมายประจำบทเรียน โดยให้ผู้เรียนส่งงานในรูปแบบต่าง ๆ ตามที่ผู้สอนกำหนด

สื่อการเรียนการสอน

1. เอกสารประกอบการสอน รายวิชาความรู้เบื้องต้นเกี่ยวกับเครือข่ายคอมพิวเตอร์ ซึ่งเรียบเรียงโดยอาจารย์สุลัยมาน เภอโส๊ะ สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์เทคโนโลยีและการเกษตร
2. สไลน์ประกอบการสอน รายวิชาความรู้เบื้องต้นเกี่ยวกับเครือข่ายคอมพิวเตอร์ ซึ่งเผยแพร่ไว้บนเว็บไซต์อีเลิร์นนิ่งของมหาวิทยาลัยราชภัฏยะลา โดยมีที่อยู่ของเว็บไซต์ คือ http://elearning.yru.ac.th

การวัดผลและการประเมินผบ

1. วัดและประเมินผลจากคะแนนแบบฝึกหัด และให้คะแนนตามเกณฑ์ที่กำหนดไว้ล่วงหน้า แล้วบันทึกเป็นคะแนนระหว่างเรียนของผู้เรียนแต่ละคน
2. ประเมินผลงานหรือการบ้านที่ผู้สอนมอบหมายให้ผู้เรียนปฏิบัติประจำบทเรียน และให้คะแนนตามเกณฑ์ที่กำหนดไว้ล่วงหน้า แล้วบันทึกเป็นคะแนนระหว่างเรียนของผู้เรียนแต่ละคน

บทที่ 6
การอิมพลีเมนต์ VLAN ในเน็ตเวิร์ก

VLAN เป็นความสามารถอีกขั้นหนึ่งของอุปกรณ์สวิตช์ที่ได้รับการนำไปอีมพลีเมนต์ในเน็ตเวิร์กส่วนใหญ่ มันทำให้การวางแผนออกแบบเน็ตเวิร์กที่ใช้สวิตช์มีประสิทธิภาพมากขึ้น ในบทนี้จะกล่าวถึงความหมายของ VLAN ความสัมพันธ์ระหว่าง VLAN กับโพรโทรคอล TCP/IP และประโยชน์ที่ได้รับจากการทำ VLAN

6.1 ความหมายของ VLAN (Virtual LAN)

VLAN (Virtual LAN) เป็นความสามารถอีกขั้นหนึ่งของอุปกรณ์สวิตช์ที่ได้รับการนำไปอีมพลีเมนต์ในเน็ตเวิร์กส่วนใหญ่ มันทำให้การวางแผนออกแบบเน็ตเวิร์กที่ใช้สวิตช์มีประสิทธิภาพมากขึ้นหากจะหานิยามสั้นๆ แบบง่ายๆ สักนิยามหนึ่งที่อธิบายความหมายว่า VLAN คืออะไร เราสามารถอธิบายได้ว่า VLAN นั้นเป็นความสามารถในการกำหนดขอบเขตของบรอดคาสต์โดเมน (broadcast domain) ขึ้นมาใหม่ในเน็ตเวิร์กที่ใช้อุปกรณ์สวิตช์เลเยอร์ 2

คำว่า บอรดคาสต์โดเมน นั้นหมายถึง ขอบเขตของการรับและส่งบรอดคาสต์เฟรม (broadcast frame เป็นเฟรมที่มีแอดเดรสปลายทางเป็นบรอดคาสต์แอดเดรส มีจุดประสงค์เพื่อให้ทุกๆ เครื่องได้รับเฟรมนั้นไปประมวลผล) หากเครื่อง A และ B อยู่ในบรอคสต์โดเมนเดียวกัน เครื่อง B จะได้รับบรอดคาสต์เฟรมจากเครื่อง A และในทางกลับกันด้วย จากเนื้อหาในบทที่ 12 เราได้ทราบไปแล้วว่า โดยดีฟอลต์เมื่อสวิตช์ได้รับบรอดคาสต์เฟรมมาจากพอร์ตใดพอร์ตหนึ่งของฉัน มันจะกระจายบรอดคาสต์เฟรมออกไปทุกๆ พอร์ต แต่เมื่อมีการกำหนด VLAN ขึ้นมาแล้ว บรอดคาสต์เฟรมจะถูกส่งออกไปเฉพาะพอร์ตที่เป็นสมาชิกใน VLAN เดียวกันเท่านั้น ไม่ข้ามไปยังพอร์ตที่เป็นสมาชิกของ VLAN อื่น

กล่าวอีกนัยหนึ่งได้ในทางปฏิบัติว่า VLAN นั้นเสมือนเป็นการแบ่งกลุ่มของเครื่องคอมพิวเตอร์ปลายทางออกเป็นกลุ่มย่อย ๆ ราวกับว่ามันอยู่ LAN เดียวกัน และสื่อสารกันได้เฉพาะเครื่องในกลุ่มของตนที่อยู่ภายใน VLAN เดียวกันเท่านั้น โดยปราศจากข้อจำกัดเชิงกายภาพ คำว่าปราศจากข้อจำกัดเชิงกายภาพก็คือ เครื่องคอมพิวเตอร์ที่อยู่ใน VLAN เดียวกันนั้นสามารถเชื่อมต่ออยู่กับพอร์ตของสวิตช์ตัวเดียวกัน หรือจะเชื่อมต่ออยู่กับพอร์ตบนสวิตช์ตัวเดียวกัน หรือจะเชื่อมต่ออยู่กับพอร์ตบนสวิตช์บนสวิตช์คนละตัวกันก็ได้

อย่างไรก็ดีโดยดีฟอลต์หลังจากกำหนด VLAN ขึ้นมาแล้ว เฉพาะเครื่องคอมพิวเตอร์ที่อยู่ใน VLAN เดียวกันเท่านั้นที่จะสามารถติดต่อสื่อสารกันได้ โดยดีฟอลต์ เครื่องคอมพิวเตอร์ที่อยู่ต่างๆ VLAN กันจะไม่สามารถติดต่อสื่อสารกันได้ วิธีการที่จะทำให้เครื่องคอมพิวเตอร์ที่อยู่ต่าง VLAN กันจะสามารถสื่อสารกันได้ก็คือ การใช้อุปกรณ์ในเลเยอร์ที่ 3 ได้แก่เราเตอร์จริงที่ต่อภายนอก (external router) หรือสวิตช์เลเยอร์ที่ 3 (layer 3 switch) เข้ามาทำการเร้าต์ (route) ทราฟฟิกระหว่าง VLAN

6.2 ความสัมพันธ์ระหว่าง VLAN กับโพรโทคอล TCP/IP

หากมองจากมุมของเลเยอร์ 2 การแบ่ง VLAN เป็นการแบ่งกลุ่มของเครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่กับพอร์ตของสวิตช์ให้เสมือนว่าอยู่ใน LAN เดียวกันโดยไม่เกี่ยวข้องกับ VLAN อื่นๆ และเฉพาะเครื่องในกลุ่มดังกล่าวเท่านั้นที่สามารถสื่อสารกันได้ และบรอดคาสต์ทราฟฟิกจะถูกจำกัดให้อยู่เฉพาะใน VLAN นั้น ๆ เท่านั้นไม่กระจายไปยังพอร์ตของสวิตช์ที่อยู่ใน VLAN อื่น

เมื่อมองจากแง่มุมของเลเยอร์ที่ 3 ซึ่งเป็นเลเยอร์ของโพรโทคอล IP นั้น สิ่งที่เราสนใจก็คือ การวางแผนหมายเลขซับเน็ตแอดเดรส และการเซตหมายเลข IP Address ให้กับเครื่องคอมพิวเตอร์ของผู้ใช้ เนื่องจากซับเน็ตหนึ่งซับเน็ตในโลกของ IP เป็นการกำหนดขอบเขตของบรอดคาสต์โดเมนขึ้นมา ในขณะเดียวกัน VLAN หนึ่ง VLAN ก็เป็นการกำหนดขอบเขตของบรอดคาสต์โดเมนขึ้นมาเช่นเดียวกัน ดังนั้น จึงส่งผลให้กับซับเน็ต 1 ซับเน็ตมีความสอดคล้องกับ VLAN 1 VLAN นี่จึงเป็นที่มาของหลักการในทางปฏิบัติว่า “หมายเลขซับเน็ตแอดเดรสของโพรโทคอล IP บนเครื่องคอมพิวเตอร์ที่อยู่ใน VLAN หนึ่ง ๆ จะต้องเป็นค่าเฉพาะตัว (unique) ที่ไม่ซ้ำกันออกแบบและวางแผนแอดเดรสบนเครื่องคอมพิวเตอร์ที่อยู่ใน VLAN อื่น” กล่าวสรุปได้อีกแบบหนึ่งว่า ในออกแบบและวางแผนแอดเดรสให้กับเน็ตเวิร์กที่ใช้ VLAN นั้น เราจะต้องออกแบบให้ VLAN ได้รับการจัดสรร 1 ซับเน็ตแอดเดรสเฉพาะตัวไป ถ้ามีอยู่ 10 VLAN ซับเน็ตแอดเดรสที่ต้องจัดสรรให้ก็ควรจะเท่ากับ 10 ซับเน็ตแอดเดรส (1 VLAN ต่อ 1 ซับเน็ตแอดเดรส)

ซิสโก้แนะนำหลักการปฏิบัติที่ดีกว่า ภายใน 1 VLAN ควรประกอบด้วยเฉพาะ 1 ซับเน็ตแอดเดรสเท่านั้น แต่ในการใช้งานจริงบางครั้ง ก็เป็นไปได้เหมือนกันที่ภายใน 1 VLAN จะได้รับการจัดสรรให้มีซับเน็ตแอดเดรสมากกว่า 1 ซับเน็ตแอดเดรส ตัวอย่างเช่น ในครั้งแรกของการอิมพลีเมนต์เน็ตเวิร์ก เราออกแบบให้ 1 VLAN ใช้งานซับเน็ตแอดเดรสในคลาส C ดังที่ได้ทราบไปแล้วว่าแอดเดรสในคลาส C นั้นสามารถรองรับการกำหนดหมายเลข IP Address ได้สูงสุดเท่ากับ 254 IP Address แต่บังเอิญในอนาคต

มีความจำเป็นต้องเพิ่มขยายเครื่องคอมพิวเตอร์ใหม่เข้าไปใน VLAN เดิมได้ กลายเป็น 1 VLAN ประกอบด้วยซับเน็ตแอดเดรสมากกว่า 1 ซับเน็ตแอดเดรส สำหรับกรณีเช่นนี้ ถึงแม้เครื่องจะได้รับการกำหนดซับเนตแอดเดรสต่างกัน แต่บรอดคาสต์เฟรมก็ยังมีโอกาสที่จะถูกส่งไปยังเครื่องที่อยู่ต่างซับเน็ตกันได้ ทั้งนี้เพราะเครื่องทั้งหมดเป็นสมาชิกของ VLAN เดียวกัน กล่าวอีกอย่างคือ ถึงแม้จะแบ่งแยกเป็นซับเน็ตใหม่ได้ก็จริง แต่บรอดคาสต์ทราฟฟิกจากซับเน็ตหนึ่งก็สามารถถูกแพร่กระจายไปถึงอีกซับเน็ตหนึ่งไป ทั้งนี้เพราะซับเน็ตทั้งสองอาศัยอยู่ภายใต้ VLAN เดียวกัน

6.3 ความสัมพันธ์ระหว่าง VLAN กันมุมมองของเครื่องคอมพิวเตอร์ที่ผู้ใช้ใช้งานอยู่

จะได้เห็นในอนาคตว่า ขั้นตอนหนึ่งที่อยู่ในกระบวนการอิมพลีเมนต์ VLAN ก็คือ การแมปพอร์ตบนสวิตช์เข้ากับหมายเลข VLAN ลักษณะนี้เรียกว่า การกำหนดว่าพอร์ตนั้นเป็นสมาชิกของ VLAN ใด การกระทำดังกล่าวจะส่งผลให้เครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่กับพอร์ตนั้นเป็นสมาชิกของ VLAN นั้นๆ ไปด้วยโดยปริยายโดยที่จะไม่มีการเซตคอนฟิกูเรชันใดๆ เลยเกี่ยวกับหมายเลข VLAN เกิดขึ้นบนเครื่องคอมพิวเตอร์ปลายทางของผู้ใช้ สิ่งที่ต้องถูกเซตลงไปให้เหมาะสมบนเครื่องของผู้ใช้ก็แค่เพียง พารามิเตอร์ของ TCP/IP อย่างเช่นหมายเลข IP Address ที่คำนวณมาจากซับเน็ตแอดเดรสที่ได้รับการจัดสรรให้เป็นซับเน็ตแอดเดรสประจำ VLAN นั้น ๆ เท่านั้น (รวมทั้ง Subnet Mask และ Default Gateway ที่เหมาะสม)

6.4 ประโยชน์ที่ได้รับจากการสร้างและแบ่ง VLAN

จำกัดขอบเขตการแพร่กระจายของบรอดคาสต์ทราฟฟิกไม่ให้ส่งผลกระทบต่อประสิทธิภาพโดยรวมของเน็ตเวิร์ก โดยปกติ หลายๆ แอปพลิเคชันบนเน็ตเวิร์ก รวมทั้งไดรเวอร์ของดปรโตคอลต่าง ๆ เช่น ไดรเวอร์ของ TCP/IP, IPX/SPX มักจะมีการส่งบรอดคาสต์เฟรมออกมาเป็นระยะๆ เพื่อประโยชน์ต่าง ๆ อันเอื้ออำนวยต่อการปฏิบัติงานของมัน ถึงแม้บรอดคาสต์ทราฟฟิกจะมีประโยชน์ แต่ในเวลาเดียวกัน มันจะก็ส่งผลกระทบต่อประสิทธิภาพโดยรวมได้ หากไม่มีการจำกัดขอบเขตของบรอดคาสต์ทราฟฟิก

ทำไมบรอดคาสต์ทราฟฟิกจึงมีผลต่อประสิทธิภาพของเน็ตเวิร์ก?

1) เพราะบรอดคาสต์เฟรมเป็นเฟรมพิเศษที่ “บังคับ” ให้ทุก ๆ เครื่องในบรอดคาสต์โดเมนนั้น ๆ ต้องรับเอาบรอดคาสต์เฟรมไปใส่ไว้ในบัเฟอร์ของเน็ตเวิร์กการ์ดของตน และทำการประมวลผลบรอดคาสต์เฟรมด้วยการส่งสัญญาณไปอินเตอร์รัปต์ซีพียูของเครื่องและให้ไดรเวอร์ของโพรโทคอลในเลเยอร์ 3 เป็นผู้ประมวลผลต่อไม่ว่าตนเองจะมีหรือไม่มีส่วนเกี่ยวข้องใด ๆ กับเนื้อหาภายในเฟรมนั้น ๆ ก็ตาม ภายหลังหากพบว่าตนเองจำเป็นต้องมีส่วนร่วมกับเนื้อหาภายในบรอดคาสต์เฟรมนั้น ๆ มันก็จะส่งแพ็กเก็ตออกมาและส่งต่อให้ไดรเวอร์ของโพรโทคอลในเลเยอร์ที่สูงกว่าต่อไป (ตามหลักการ De-encapsulate ของ OSI Model) แต่หากพบว่าตนเองไม่มีส่วนเกี่ยวข้องใด ๆ เลยกับเฟรมดังกล่าว มันก็จะโยนทิ้ง (discard) บรอดคาสต์เฟรมนั้น ๆ ทิ้งไป ปัญหาที่เราสนใจที่นี้คือ หากมันต้องคอยรับบรอดคาสต์เฟรมอยู่เป็นระยะ ๆ ตลอดเวลา ซีพียูของเครื่องคอมพิวเตอร์ก็จะต้องถูกอินเตอร์รัปต์อยู่ตลอดเวลาให้ทำการประมวลผลบรอดคาสต์เฟรม และแม้จะเป็นเน็ตเวิร์กการ์ดสมัยใหม่ที่มีส่วนประมวลผลในตัวหรือมีซีพียูความเร็วสูงก็ตาม มันก็จะต้องเสียเวลาและเพิ่มโหลดโดยไม่จำเป็น

2) เพราะบรอดคาสต์เป็นเฟรมพิเศษที่เมื่อสวิตช์ได้รับเฟรมดังกล่าวแล้ว มันจำเป็นต้องส่งผ่าน (forward) บรอดคาสต์เฟรมออกไปที่ทุก ๆ พอร์ต เพื่อให้ทุก ๆ เครื่องที่ต่ออยู่สวิตช์ได้รับบรอดคาสต์เฟรม นี่เท่ากับเป็นการส่งเฟรมออกไปแย่งใช้งานแบนด์วิดธ์ (bandwidth) ของพอร์ตอื่น ๆ การแบ่ง VLAN เท่ากับเป็นการจำกัดปริมาณพอร์ตที่บรอดคาสต์ทราฟฟิกต้องถูกส่งออกไปให้น้อยลง

สามารถสร้างกลไกด้านความปลอดภัยได้ง่ายขึ้น เช่น การสร้าง ACL บนอุปกรณ์ในเลเยอร์ 3 และการลดความเสี่ยงเกี่ยวกับการดักจับทราฟฟิก

ทำไมการแบ่ง VLAN จึงช่วยเพิ่มความปลอดภัย?

1) ดังที่ได้กล่าวไปในตอนต้น (หัวข้อ “ความสัมพันธ์ระหว่าง VLAN กับโพรโทคอล TCP/IP”) แล้วว่า การแบ่งแยก VLAN เท่ากับเป็นการแบ่งแยกซับเน็ตแอดเดรสของเครื่องคอมพิวเตอร์ และเครื่องคอมพิวเตอร์ใน VLAN หนึ่งๆ จำเป็นต้องส่งแพ็กเก็ตไปยังอุปกรณ์ในเลเยอร์ที่ 3 อย่างเช่น เราเตอร์หรือสวิตช์เลเยอร์ 3 ก่อน เพื่อให้อุปกรณ์ดังกล่าวช่วยส่งผ่านแพ็กเก็ตไปให้ถึงเครื่องคอมพิวเตอร์ใน VLAN ปลายทาง ในจังหวะที่แพ็กเก็ตกำลังถูกเร้าต์ (route) อยู่บนอุปกรณ์ดังกล่าว เราสามารถ Access Control List (ACL) บนเราเตอร์เพื่อตรวจเช็กเงื่อนไขต่าง ๆ ของแพ็กเก็ตและทราฟฟิกต่าง ๆ ได้ก่อนที่จะยิมยอมให้ส่งผ่านออกไปยัง VLAN ปลายยทาง

2) โดยปกติทราฟฟิกที่อยู่ใน VLAN เดียวกันมีโอกาสถูกดักจับได้ด้วยเทคนิคการ “Spoofing” ต่างๆ การแบ่งแยกเน็ตเวิร์กออกมาเป็น VLAN ใหม่จะช่วยลดความเสี่ยงการโจมตีด้วยเทคนิค “spoofing”

ตัวอย่างหนึ่งของการแบ่ง VLAN เพื่อเพิ่มความปลอดภัยได้แก่ การแบ่งแยกกลุ่มของเซิร์ฟเวอร์ออกไปอยู่ใน VLAN ต่างหากเฉพาะ เพื่อที่จะได้สามารถประยุกต์ใช้ ACL บนสวิตช์เลเยอร์ 3 เพื่ออนุญาตหรือปฏิเสธการเข้าถึงเซิร์ฟเวอร์จากเครื่องคอมพิวเตอร์บางเครื่องหรือจากบาง VLAN ได้ หรือเพื่อควบคุมประเภทของทราฟฟิกที่สามารถรับส่งกับเซิร์ฟเวอร์ได้ ถ้าหากนำไม่แบ่ง VLAN ให้กับกลุ่มของเซิร์ฟเวอร์ เราจะไม่มีทางในการใช้ ACL เพื่อทำงานดังกล่าวได้ เพราะเซิร์ฟเวอร์กับไคลเอนต์จะอยู่ในซับเน็ตเวิร์กเดียวกัน และสามารถสื่อสารกันได้โดยตรงโดยไม่ผ่านสวิตช์เลเยอร์ 3

ผู้ใช้สามารถเคลื่อนย้ายไป VLAN (หรือ Subnet) อื่น ๆ ได้โดยเพียงแค่เปลี่ยนคอนฟิกูเรชันของสวิตช์และบนโพรโทคอล TCP/IP บนเครื่องเพียงนิดเดียว โดยไม่ต้องมีการย้ายสายเคเบิลใด ๆ เลย

ระบบสามารถรองรับการขยายตัวในอนาคตได้โดยง่าย บางท่าน เมื่อเริ่มต้นออกแบบและติดตั้งเน็ตเวิร์กก็เซตให้ทั้งหมดอยู่ภายใต้ VLAN เดียวกันไป ครั้นต่อๆ มาเครื่องคอมพิวเตอร์เพิ่มปริมาณมากขึ้นเรื่อย ๆ ส่งผลให้ปริมาณบรอดคาสต์ทราฟฟิกมีมากขึ้น และถูก FLOOD แพร่กระจายไปทั่วถึงกันทุก ๆ ชั้น ในลักษณะที่เรียกว่า “FLAT NETWORK” ครั้นพอจะแบ่งเป็น VLAN ย่อย ๆ ก็อาจมาติดปัญหาหลายเรื่อง ๆ เช่น เรื่องของ IP Address ที่จัดสรรให้กับเครื่องต่าง ๆ โดยเฉพาะเซิร์ฟเวอร์ระบบงานสำคัญที่ถูกซับไว้แล้ว IP Address ที่อยู่บนเครื่องเซิร์ฟเวอร์เหล่านี้อาจมีความจำเป็นต้องเปลี่ยนแปลงไปหลังจากอิมพลีเมนต์ VLAN ขึ้นมาซึ่งกลายเป็นภาระยุ่งยาก เพราะบางทีก็เปลี่ยนไม่ได้เนื่องจาก IP Address ได้ถูก “hard coded” เข้าไปในแอปพลิเคชันโปรแกรมแล้ว เป็นต้น ถ้าหากมีการวางแผนแบ่ง VLAN ไว้ก่อนในอนาคตหากมีการเพิ่มขยายระบบออกไปเช่น มีการเชื่อมต่อสวิตช์ใหม่กับสวิตช์ตัวเดิมหรือมีปริมาณเครื่องคอมพิวเตอร์มากขึ้น ก็ไม่ต้องกังวนว่าปริมาณเครื่องที่เพิ่มขึ้นจะส่งผลกระทบต่อประสิทธิภาพโดยรวมของเน็ตเวิร์ก

ตัวอย่างหลักเกณฑ์การออกแบบ VLAN

หลักการในการแบ่ง VLAN นั้นไม่ได้มีข้อกำหนดตายตัวใด ๆ ขึ้นอยู่กับความพอใจของผู้ออกแบบและความเหมาะสมเป็นสำคัญ อย่างไรก็ดี อย่าได้มองข้ามหลักพื้นฐานว่าระบบเน็ตเวิร์กนั้นมีขึ้นมาเพื่อรองรับแอปพลิเคชันต่าง ๆ ในองค์กร ฉะนั้น หลักในการแบ่ง VLAN ที่ดีขอให้มองจากมุมของแอปพลิเคชันที่ทำงานอยู่บนสวิตช์เน็ตเวิร์กประกอบด้วย เพราะถึงแม้บรอดคาสต์ทราฟฟิกโดยทั่วไปจะมีผลต่อการ

ทำงานโดยรวมของระบบเน็ตเวิร์กแต่ในบางครั้งบางโอกาส องค์กรนั้นอาจจำเป็นต้อใช้งานแอปพลิเคชันรุ่นเก่า ๆ สำหรับการดำเนินธุรกิจซึ่งแอปพลิเคชันดังกล่าวจำเป็นต้องอาศัยการส่งผ่านข้อมูลแบบบรอดคาสต์ทราฟฟิกตลอดเวลา ลักษณะนี้เครื่องคอมพิวเตอร์ทั้งหมดที่ใช้งานแอปพลิเคชันดังกล่าวก็สมควรได้รับการเซตให้ห้อยู่ใน VLAN เดียวกันทั้งหมดไม่ควรแบ่งแยกออกเป็น VLA ย่อย ๆ ทั้งนี้เพื่อให้เครื่องทั้งหมดมีโอกาสไดรับข้อมูลของแอปพลิเคชันที่ส่งมาแบบบรอดคาสต์ และขจัดปัญหาต่าง ๆ ในการสื่อสารที่อาจเกิดขึ้นในอนาคตได้

โดยดีฟอลต์ สวิตช์ไม่มีการแบ่ง VLAN ทุกพอร์ตของมันจะถือว่าอยู่ใน VLAN ดีฟอลต์เดียวกัน นั่นคือ VLAN หมายเลข 1

ตัวอย่างต่อไปนี้แสดงหลักเกณฑ์ต่างๆ ที่นำมาใช้ในการพิจารณาแบ่ง VLAN ได้ ได้แก่

1) แบ่งตามตำแหน่งทางกายภาพ เช่น แบ่งตามแต่ละชั้นในอาคาร หรือแบ่งตามสวิตช์ หรือแบ่งตามตำแหน่งที่ตั้งของหน่วยงาน เช่น เครื่องคอมพิวเตอร์ที่เชื่อมต่อสวิตช์ปลายทางที่อยู่ในชั้น 2 ให้อยู่ใน VLAN 2 ส่วนเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับสวิตช์ปลายทางในชั้น 3 ก็ให้อยู่ใน VLAN 3 ดังนี้เป็นต้น

2) แบ่งตามหน่วยงาน ถึงแม้ว่าเครื่องคอมพิวเตอร์จะได้รับการเชื่อมต่ออยู่บนสวิตช์คนละตัวกัน แต่ก็สามารถนำมารวมเข้าเป็นสมาชิกของ VLAN เดียวกันได้ รูปข้างล่างนี้แสดงตัวอย่างการแบ่ง VLAN ตามหน่วยงาน เช่น ที่แต่ละชั้นมีพนักงานของฝ่ายขาย ฝ่ายบริหารโครงการ และฝ่ายช่างนั่งอยู่รวมกัน เราสามารถจัดสรรพอร์ตบนสวิตช์ที่แต่ละชั้นให้ให้อยู่ใน VLAN ของแต่ละแผนกแยกกันได้ (นี่คือตัวอย่างหนึ่งของการแบ่ง VLAN โดยไม่มีข้อจัดทางกายภาพ)

3) แบ่งตามฟังก์ชันการทำงานหรหรือแบ่งตามกลุ่มคณะทำงาน เช่น เรามีกลุ่มของคณะทำงานเดียวกันนั่งอยู่กระจัดการะจายตามแต่ละชั้น เราสามารถจัดสรรพอร์ตสวิตช์ที่เครื่องคอมพิวเตอร์เหล่านั้นเชื่อมต่ออยู่ให้เข้ามาอยู่ในกลุ่ม VLAN เดียวกันได้ ไม่ว่าเครื่องของผู้ใช้เหล่านั้นจะเชื่อมต่ออยู่กับพอร์ตของสวิตช์ที่ชั้นไหนก็ตาม

4) แบ่งตามลักษณะของแอปพลิเคชันที่ใช้งาน มีโรงงานผลิตอุปกรณ์อิเล็กทรอนิกส์แห่งหนึ่งที่ผู้ใช้ที่นั่งอยู่ตามโรงงานย่อยต่าง ๆ จำเป็นต้องรัน 2 แอปพลิเคชัน แอปพลิเคชันแรกสำหรับควบคุมการผลิตและอีกแอปพลิเคชันที่สองสำหรับใช้ในการทำงานทั่วไป ผู้ออกแบบเน็ตเวิร์กได้ออกแบบให้เครื่องคอมพิวเตอร์ที่ใช้งานแอปพลิเคชันสำหรับควบคุมการผลิตเชื่อมต่อเข้ากับพอร์ตของสวิตช์ที่อยู่ใน VLAN หนึ่ง (เช่น VLAN 10) และเครื่องคอมพิวเตอร์ที่ใช้ในงานทั่วไปเชื่อมต่ออยู่กับพอร์ตของสวิตช์ที่อยู่ในอีก VLAN หนึ่งแยกต่างหากไป (เช่น VLAN 20) ทั้งนี้เพื่อป้องกันไม่ใช้ทราฟฟิกของทั้ง 2 แอปพลิชันเข้ามาปะปนกัน เพราะแอปพลิเคชันสำหรับควบคุมการผลิตนั้นมีความสำคัญอย่างยิ่งยวดต่อธุรกิจของโรงงาน

หากทราฟฟิกใน VLAN 20 (ของแอปพลิเคชันทั่วไป) เกิดความไม่มีเสถียรภาพขึ้นจะด้วยเหตุผลใด ๆ ก็แล้วแต่ มันจะได้ไม่มีผลกระทบต่อการทำงานของแอปพลิเคชันที่เป็นหัวใจสำคัญของโรงงาน

6.5 การสร้าง VLAN และการเข้าเป็นสมาชิกของ VLAN

มีอยู่ 2 วิธีในการเซตให้พอร์ตของสวิตช์ (ส่งผลถึงเครื่องคอมพิวเตอร์ปลายทางที่ต่ออยู่กับพอร์ตสวิตช์) เข้าเป็นสมาชิกของ VLAN ได้แก่ static VLAN และ dynamic VLAN

6.5.1 Static VLANs

สแตกติก VLAN หรือเรียกอีกชื่อหนึ่งว่า “port-based membership” (การเป็นสมาชิกของ VLAN โดยพิจารณาจากพอร์ตสวิตช์) ในลักษณะนี้เครื่องคอมพิวเตอร์ขอผู้ใช้ปลายทางจะเป็นสมาชิกของ VLAN โดยขึ้นกับพอร์ตสวิตช์ที่มันคอนเน็กอยู่ด้วย

พอร์ตของสวิตช์จะถูกเซตให้เป็นสมาชิกของ VLAN โดยการเซตอัปของผู้ดูแลระบบ ถึงแม้เครื่องคอมพิวเตอร์สองเครื่องจะเชื่อมต่ออยู่บนสวิตช์ตัวเดียวกัน แต่หากพอร์ตที่มันเชื่อมต่ออยู่เป็นสมาชิกของต่าง VLAN กัน เครื่องสองเครื่องดังกล่าวจะไม่มีทางสื่อสารกันได้ ในการทำให้เครื่องที่อยู่ต่าง VLAN กันพูดคุยกันได้ เราจำเป็นต้องมีอุปกรณ์เลเยอร์ 3 อย่างสวิตช์เลเยอร์ 3 และเราเตอร์เข้ามาช่วย

การคอนฟิก Static VLAN ขั้นแรก ต้องสร้างหมายเลข VLAN ขึ้นมาเก็บไว้ในฐานข้อมูล VLAN (VLAN Database ต่อไปบางทีผู้เขียนจะเรียกกับศัพท์ว่า “ดาต้าเบสของ VLAN”) ก่อนในขั้นที่สองจึงค่อยแมปหมายเลข VLAN นั้นเข้ากับพอร์ตของสวิตช์

ในการคอนฟิกสแตติก VLAN บนสวิตช์แบบ IOS BASED ขั้นตอนและคำสั่งมีดังนี้

Switch# vlan database เป็นคำสั่งที่ใช้เข้าสู่ฐานข้อมูลหรือดาต้าเบสของ VLAN

Switch vlan # vlan <หมายเลข VLAN> name <ชื่อของ VLAN – มีหรือไม่ก็ได้>

Switch vlan # exit

Switch #configure terminal

Switch(config) #interface interface –type module / number เช่น interface fa0/1

Switch(congig-if) #switchport access vlan <หมายเลข VLAN> แมปพอร์ตทำงานอยู่ในโหมด access (อ่านเพิ่มเติมในหัวข้อต่อไป)

Switch(congig-if) #switchport access vlan <หมายเลข VLAN> แมปพอร์ตให้เป็นสมาชิกของ VLAN

Switch(congig-if) #end

หมายเหตุ เพื่อเติมเกี่ยวกับการสร้าง VLAN บนสวิตช์แบบ IOS BASED

1) ถ้าหากเราเข้าสู่อินเตอร์เฟซคอนฟิกูเรชันโหมดก่อน แล้วพิมพ์คำสั่ง switch port access vlan <หมายเลข VLAN> ก่อนที่จะสร้างหมายเลข VLAN ภายใน VLAN Database สวิตช์จะจัดการสร้างหมายเลข VLAN นั้นขึ้นมาใน VLAN Database ให้อัตโนมัติ

2) สำหรับสวิตช์บางรุ่นเช่น รุ่น 3550 เราสามารถสร้างหมายเลข VLAN จากโกลบอลคอนฟิกูเรชันโหมดได้ เช่น Switch(config)#vlan <หมายเลข VLAN> จากนั้นมันจะให้ใส่ชื่อของ VLAN แล้ว exit ออกมา

3) ก่อนการสร้างหมายเลข VLAN ควรมีการพิจารณาใช้งานโพรโทคอล VIP ก่อนทุกครั้ง ว่าจะให้สวิตช์ปัจจุบันทำงานในโหมดใดและจะสร้างหมายเลข VLAN จากศูนย์กลางหรือไม่ หรือจะสร้างบนแต่ละสวิตช์แยกจากกัน

ในการคอนฟิกสแตติก VLAN บนสวิตช์แบบ SET BASED ขั้นตอนและคำสั่งมีดังนี้

Switch(enable) set vlan <หมายเลข VLAN> [name <ชื่อของ VLAN – มีหรือไม่ก็ได้>]

Switch(enable) set vlan <หมายเลข VLAN> หมายเลขโมดูล / หมายเลขพอร์ต

ตัวอย่างเช่น คำสั่งข้างล่างนี้จะสร้าง VLAN หมายเลข 80 ขึ้นมาและแมปเข้าพอร์ต 3/4-3/7

Console> (enable) set vlan 80 3/4-7

VLAN 80 modified

VLAN Mod/ports

_____ _____

80 3/4-7

Console> (enable)

ในการตรวจเช็คดูว่า บนสวิตช์ปัจจุบันอยู่กี่ VLAN และมีหมายเลขใดบ้าง ให้ใช้คำสั่ง show vlan และถ้าต้องการดูหมายลข VLAN แบบสรุปย่อ ให้ใช้คำสั่ง show vlan brief เอาต์พุตข้างล่างนี้เป็นตัวอย่างของคำสั่ง show vlan

VLAN	NAME	Status	Ports
1	default	active	Fa0/24, Gi0/2
10	VLAN0010	active	Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/21, Fa0/22, Fa0/23
12	VLAN0012	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

เอาต์พุตข้างต้นแสดงว่าพอร์ตั้งแต่ fa0/1-fa0/15 ได้รับการแมปให้เป็นสมาชิกของ VLAN หมายเลข 12 และพอร์ตตั้งแต่ fa0/16-fa0/23 ได้รัยการแมปให้เป็นสมาชิกของ VLAN หมายเลข 10

จำนวนหมายเลข VLAN ที่สามารถสร้างและจัดเก็บในดาต้าเบส VLAN ได้สูงสุดจะขึ้นกับสวิตช์รุ่นนั้น ๆ ให้ศึกษาดูจากคู่มือของแต่ละรุ่นอีกครั้งหรอไม่ก็ลองใช้คำสั่ง show vtp status และสังเกตฟิลด์ที่เขียนว่า “Maximum VLANs supported locally”

2950Switch11#sh vtp status
VTP Version : 2
Configuration Revision : 11
Maximum VLANs supported locally : 250
3750Switch22#sh vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 1005

6.5.2 Dynamic VLAN

เป็นการกำหนด VLAN ให้กับเครื่องคอมพิวเตอร์ของผู้ใช้โดยพิจารณาจากหมายเลข MAC Address เมื่อเครื่องคอมพิวเตอร์เชื่อมต่อกับพอร์ตของสวิตช์ สวิตช์จะตรวจเช็คหมายเลข MAC Address ของเครื่องคอมพิวเตอร์ และส่งหมายเลขดังกล่าวไปเช็กที่ฐานข้อมูลกลางบนเซิร์ฟเวอร์เพื่อดูว่าหมายเลข MAC Address ดังกล่าวควรเป็นสมาชิกของ VLAN ใด ผู้ดูแลระบบสามารถแมปความสัมพันธ์ระหว่าง MAC Address กับหมายเลข VLAN ได้โดยการเซตฐานข้อมูลที่อยู่บนเซิร์ฟเวอร์ที่ทำหน้าที่เป็น VLAN Membership Policy Server (VMPS)

สำหรับสวิตช์ของซิสโก้ dynamic VLAN สามารถถูกสร้างและเซตอัปได้ผ่านทางการใช้เครื่องมือบริหารจัดการอย่างเช่น CiscoWorks 2000 หรือ CiscoWorks for Switched Internetwork (CWSI) ถึงแม้ว่า dynamic VLAN ดูเหมือนจะให้ความยืดหยุ่นในการจัดสรร VLAN แต่มันก็เพิ่มภาระที่ค่อนข้างมากทีเดียวให้กับผู้ดูแลเน็ตเวิร์กและไม่ได้รับความนิยม

6.6 ความหมายของ Access Port และ Trunk Port

จุดเริ่มต้นของการอิมพลีเมนต์ VLAN ก็คือ การสร้างหมายเลข VLAN ขึ้นมา จากนั้นก็ทำการเซตคอนฟิกูเรชันเพื่อกำหนดลงไปว่าแต่ละพอร์ตของสวิตช์เป็นสมาชิกของหมายเลข VLAN ใดบ้าง โดยปกิพอร์ตที่เชื่อมต่อยู่กับเครื่องคอมพิวเตอร์ของผู้ใช้จะถูกกำหนดให้เป็นสมาชิกของ VLAN ใด VLAN หนึ่งเพียง VLAN เดียวเราเรียกพอร์ตดังกล่าวนี้ว่า “access port” กล่าวอีกอย่างหนึ่งก็คือ ทราฟฟิกที่วิ่งเข้าออกพอร์ตประเภท “access port” นี้เป็นทราฟฟิกของ VLAN เพียง VLAN เดียว

ตัวอย่างกรณีของการเซตพอร์ตให้เป็น access port

1) พอร์ตที่เชื่อมต่อโดยตรงกับเครื่องคอมพิวเตอร์ของผู้ใช้

2) พอร์ตที่เชื่อมต่อโดยตรงกับเครื่องเซิร์ฟเวอร์

3) พอร์ตที่เชื่อมต่อกับเราเตอร์ (โดยที่เราเตอร์นั้นไม่ได้ทำหน้าที่เราต์ (route) ทราฟฟิกระหว่าง VLAN คือเป็นพอร์ตเราเตอร์ที่คอนเน็ตเข้าเน็ตเวิร์กโดยผ่านทางพอร์ตของสวิตช์ธรรมดา)

ขั้นตอนต่อไปนี้เป็นการเซตพอร์ตของสวิตช์ให้ทำงานในโหมด access port

Switch (config) #interface <interface module / port> (เช่น interface fa0/1)

Switch (config-if) #switchport mode access

นอกจากพอร์ตประเภท “access port” แล้ว ยังมีพอร์ตอีกประเภทหนึ่งที่เรียกว่า “trunk port”, trunk port เป็นพอร์ตพิเศษที่เป็นสมาชิกของ VLAN ได้มากกว่าหนึ่ง VLAN กล่าวอีกอย่างหนึ่งก็คือ ทราฟฟิกของ VLAN มากกว่าหนึ่ง VLAN สามารถวิ่งผ่านพอร์ตที่เป็น trunk port ขึ้นมานี้ก็เพื่อรองรับความสามารถในการที่ VLAN หนึ่ง ๆ สามารถขยายออกไปบนพอร์ตสวิตช์หลายๆ ตัวได้อย่างเช่น VLAN ของแผนการขายสามารถมีสมาชิกเป็นพอร์ชสวิตช์หลาย ๆ ตัวกระจายอยู่ตามชั้นต่าง ๆ ได้

6.7 โพรโทคอลที่ช่วยให้ง่ายต่อการอิมพลีเมนต์ VLAN ในสวิตช์เน็ตเวิร์ก

ดังที่ได้รับทราบไปแล้วในตอนต้นว่า งานสำคัญประการหนึ่งของการอิมพลีเมนต์ VLAN ขึ้นมาก็คือ การสร้างหมายเลข VLAN โพรโทคอล VTP (Virtual Trunking Protocol) ของซิสโก้ได้รับการออกแบบและพัฒนาขึ้นมาเพื่อให้ง่ายต่อการสร้างหมายเลข VLAN ขึ้นมาบนสวิตช์ต่างๆ โดยแทนที่จะเสียเวลาสร้างหมายเลข VLAN ชุดเดียวกันโดยใช้คำสั่งเดียวกันซ้ำๆ กันหลายครั้งบนสวิตช์แต่ละตัว

โพรโทคอล VIP จะกำหนดให้ผู้ติดตั้งระบบทำการเลือกสวิตช์หลักตัวหนึ่งหรือมากกว่า ทำหน้าที่เป็น VTP Server และสร้างหมายเลข VLAN ลงไปเก็บไว้ที่ดาต้าเบส VLAN และ VTP Server ตัวนั้น จากนั้น ปล่อยให้ VTP Server ประกาศหมายเลข VLAN ที่ตนมีอยู่ผ่านทางพอร์ตที่เป็น Trunk ออกไปให้สวิตช์ตัวอื่น ๆ ได้รับทราบและเก็บหมายลข VLAN ที่ได้มาไว้ในดาต้าเบส VLAN ของตน โดยขั้นตอนและกระบวนการสื่อสารระหว่างสวิตช์ที่ทำหน้าที่เป็น VTP Server กับสวิตช์อื่น ๆ จะเกิดขึ้นผ่านทางเมสเสจที่ได้นิยามไว้ในโพรโทคอล VIP

หากได้ศึกษาจากนิยามต้นแบบของซิสโก้จะนิยาม VTP ว่าเป็น “โปรโตคคอลสื่อสารพิเศษที่ใช้งานเฟรมที่ส่งผ่านพอร์ต Trunk เพื่อช่วยให้ง่ายต่อการสร้าง ลบ และเปลี่ยนชื่อของ VLAN ในเน็ตเวิร์ก”

ก่อนจะศึกษาวิธีการเซตอัป VTP มีนิยามย่อย ๆ ที่ควรรู้ก่อนได้แก่

6.7.1 VTP Domain

คำว่า VTP Domain (โดเมนของ VTP) เป็นการรวมกลุ่มเอาสวิตช์ทั้งหมดที่ต้องการให้อยู่ในขอบเขตของการบริหารจัดการเดียวกันเข้ามาไว้ภายใต้หน่อยย่อยที่เรียกว่า “โดเมน”เดียวกัน สวิตช์ที่อยู่ภายใต้ดดเมนเดียวกันจะมีดาต้าเบสของ VLAN เป็นชุดเดียวกัน และสวิตช์จะไม่แชร์ดาต้าเบสของ VLAN เป็นชุดเดียวกัน และสวิตช์จะไม่แชร์ดาต้าเบสของ VLAN ของตนให้กับสวิตช์อื่นที่อยู่ต่างโดเมนกัน ค่าของ VTP Domain จะเป็นสตริงตัวอักษรที่ผู้ดูแลระบบสามารถเซตขึ้นมาเองได้ วิธีการทำให้สวิตช์ทุกตัวเข้ามาอยู่ภายใต้โดเมนเดียวกัน ก็คือ การเซตชื่อของ vtp domain ลงไปบนสวิตช์แต่ละตัวให้เหมือนกัน

6.7.2 VTP Modes

ในการเข้าร่วมเป็นสมาชิกของ VTP Domain สวิตช์แต่ละตัวจำเป็นต้องได้รับการคอนฟิกให้ทำงานในโหมดใดโหมดหนึ่งต่อไปนี้ โหมดของ VTP จะเป็นตัวกำหนดวิธีการและความสามารถในการประกาศหมายเลข VLAN ไปยังสวิตช์ตัวอื่นหรือรับหมายเลข VLAN มาจากสวิตช์ตัวอื่น

1) Server Mode สวิตช์ที่ทำงานในโหมด VTP Server มีสิทธิเต็มที่ในการเพิ่ม ลบ และแก้ไข้หมายเลข VLAN ของโดเมนปัจจุบัน หมายเลข VLAN ที่อยู่ในดาต้าเบส VLAN ของสวิตช์ที่อยู่ในโหมด VTP Server จะถูกประกาศและอัปไปยังสวิตช์ตัวอื่นๆ ในโดเมน โดยดีฟอลต์ สวิตช์ทุกตัวที่เป็นขึ้นมาจะทำงานในโหมด VTP Server โปรดสังเกตว่าใน 1 VTP Domain จะต้องมีอย่างน้อย 1 สวิตช์ที่ทำงานอยู่ในโหมด VTP Server แต่สามารถมีมากกว่า 1 สวิตช์ได้

2) Client Mode สวิตช์ที่ทำในโหมด VTP Client จะไม่สามารถสร้าง ลบ หรือแก้ไขหมายเลข VLAN ได้ มันจะหน้าที่หลักในการคอยรับฟังประกาศเกี่ยวกับหมายเลข VLAN (vtp

advertisement) ที่ถูกส่งมาจากสวิตช์ที่ทำงานอยู่ในโหมด VTP Server และจากนั้นก็แก้ไขหรือเพิ่มเติมหมายเลข VLAN บนดาต้าเบส VLAN ของตนเองให้สอดคล้องตามหมายเลข VLAN ที่ได้รับอัปเดตมาจาก VTP Server

3) Transparent Mode สวิตช์ที่ทำงานอยู่ในโหมด VTP Transparent จะไม่เข้าร่วมในการอัปเดตหมายเลยข VLAN กับสวิตช์ตัวอื่น มันจะไม่ส่งอัเดตหมายเลข VLAN ใหม่หรือที่แก้ไขไปให้ใคร และในขณะเดียวกันก็จะไม่รับหมายเลข VLAN จากใครมา กล่าวอีกอย่างหนึ่งก็คือ ผู้ดูแลระบบสามารถสร้าง ลบ และแก้ไขหมายเลข VLAN ที่มีอยู่บนดาต้าเบส VLAN บนสวิตช์ของตนได้โดยอิสระไม่เกี่ยวข้งกับสวิตช์ตัวอื่น สำหรับ VTP เวอรชัน 1 สวิตช์ในโหมด Transparent จะไม่ส่งผ่านข้อมูลเกี่ยวกับ VTP ออกไปให้สวิตชือื่นๆ แต่ VTP เวอร์ชัน 2 นั้น ถึงแม้มันจะไม่สนใจที่จะอัปเดตหมายเลข VLAN กับสวิตช์อื่น แต่มันก็จะส่งผ่านข้อมูลเกี่ยวกับ VTP ที่ได้รับมาจากสวิตช์ตัวหนึ่งผ่านไปให้กับสวิตช์ตัวอื่นผ่านทงสพอร์ต Trunk ของมัน (เรียกว่า การ relay ข้อมูลของ VTP)

6.7.3 VTP Advertisements

แต่ละสวิตช์ใน VTP Domain ที่ทำงานในโหมด VTI Server จะมีการประกาศ (advertise) หมายเลข VLAN และแอตตริบิวต์ต่าง ๆ ที่เกี่ยวข้องเช่น หมายเลข configuration revision number ปัจจุบันของดาต้าเบส VLAN ผ่านทางพอร์ต Trunk ออกไปแจ้งให้สวิตช์ตัวอื่นในโดเมนเดียวกันรับทราบ ด้วยการส่งเฟรมแบบมัลติคลสต์ เมื่อใดก็ตามที่มีการเพิ่มหรือลบหมายเลข VLAN บนดาต้าเบส VLAN ของสวิตช์ที่เป็น VTP Server สวิตช์ตัวนั้นจะส่ง vtp advertisement ออกไปให้สวิตช์ตัวอื่น ๆ ได้อัปเดตหมายเลข VLAN ตามไปด้วยทุกครั้งและเช่นเดียวกันเมื่อใดก็ตามที่ต้องการลบหมายเลข VLAN หรือแก้ไขชื่อของ VLAN เราก็สามารถกระทำที่สวิตช์ที่เป็น VTP Server เพียงครั้งเดียว จากนั้น VTP Server ก็จะช่วยประกาศ (advertise) ออกไปให้สวิตช์อื่นรับทราบว่าขณะนี้หมายเลข VLAN เดิมบางหมายเลขได้ถูกลบออกไปแล้วเพื่อให้สวิตช์ตัวอื่นลบ VLAN เดิมนั้นออกตามไปด้วย (VLAN ที่ถูกลบออกไปจะถูกประกาศออกไปว่าเป็น VLAN ที่ “non-existent” หรืออยู่ในสถานะที่ “deleted”)

การส่ง vtp advertisement สามารถเกิดขึ้นได้ใน 3 รูปแบบได้แก่

1) Summary advertisement เป็นการส่ง vtp advertisement จาก VTP Server เมื่อมีการแก้ไข้ค่าเซตของ VTP เอง แอตตริบิวต์ภายใน advertisement แบบนี้ได้แก่ ชื่อโดเมน, เวอร์ชัน VTP (1 หรือ 2), หมายเลข configuration revision number หรือค่าแฮชที่สร้างจากรหัสผ่านของ vtp เป็นต้น

2) Subset advertisement เป็นการส่ง vtp advertisement จาก VTP Server เมื่อมีการแก้ไขหมายเลข VLAN ภายในดาต้าเบส VLAN โดยปกติ การส่งแบบนี้มักเกิดขึ้นหลังการส่ง summary advertisement แอตตริบิวต์ภายใน advertisement แบบนี้ได้แก่ หมายเลข VLAN , ชื่อของ VLAN และอื่นๆ ที่เกี่ยวข้อง

3) Advertisement request from client เป็นการส่งการร้องขอจากสวิตช์ในโหมด VTP client ไปหา VTP Server เพื่อร้องขอข้อมูลบางอย่างเกี่ยวกับ VLAN อย่างเช่น สวิตช์ในโหมด VTP Client เพิ่งได้รับการเคลียร์ค่า VLAN ออกไปและมีการรีโหลด หลังจากรีโหลดเสร็จ มันส่งการร้องขอไปยัง VTP Server

หมายเลข Configuration Revision Number โดยดีฟลอต์ค่าแอตตริบิวต์ที่เรียกว่า Configuration Revision Number บนดาต้าเบส VLAN จะมีค่าเท่ากับศูนย์ (()) เมื่อใดก็ตามที่มีการไข้ VLAN ค่าของ Configuration Revision Number นี้จะถูกเพิ่มขึ้นทีละหนึ่งคำว่าการแก้ไขนั้นครอบคลุมไม่ว่าจะเป็น การเพิ่ม การลบ หรือการเปลี่ยนชื่อ VLAN ค่าแอตตริบิวต์นี้ถือเป็นส่วนหนึ่งที่อยู่ใน vtp advertisement

เมื่อสวิตช์ปัจจุบันได้รับ advertisement มาจากสวิตช์ตัวอื่นๆ สิ่งแรกที่มันทำคือการตรวจสอบค่าของ Configuration Revision Number ซึ่งเป็นแอตตริบิวต์หนึ่งที่อยู่ภายใน advertisement ที่ได้รับมาเพื่อเปรียบเทียบดูว่าค่าดังกล่าวมีค่ามากหรือน้อยกว่าค่า Configuration Revision Number ปัจจุบันบนดาต้าเบส VLAN ของตนหากผลการเปรียบเทียบปรากฏว่า

1) ค่า Revision Number ของ advertisement ที่ได้รับมามีค่ามากกว่า มันก็จะอัปเดตดาต้าเบส VLAN ของตนให้สอดคล้องตามหมายของ VLAN ที่อยู่ใน advertisement

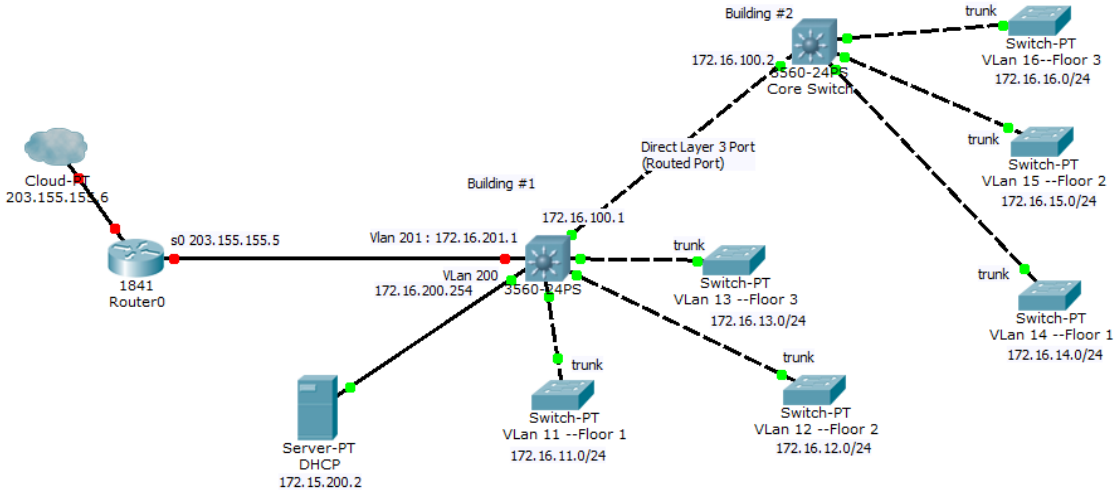
2) หากค่า Revision Number ของ advertisement ที่ได้รับมามีค่าต่ำกว่า มันจะไม่สนใจ advertisement นั้นๆ

6.7.4 VTP Password

โดยดีฟอลต์ การส่ง vtp advertisement ออกไปจะส่งแบบเคลียร์เท็กซ์ แต่เราสามารถเซต รหัสผ่าน“ ให้กับโดเมนของ VTP (vtp advertisement) ได้เพื่อสร้างความปลอดภัย สวิตช์ทุกตัวในโดเมนเดียวกันจะต้องได้รับการเซต “รหัสผ่าน” ให้เป็นรหัสผ่านเดียวกันทั้งหมดจึงสามารถรับส่ง vtp advertisement ระหว่างกันได้

6.8 กรณีศึกษา : ขั้นตอนการอิมพลีเมนต์ VLAN ในเน็ตเวิร์กจริง

ภาพที่ 6.1 เป็นตัวอย่างเน็ตเวิร์กจริงแบบไม่ซับซ้อนมากนักที่มีการใช้งานสวิตช์ทั้งแบบเลเยอร์ 2 และแบบเลเยอร์ 3 รวมไปถึงการเชื่อมต่อกับเราเตอร์เพื่อออกสู่อินเทอร์เน็ตภายนอก



ภาพที่ 6.1 ตัวอย่างการอิมพลีเมนต์ VLAN ในเน็ตเวิร์กจริง
ที่มา : เอกสิทธิ์ วิริยจารี. (2548).

รายละเอียดของการออกแบบในกรณีศึกษา

อุปกรณ์ที่ใช้

1) สวิตช์ Cisco Catalyst 3750 ทำหน้าที่เป็น “CORE SWITCH” ภายในแต่ละอาคาร บนสวิตช์รุ่นนี้มีพอร์ตที่เป็นแบบ 10/100/1000 ไว้รองรับคอนเน็กชันจาก Catalyst 2950T ที่ติดตั้งอยู่ในแต่ละชั้น พร้อมกันนั้น ยังทำหน้าที่เร้าต์ทราฟฟิกระหว่าง VLAN ต่างๆ ที่อยู่ภายในอาคารเดียวกัน และทำหน้าที่เชื่อมต่อผ่านสายไฟเบอร์ไปยัง “CORE SWITCH” อีกแล้วที่อยู่ในอีกอาคารหนึ่ง สวิตช์รุ่นนี้ทำงานได้ทั้งฟังก์ชันของเลเยอร์ 3 และเลเยอร์ 2 ในตัวเดียวกัน

2) สวิตช์ Cisco Catalyst 2950T ทำหน้าที่เป็น “ACCESS SWIRCH” เพื่อเชื่อมโยงขึ้นไปยังสวิตช์ Catalyst 3750 ซึ่งทำหน้าที่เป็น Core switch ภายในอาคารเดียวกัน

6.8.1 แนวทางการแบ่ง VLAN และหมายเลข IP Address

ในที่นี้ผู้เขียนแบ่ง VLAN โดยพิจารณาแบ่งตามแต่ละชั้นที่เป็นทั้งตั้งของ ACCRESS SWITCH กล่าวคือพอร์ตทุกพอร์ตของสวิตช์ที่กระจายอยู่ตามชั้นของแต่ละอาคารจะได้รับการกำหนด VLAN เป็นของตนเอง เพื่อให้ง่ายต่อการเซตคอนฟิกูเรชัน สรุปเป็นตารางดังนี้

ตารางที่ 6.1 สรุปการแบ่ง VLAN และหมายเลข IP Address

VLAN ID	VLAN Name	Location	IP Subnet	Gateway
11	VLAN11	อาคาร 1 ชั้น 1	172.16.11.0/24	172.16.11.254
12	VLAN12	อาคาร 1 ชั้น 2	172.16.12.0/24	172.16.12.254
13	VLAN13	อาคาร 1 ชั้น 3	172.16.13.0/24	172.16.13.254
14	VLAN14	อาคาร 2 ชั้น 1	172.16.14.0/24	172.16.14.254
15	VLAN15	อาคาร 2 ชั้น 2	172.16.15.0/24	172.16.15254
16	VLAN16	อาคาร 2 ชั้น 3	172.16.16.0/24	172.16.16.254

การเร้าต์ทราฟฟิกระหว่าง VLAN (Inter VLAN Routing)

1) สวิตช์ CORE SWITCH ทำหน้าที่เร้าต์ทราฟฟิกระหว่าง VLAN ภายในอาคารเดียวกัน โดยการสร้าง INTERFACE VLAN ขึ้นมาทำหน้าที่เป็นดีฟอลต์เกตเวย์ให้กับเครื่องคอมพิวเตอร์ที่ต่ออยู่กับพอร์ตของ ACCESS SWIRCH ในชั้นต่าง ๆ

2) CORE SWITCH แต่ละตัวจะดูแลทำหน้าที่เร้าต์ทราฟฟิกระหว่าง VLAN ให้กับเฉพาะ VLAN ที่อยู่ภายในอาคารเดียวกันเท่านั้น

ถ้าแบ่งให้แต่ละ CORE SWITCH เร้าต์ทราฟฟิกของ VLAN ภายในอาคาร ถ้าไฟเบอร์ลิงก์ระหว่างอาคาร 2 กับอาคาร 1 ขาดไป ถึงแม้เครื่องคอมพิวเตอร์ในอาคาร 2 จะไม่สามารถออกสู่อินเทอร์เน็ตผ่านทางอาคาร 1 ได้ เหมือนปกติ แต่อย่างน้อย ๆ มันก็ยังสามารถติดต่อกันระหว่าง VLAN ภายในอาคารเดียวกันได้อยู่

ภาพรวมของการทำ Routing ของเน็ตเวิร์กทั้งหมด

ในที่นี้ เนื่องจากเน็ตเวิร์กที่ไม่ซับซ้อนนัก เราสามารถใช้งาน Static Route ได้เพื่อเร้าต์ทราฟฟิกระหว่างอาคาร และจากเน็ตเวิร์กภายในออกไปยังอินเทอร์เน็ตภายนอก

การเชื่อมต่อระหว่าง CORE SWITCH 3750

1) ในที่นี้ ผู้เขียนจะเซตพอร์ตที่เชื่อมต่อระหว่าง CORE SWITCH 3750 ให้ทำงานในเลเยอร์ 3 โดยตรง (direct L3 port หรือ routed port) ด้วยการใช้คำสั่ง no switchport ในอินเตอร์เฟซโหมดและระบุหมายเลข IP Address ลงไปตรงๆ บนพอร์ตนั้นๆ เลย เพื่อที่ในการเร้าต์ทราฟฟิกระหว่างอาคาร เราสามารถใช้คำสั่ง ip route (แบบสแตติก) เพื่อชี้ Next Hop ไปยังหมายเลข IP Address ของ CORE SWITCH ฝั่งตรงข้ามได้โดยตรง

2) คอนเน็กชันระหว่าง CORE SWITCH ทั้ง 2 อาคารจะเป็นแบบเลเยอร์ 3 แท้ ความหมายก็คือไม่มีเรื่องของ Spanning Tree ในเลเยอร์ 2 เข้ามาเกี่ยวข้องเลย ดังนั้น ขอบเขตของ VLAN หนึ่งๆ จึงสมควรอยู่ภายในอาคารเดียวกันเท่านั้น ตัวอย่างเช่น ที่ออกแบบไว้เดิม VLAN 11 นั้นครอบคลุมทุกๆ พอร์ตสวิตช์ 2950T ที่อยู่ชั้น 1 อาคาร 1 และสามารถเซตให้พอร์ตของสวิตช์ 2950T ที่อยู่ชั้นที่ 2,3 ของอาคาร 1 ให้เข้าเป็นสมาชิกของ VLAN 11 ได้กล่าวอีกอย่างก็คือพอร์ตของสวิตช์ที่อยู่ในอาคาร 1 สามารถถูกเซตให้เข้าเป็นสมาชิกของ VLAN 11, 12 หรือ 13 VLAN ใดก็ได้ในขณะที่พอร์ตของสวิตช์ที่อยู่ในอาคาร 2 สามารถถูกเซตให้เป็นสมาชิกของ VLAN 14, 15 หรือ 16 VLAN ใดก็ได้

การเชื่อมต่อระหว่าง ACCESS SWITCH กับ CORE SWITCH

การเชื่อมต่อระหว่างสวิตช์ที่เป็น ACCESS SWITCH กับ CORE SWITCH ของตน จะถูกเซตให้เป็นพอร์ต Trunk และใช้การ encapsulation แบบ 802.1Q

6.8.2 การออกแบบโดเมนของ VTP

เมื่อขอบเขตของเลเยอร์ 2 สิ้นสุดที่ CORE SWITCH แต่ละตัวในอาคาร ผู้เขียนจึงออกแบบให้สวิตช์ทั้งหมดที่อยู่ในอาคารเดียวกันอยู่ภายใต้โดเมนเดียวกัน และเป็นคนละโดเมนกับอีกอาคารหนึ่ง (แยกไว้ 2 โดเมน โดเมนใครโดเมนมันแยกกันสำหรับกลุ่มของสวิตช์ที่อยู่ในแต่ละอาคาร) พร้อมทั้งให้ CORE SWITCH ของแต่ละอาคารทำหน้าที่เป็น VTP Server เพื่อเป็นศูนย์กลางของการเพิ่ม ลบ และแก้ไขหมายเลข VLAN ที่ใช้งานภายในอาคารนั้น ๆ

6.8.3 การแจกจ่ายหมายเลข IP Address

เซิร์ฟเวอร์เครื่องหนึ่งที่อยู่ใน VLAN 200 ทำหน้าที่เป็น DHCP Server เพื่อแจกจ่ายหมายเลข IP Address ของแต่ละ Subnet ที่ใช้งานภายในแต่ละ VLAN ในแต่ละชั้น และเซตคอนฟิกูเรชันบนสวิตช์เลเยอร์ 3 (CORE SWITCH) ให้ส่งผ่านการร้องขอจาก DHCP Client ไปยัง DHAP Server

6.8.4 ขั้นตอนการเซตคอนฟิกูเรชัน

ได้แก่คำสั่งต่างๆ และวิธีการเซตให้ศึกษาจากหัวข้อต่างๆ ที่ได้อธิบายผ่านมาแล้วก่อนหน้านี้

1) เปิดสวิตช์ขึ้นมาและเซตคอนฟิกพื้นฐาน เช่น หมายเลข IP Address ของสวิตช์เองบน VLAN หมายเลข 1 หรือ VLAN หมายเลขอื่นที่ออกแบบไว้แล้วให้ทำหน้าที่เป็น Management VLAN, พารามิเตอร์เกี่ยวกับ speed/duplex และรหัสผ่านต่างๆ

2) การเซตอัป CORE SWITCH ของแต่ละอาคารให้ทำหน้าที่เป็น VTP Server ในโดเมนของตนเอง

3) การสร้างหมายเลข VLAN ภายในอาคารของตนขึ้นมาบนแต่ละ VTP Server

4) การเซตพอร์ตที่คอนเน็กระหว่าง ACCESS SWITCH กับ CORE SWITCH ให้ทำงานเป็นพอร์ต Trunk

5) การอัป ACCESS SWITCH ของแต่ละชั้นในอาคารให้ทำงานเป็น VTP Client ในโดเมนของตน (เซตชื่อ VTP Domain ให้ตรงกันกับที่เซตไว้บน CORE SWITCH และเปลี่ยนโหมดให้เป็นโหมด VTP Client)

6) การใช้คำสั่ง show vtp counters และ show status เพื่อตรวจสอบดูสถานะของ VTP และสถานะของพอร์ต Trunk (เพราะพอร์ต Trunk จำเป็นต้องทำงานก่อน ก่อนที่หมายเลข VLAN จะถูกส่งจาก VTP Server มายังสวิตช์แต่ละตัวได้)

7) การใช้คำสั่ง show vlan บนแต่ละ ACCESS SWITCH เพื่อตรวจสอบดูว่าได้รับหมายเลข VLAN ที่ประกาศมาจาก VIP Server หรือไม่ ในขั้นนี้ควรจะได้หมายเลข VLAN ที่เหมาะสมครบทั้งหมด

8) การแมปพอร์ตบนแต่ละสวิตช์เข้าเป็นสมาชิกของ VLAN ตามที่ได้ออกแบบไว้ในไดอะแกรมข้างต้น

9) การเซตให้พอร์ตที่คอนเน็กระหว่าง CORE SWITCH ทำงานในเลเยอร์ 3 โดยตรง

10) การเซตตคอนฟิกูเรชันเกี่ยวกับการเร้าติ้งทั้งหมด

11) การจัดการเรื่อง DHCP Server กับการเซต IP HELPER-ADDRESS ภายใต้ INTERFACE VLAN

12) การตรวจสอบดูว่าเครื่องคอมพิวเตอร์ของผู้ใช้ได้รับหมายเลข IP Address และพารามิเตอร์ต่างๆ ของโพรโทคอล TCP/IP มาจากเครื่อง DHCP Server ตามที่ได้ออกแบบไว้หรือไม่

13) การ PING TEST และการทดสอบแอปพลิเคชันต่างๆ

เอาต์พุตของการ show run บนสวิตช์มาแสดงและชี้ให้เห็นคอนฟิกที่สำคัญพร้อมทั้งแสดงเอาต์พุตของบางคำสั่งที่เกี่ยวข้องเช่น Show vtp status, show ip route เป็นต้น เพื่อไม่ให้เกิดความเยิ่นเย้อและให้เนื้อหากระชับ ผู้เขียนจึงขอแสดงเฉพาะคอนฟิกูเรชันของ CORE SWITCH หลักทั้ง 2 ตัว ของ ACCESS SWITCH ที่อยู่ในแต่ละอาคาร โดยนำเอาเฉพาะคอนฟิกของสวิตช์ 2950T ชั้นที่ 1 อาคาร 1 และชั้น 1 อาคาร 2 มาแสดง และคอนฟิกูเรชันของเราเตอร์ด้านนอก

เพื่อให้หน้าตาของคอนฟิกูเรชันที่ได้จากการ show run กระชับและเข้าใจง่าย จึงได้มีการตัดต่อหน้าตาของคอนฟิกไปบ้างบางส่วน และแสดงเฉพาะส่วนที่จำเป็นและเกี่ยวข้องกับหัวใจสำคัญต่างๆ เท่านั้นโดยจะขอละเว้นบรรทัดที่ไม่เกี่ยวข้องออกไป ซึ่งมีอยู่ด้วยกันหลายบรรทัด ตัวอย่างเช่น ลิสต์รายชื่ออินเตอร์เฟซ จะถูกแสดงอินเตอร์เฟซที่ถูกใช้งานจริงเท่านั้น

SHOW RUN ของอุปกรณ์ต่างๆ

SHOW RUN ของ CORE SWITCH 3750 อาคาร 1

3750COREONE#sh run

Building Configuration

Hostname 3750COREONE

!

Ip subnet-zero

Ip routing อีนาเบิลความสามารถในการรันเร้าติ้งโพรโทคอล

!

Interface GigabitEthernet1/0/1

Description ***Connection to 2950 Floor 1***

Switchport trunk encapsulation dotlq ต้องเซตประเภทของ encapsulation ให้เป็น Dot1Q เพราะพอร์ต UPLINK ของ 2950T สนับสนุนเฉพาะ Dot1Q

Switchport mode trunk พอร์ตนี้ถูกเซตให้เป็น Trunk เพื่อคอนเน็กไปยังพอร์ต UPLINK ของสวิตช์ 2950T ของชั้นที่ 1

!

Interface GigabitEthernet1/0/2

Description ***Connection to 2950 Floor 2***

Switchport trunk ncapsulation dotlq

Switchport mode trunk พอร์ตนี้ถูกเซตให้เป็น Trunk เพื่อคอนเน็กไปยังพอร์ต UPLINK ของสวิตช์ 2950T ของชั้นที่ 2

!

Interface GigabitEthernet1/0/3

Description ***Connection to 2950 Floor 3***

Switchport trunk ncapsulation dotlq

Switchport mode trunk พอร์ตนี้ถูกเซตให้เป็น Trunk เพื่อคอนเน็กไปยังพอร์ต UPLINK ของสวิตช์ 2950T ของชั้นที่ 3

!

Interface GigabitEthernet1/0/11

Description ***To Server***

Switchport access vlan 200 เซตให้พอร์ตที่คอนเน็กไปยังเซิร์ฟเวอร์ให้อยู่ใน VLAN 200

Switchport mode access พอร์ตที่ต่อกับเครื่องเซิร์ฟเวอร์ควรได้รับการเซตให้เป็นโหมด Accesss

Spanning-tree portfast อ่านบทที่ 15 เรื่อง Spanning-tree (จะทำให้พอร์ตที่ต่อกับเซิร์ฟเวอร์ UP ได้อย่างรวดเร็ว)

!

Interface GigabitEthernet1/0/20

Description *** To Internet ROUTER ***

Switchport access vlan 201 เซตให้พอร์ตที่คอนเน็กกับเราเตอร์ขออกอินเทอร์เน็ตให้อยู่ใน VLAN 201

Switchport mode access พอร์ตที่ต่อกับเราเตอร์ (ที่ไม่ได้ทำการเราเตอร์ทราฟฟิกระหว่าง VLAN) ควรถูกเซตให้อยู่ในโหมด Access

!

Interface GigabitEthernet1/0/25 พอร์ตนี้เป็น routed port ที่คอนเน็กเลเยอร์ 3 โดยตรงกับพอร์ตของ CORE SWITCH ที่อาคาร 2 (ฝั่งตรงข้าม)

Description ***Connection to Catalyst 3750 CORE Switch Building Two***

No switchport ดิสเอเบิลฟีเจอร์ในเลเยอร์ 2 และทำให้พอร์ตเป็นพอร์ตของเลเยอร์ 3 โดยตรง (routed port)

Ip address 172.16.100.1 255.255.255.252 ใส่หมายเลข IP Address และ Subnet Mask ลงไปตรงๆ

!

Interface Vlan11 สร้างเวอร์ชวลอินเตอร์เฟซขึ้นมาสำหรับทำหน้าที่เป็นดีฟอลต์เกตเวย์ให้กับเครื่องพีซีที่อยู่กับพอร์ตที่เป็นสมาชิกของ VLAN 11

Ip address 172.16.11.254 255.255.255.0 ระบุหมายเลข IP Address เพื่อให้ไคลเอนต์พีซีใน VLAN 11 ชี้ดีฟอลต์เกตเวย์มาที่นี้

Ip helper-address 172.16.200.2 คำสั่ง Helper จะระบุหมายเลข IP Address ของ DHCP Server ช่วยส่ง DHCP Request จากเครื่องไคลเอนต์ใน VLAN นี้ไปยัง DHCP Server

!

Interface Vlan12 สร้างเวอร์ชวลอินเตอร์เฟซขึ้นมาสำหรับทำหน้าที่เป็นดีฟอลต์เกตเวย์ให้กับเครื่องพีซีที่อยู่กับพอร์ตที่เป็นสมาชิกของ VLAN 12

Ip address 172.16.12. 255.255.255.0 ระบุหมายเลข IP Address เพื่อให้ไคลเอนต์พีซีใน VLAN 12 ชี้ดีฟอลต์เกตเวย์มาที่นี้

Ip helper-address 172.16.20.2 ระบุหมายเลข IP Address ของ DHCP Server

!

Interface Vlan13 สร้างเวอร์ชวลอินเตอร์เฟซขึ้นมาสำหรับทำหน้าที่เป็นดีฟอลต์เกตเวย์ให้กับเครื่องพีซีที่อยู่กับพอร์ตที่เป็นสมาชิกของ VLAN 13

Ip address 172.16.13.254 255.255.255.0 ระบุหมายเลข IP Address เพื่อให้ไคลเอนต์พีซีใน VLAN 13 ชี้ดีฟอลต์เกตเวย์มาที่นี้

Ip helper-address 176.16.200.2 ระบุหมายเลข IP Address ของ DHCP Server

!

Interface Vlan200 เป็นเวอร์ชวลอินเตอร์เฟซเลเยอร์ 3 ที่ทำงานบนพอร์ตที่เป็นสมาชิกของ VLAN 200, ในที่นี้เพื่อทำหน้าที่เป็นดีฟอลต์เกตเวอร์ให้กับ VLAN 200 ซึ่งเป็น VLAN ของกลุ่มเซิร์ฟเวอร์

Ip address 172.16.200.254 255.255.255.0

!

Interface Vlan201 เป็นเวอร์ชวลอินเตอร์เฟซเลเยอร์ 3 ที่ทำงานบนพอร์ตที่เป็นสมาชิกของ VLAN 201 (ซึ่งสมาชิกหนึ่งใน VLAN 201 นี้ก็คือฮาร์ดแอวร์พอร์ต FastEthenet ของเราเตอร์ที่ออกอินเตอร์เน็ต) สวิตช์ 3750 จะใช้เวอร์ชวลอินเตอร์เฟซนี้ในการสื่อสารรับส่งแพ้กเตกับเราเตอร์ที่ต่อออกอินเตอร์เน็ต

Ip address 172.16.201.1 255.255.255.0

!

Ip classless

Ip route 0.0.0.0.0.0.0.0 172.16.201.2 ชี้ดีฟอลต์เร้าต์ออกทางอินเทอร์เน็ตเราเตอร์ที่พอร์ต FastEthenetของเราเตอร์(172.16.201.1)

Ip route 172.16.14.0 255.255.255.0 172.16.100.2 บอกให้เราเตอร์รู้ว่า ถ้าต้องการส่งแพ็กเก็ตไปยังซับเน็ตแอดเดรส 172.16.14.0/24 มันต้องส่งออกไปหาเราเตอร์ตัวถัดไป (next hop router) ที่มีหมายเลข IP Address เท่ากับ 172.16.100.2 (ซึ่งเป็นหมายเลข IP Address ของ “routed port”บนสวิตช์ 3750 ที่อาคาร 2 (พอร์ต Gigabit1/0/25)

Ip route 172.16.15.0 255.255.255.0 172.16.100.2 เซตเร้าติ้งเอ็นทรีชี้กลับไปยัง Subnet Address ของ VLAN 15(172.16.15.0/24) ที่อาคาร 2

Ip route 172.16.16.0 255.255.255.0 172.16.100.2 เซตเร้าติ้งเอ็นทรีชี้กลับไปยัง Subnet Address ของ VLAN 15(172.16.15.0/24) ที่อาคาร 2

End

SHOW RUN ของ ACCESS SWITCH 2950T อาคาร 1 ชั้น 1

2950BLDG1FLOOR1#sh run

Building configuration

Hostname 2950BLDG1FLOOR1

!

Interface FastEthernet0/1

Switchport mode access เซตพอร์ตที่ต่อกับเครื่องไคลเอนต์พีซีให้อยู่ในโหมด Access

Switchport access Vlan11 เซตพอร์ตทุกพอร์ตบนสวิตช์นี้ให้เป็นสมาชิกของ VLAN 11 ตามที่ได้ออกแบบไว้แต่ต้น

Spanning-tree portfact ทำให้พอร์ต UP ได้อย่างรวดเร็ว

!

Interface FastEthernet0/2

Switchport mode access

Switchport access Vlan11

Spanning-tree portfact

!

(พอร์ตอื่นๆ ตั้งแต่ interface fastetherne0/3- fastetherne0/22 มีคอนฟิก
เหมือนกัน)

Interface FastEthernet0/23

Switchport mode access

Switchport access Vlan11

Spanning-tree portfact

!

Interface FastEthernet0/24

Switchport mode access

Switchport access Vlan11

Spanning-tree portfact

!

Interface FastEthernet0/2

Switchport mode trunk เซตพอร์ตที่ UPLINK ขึ้นไปยัง CORE SWITCH 3750 ในอาคารของ
ให้อยู่ในโหมด Trunk

!

Interface FastEthernet0/2

!

End

SHOW RUN ของ CORE SWITCH 3750 อาคาร 2

3750CORETWO#sh run

Building configuration

Hostname 3750CORETWO

!

Ip subnet-zero

Ip routing

!

Interface FastEthernet1/0/1 เซตพอร์ตที่ UPLINK ขึ้นไปยัง CORE SWITCH 2950 ในอาคารของให้อยู่ในโหมด Trunk

Description ***connection to 2950 Floor 1***

Switchport trunk encapsulation dotlq

Switchport mode trunk

!

Interface FastEthernet1/0/2

Description ***connection to 2950 Floor 2***

Switchport trunk encapsulation dotlq

Switchport mode trunk

!

Interface FastEthernet1/0/3

Description ***connection to 2950 Floor 3***

Switchport trunk encapsulation dotlq

Switchport mode trunk

!

Interface FastEthernet1/0/25 พอร์ตนี้เป็น routed port ที่คอนเน็กเลเยอร์ 3 โดยตรงกับพอร์ตของ CORE SWITCH ที่อาคาร 1 (ฝั่งตรงข้าม)

No switchport ดิสเอเบิลฟีเจอร์ในเลเยอร์ 2 และทำให้พอร์ตเป็นพอร์ตของเลเยอร์ 3 โดยตรง (routed port)

Ip address 172.16.100.2 255.255.255.252 ใส่หมายเลข IP Address และ Subnet Mask ลงไปตรงๆ

!

Interface Vlan14 สร้างเวอร์ชวลอินเตอร์เฟซขึ้นมาสำหรับทำหน้าที่เป็นดีฟอลต์เกตเวย์ให้กับเครื่องพีซีที่ต่ออยู่กับพอร์ตที่เป็นสมาชิกของ VLAN 14

Ip address 172.16.14.254 255.255.255.0 ระบุหมายเลข IP Address เพื่อให้ไคลเอนต์พีซีใน VLAN 14 ชี้ดีฟลอต์เกตเวย์มาที่นี้

Ip helper-address 172.16.200.2 ระบุหมายเลข IP Address ของ DHCP Server

!

Interface Vlan15 เวอร์ชวลอินเตอร์เฟซที่เป็นดีฟอลต์เกตเวอร์ของ Vlan15 พร้อมด้วย IP Address

Ip address 172.16.15.254 255.255.255.0

Ip helper-address 172.16.200.2

!

Interface Vlan16 เวอร์ชวลอินเตอร์เฟซที่เป็นดีฟอลต์เกตเวอร์ของ Vlan16 พร้อมด้วย IP Address

Ip address 172.16.16.254 255.255.255.0

Ip helper-address 172.16.200.2

!

Ip classless

Ip route 0.0.0.0.0.0.0.0 172.16.100.1 ชี้ดีฟลอต์เร้า (default route) ออกไปทาง routed poute (พอร์ต Gigabit1/0/25) ของ CORE SWITCH ฝั่งตรงข้ามที่อาคาร 1 เพราะไม่ว่าจะต้องการเร้าต์แพ้กเก็ตออกไปหาซับเน็ต 172.16.11.0/24 , 172.16.12.0/24 , 172.16.13.0/24 หรือจะออกทางอินเทอร์เน็ตภายนอกก็ดี ก็ล้วนต้องผ่านไปยัง 172.16.100.1 ซึ่งเป็น IP Address ของ routed port (giga1/0/25) ของ CORE SWITCH#1 ทั้งสิน

End

SHOW RUN ของ ACCESS SWITCH 2950T อาคาร 2 ชั้น 1

2950BLDG2FLOOR1#sh run

Building configuration

Hostname 2950BLDG2FLOOR1

!

Interface FastEthernet0/1

Switchport mode access เซตพอร์ตที่ต่อกับเครื่องไคลเอนต์พีซีให้อยู่ในโหมด Access

Switchport access vlan 14 เซตพอร์ตทุกพอร์ตบนสสวิตช์นี้ให้เป็นสมาชิกของ VLAN 14 ตามที่ได้ออกแบบไว้แต่ต้น

Spanning-tree portfast ทำให้พอร์ต UP ได้อย่างรวดเร็ว

!

Interface FastEthernet0/2

Switchport mode access

Switchport access vlan 14

Spanning-tree portfast

!

Interface GigeabitEthernet0/1

Switchport mode access เซตพอร์ตที่ UPLINK ขึ้นไปยัง CORE SWITCH 3750 ในอาคารของตนให้อยู่ในโหมด Trunk

!

Interface GigeabitEthernet0/2

!

End

SHOW RUN ของ ROUTER

InternetRouter#sh run

Building configuration...

Hostname InternetRouter

!

Interface FastEthernet0

Ip address 172.16.201.2 255.255.255.0

Ip nat inside

Speed auto

!

Interface Seria10

Ip address 203.155.155.5 255.255.255.252

Ip nat inside

!

Ip nat inside source list 10 interface seria10 overload อ่านเรื่อง NAT ได้ในบทที่ 18

Access-list 10 permit 172.16.0.0.0.0.255.255

Ip classless

Ip route 0.0.0.0.0.0.0.0 203.155.155.6 ชี้ Default Route ออกไปทางแอดเดรสขา WAN ของเราเตอร์ที่ฝั่ง ISP เพื่อออกอินเทอร์เน็ต

Ip route 172.16.0.0 255.255.0.0 172.16.201.1 สร้างเร้าติ้งเอ็นทรีเพื่อเร้าต์แพ็กเก็ตกลับไปยังเน็ตเวิร์กแอดเสรที่ขึ้นต้นด้วย 172.16.0.0 โดยชี้ Next Hop Address ไปที่เวอร์ชวลอินเตอร์เฟซของ CORE SWITCH 3750 ที่อาคาร 1

End

คำสั่ง SHOW อื่นๆ ในกรณีศึกษาที่ให้ข้อมูลที่น่าสนใจ

SHOW VLAN BRIEF บนสวิตช์ 2950 อาคาร 1 ชั้น 1

2950BLDG1FLOOR1#sh vlan brief

VLAN	Name	Status	Ports
1	default	active	Gi0/2
10	VLAN0010	active	
11	VLAN0011	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
12	VLAN0012	active	

13 VLAN0013 active

200 VLAN_SERVER active

202 VLAN_TOROUTERPIX active

SHOW VLAN BRIEF บนสวิตช์ 2950 อาคาร 2 ชั้น 2

2950BLDG1FLOOR1#sh vlan brief

VLAN Name Status Ports

---- ---------- ------ ----------

1 default active Gi0/2

10 VLAN0010 active

14 VLAN0014 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

15 VLAN0015 active

16 VLAN0016 active

SHOW INTERFACE TRUNK บน CORE SWITCH 3750 ของอาคาร 1

3750COREONE#show interface trunk

Port Mode Encapsulation Status Native vlan

Gi1/0/1 on 802.1q trunking 1

Gi1/0/2 on 802.1q trunking 1

Gi1/0/3 on 802.1q trunking 1

Port Vlans allowed on trunk

Gi1/0/1 1-4094

Gi1/0/2 1-4049

Gi1/0/3 1-4094

Port Vlans allowed and active in management domain

Gi1/0/1 1,10-13,200,202

Gi1/0/2 1,10-13,200,202

Gi1/0/3 1,10-13,200,202

SHOW INTERFACE TRUNK บน CORE SWITCH 3750 ของอาคาร 2

3750COREONE#show interface trunk

Port	Mode	Encapsulation	Status	Native vlan
Gi1/0/1	on	802.1q	trunking	1
Gi1/0/2	on	802.1q	trunking	1
Gi1/0/3	on	802.1q	trunking	1

Port Vlans allowed on trunk

Gi1/0/1 1-4094

Gi1/0/2 1-4049

Gi1/0/3 1-4094

Port Vlans allowed and active in management domain

Gi1/0/1 1,14-16

Gi1/0/2 1,14-16

Gi1/0/3 1,14-16

SHOW IP ROUTE บน CORE SWITCH 3750 อาคาร 1

3750COREONE#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 – OSPF NSSA external type 2

E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP

I – IS – IS , L1 – IS – IS level – l, L2 – IS – IS level – 2 , ia – IS –IS inter area

*-candidate default , U – per – user static route, O – ODR

P – periodic downloaded static route

Gateway of last resort is 172.19.202.4 to network 0.0.0.0

	172..16.0.0/24	is	subnetted,	3 subnets	
S	172.16.16.0	[1/0]	via	172.16.100.2	
S	172.16.14.0	[1/0]	via	172.16.100.2	
S	172.16.15.0	[1/0]	via	172.16.100.2	
	172.16.0.0/24	is	subnetted,	5 subnets	
C	172.16.201.0	is	directlyconnected,	vlan201	
C	172.16.13.0	is	directlyconnected,	vlan13	
C	172.16.12.0	is	directlyconnected,	vlan12	
C	172.16.11.0	is	directlyconnected,	vlan11	
C	172.16.200.0	is	directlyconnected,	vlan200	
C	172.31.250.0/30	is	directlyconnected, GigabitEthernet1/0/25		
S*	0.0.0.0/0	[1/0]	via 172.19.201.2		

SHOW IP ROUTE บน CORE SWITCH 3750 อาคาร 2

	172.16.0.0/24	is	subnetted,	3 subnets	
C	172.16.16.0	is	directlyconnected,	vlan16	
C	172.16.14.0	is	directlyconnected,	vlan14	
C	172.16.15.0	is	directlyconnected,	vlan15	
C	172.31.250.0/30	is	directlyconnected, GigabitEthernet1/0/25		
S*	0.0.0.0/0	[1/0]	via 172.16.100.1		

บทสรุป

VLAN คือการนำความสามารถอีกขั้นหนึ่งของอุปกรณ์สวิตช์ที่ได้รับการนำไปอีมพลีเมนต์ในเน็ตเวิร์กส่วนใหญ่ มันทำให้การวางแผนออกแบบเน็ตเวิร์กที่ใช้สวิตช์มีประสิทธิภาพมากขึ้น

ภายใน 1 VLAN ควรประกอบด้วยเฉพาะ 1 ซับเน็ตแอดเดรสเท่านั้น

VLAN จะจำกัดขอบเขตการแพร่กระจายของบรอดคาสต์ทราฟฟิกไม่ให้ส่งผลกระทบต่อประสิทธิภาพโดยรวมของเน็ตเวิร์ก

เข้าเป็นสมาชิกของ VLAN ได้ 2 วิธีคือ static VLAN และ dynamic VLAN

การสร้างหมายเลข VLAN โดยใช้โพรโทคอล VTP ของซิสโก้ได้รับการออกแบบและพัฒนาขึ้นมาเพื่อให้ง่ายต่อการสร้างหมายเลข VLAN ขึ้นมาบนสวิตช์ต่าง ๆ

แบบฝึกหัด

จงตอบคำถามต่อไปนี้มาพอสังเขป

1. VLAN คืออะไรมีประโยชน์อย่างไร?
2. เพราะเหตุใดภายใน 1 VLAN ควรประกอบด้วยเฉพาะ 1 ซับเน็ตแอดเดรสเท่านั้น?
3. โพรโทคอล VTP มีบทบาทอย่างไรกับ VLAN?
4. Access Port และ Trunk Port คือ?
5. เครือข่ายแบบใดที่มีความจำเป็นต้องมีการจัดทำ VLAN?

อ้างอิง

เอกสิทธิ์ วิริยจารี .(2548). **เรียนรู้ระบบเครือข่ายจากอุปกรณ์ของ Cisco ภาคปฏิบัติ** กรุงเทพฯ .: ซีเอ็ดยูเคชั่น

จตุชัย แพงจันทร์) .2555). **เจาะระบบ Network 3nd Edition**. นนทบุรี: ไอดีซีฯ

Ciao Systems. (n.d). **เทคนิคการคำนวณ Summary Route (Route Summarization)**. สืบค้น 20 กุมภาพันธ์ 2559, สืบค้นจาก https://zone-network.blogspot.com/2013/12/summary-route-route-summarization.html

Stretch. (2553). **Basic Private VLAN Configuration**. Retrieved Jun 23, 2017, from http://packetlife.net/blog/2010/aug/30/basic-private-vlan-configuration/