รายงานการฝึกงาน

“ประมวลผลการฝึกงานประกอบวิชาชีพ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร”

โดย

นายสุวิทย์ สายโส รหัสนิสิต 64366751

รายงานนี้เป็นส่วนหนึ่งของการฝึกงาน ประจำปีการศึกษา 2566

สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร

รายงานการฝึกงาน

“ประมวลผลการฝึกงานประกอบวิชาชีพ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร”

โดย

นายสุวิทย์ สายโส รหัสนิสิต 64366751

รายงานนี้เป็นส่วนหนึ่งของการฝึกงาน ประจำปีการศึกษา 2566

สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร

กิตติกรรมประกาศ

ข้าพเจ้าได้มาฝึกงาน ณ บริษัท ยิบอินซอย จำกัด ตั้งแต่วันที่ 1 เมษายน พ.ศ. 2567 ถึงวันที่ 14 มิถุนายน พ.ศ. 2567 ส่งผลให้ข้าพเจ้าได้รับความรู้และประการณ์การทำงานต่างๆ ที่มีค่ามากมาย บัดนี้การฝึกปฏิบัติงานของข้าพเจ้าได้เสร็จสิ้นลงแล้ว ในการนี้ข้าพเจ้าใคร่ขอขอบพระคุณคุณ ฐิติพงษ์ ลิ้มอุดมสุข ตำแหน่ง Service Manager และบุคคลต่างๆที่มีส่วนช่วยเหลือให้การฝึกปฏิบัติงานของข้าพเจ้าได้สำเร็จลุล่วงไปด้วยดี และให้ข้อมูลรวมถึงองค์คาวมรู้ต่างๆ ที่เป็นประโยชน์ในการจัดทำรายงานการฝึกปฏิบัติงานในครั้งนี้

นอกจากนี้ข้าพเจ้าขอขอบพระคุณ อาจารย์ ดร. เศรษฐา ตั้งค้าวานิช ที่ให้คำแนะนำและให้ความช่วยเหลือในด้านการฝึกงาน รวมทั้งผู้มีส่วนเกี่ยวข้องทุกท่าน ที่มีส่วนช่วยในการดูแลและเป็นที่ปรึกษาให้การชี้แนะในการปฏิบัติงานตลอดเวลาที่ข้าพเจ้าได้ทำการฝึกปฏิบัติงานไว้ ณ โอกาสนี้

นายสุวิทย์ สายโส

ผู้จัดทำรายงาน

วันที่ 14 มิถุนายน พ.ศ. 2567

บทคัดย่อ

รายงานนี้จัดทำโดยนายสุวิทย์ สายโส นักศึกษาชั้นปีที่ 3 สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร ภายใต้การฝึกงานที่บริษัท ยิบอินซอย จำกัด ตั้งอยู่ที่ 523 ถนนมหาพฤฒาราม แขวงมหาพฤฒาราม เขตบางรัก กรุงเทพมหานคร 10500 เป็นสถานประกอบการเกี่ยวกับธุรกิจการค้าขายคอมพิวเตอร์พร้อมอุปกรณ์เครื่องคอมพิวเตอร์ ได้ฝึกงานในตำแหน่ง Field Service Engineer (Network) ซึ่งทำหน้าที่ออกแบบเครือข่ายตรวจสอบเครือข่ายและตั้งค่าอุปกรณ์เครือข่ายเพื่อให้ได้ใช้ประสิทธิภาพมากที่สุดก่อนที่จะส่งมอบให้ลูกค้า

ผลจากการฝึกงานในครั้งนี้ทำให้ได้ประสบการณ์และความรู้ใหม่ๆและได้เรียนรู้ระบบการทำงานของระบบหลังบ้านของระบบเครือข่ายและสามารถนำไปใช้ในชีวิตการทำงานแบบมืออาชีพได้จริง รวมถึงเรียนรู้เกี่ยวกับการติดตั้งหรือตั้งค่าเครื่องมือและอุปกรณ์ทางเครือข่ายอีกมากมาย

สารบัญ

สารบัญตาราง

สารบัญรูปภาพ

บทที่ 1
บทนำ

1.1 ชื่อและที่ตั้งของสถานประกอบการ

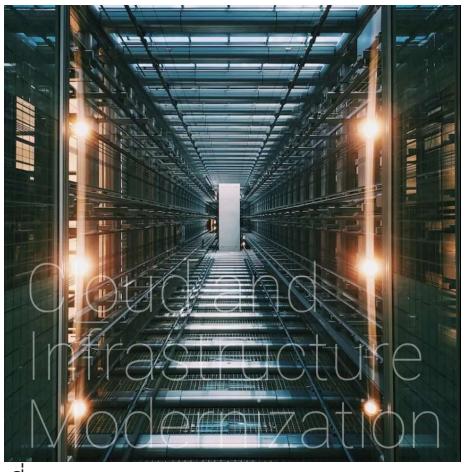
บริษัท ยิบอินซอย จำกัด 523 ถนนมหาพฤฒาราม แขวงมหาพฤฒาราม เขตบางรัก กรุงเทพมหานคร 10500

1.2 ลักษณะการประกอบการ ผลิตภัณฑ์ / ผลิตผล หรือการให้บริการหลักขององค์กร

บริษัท ยิบอินซอย จำกัด ประกอบธุรกิจประเภท การขายส่งและการขายปลีกการซ่อมยานยนต์และ จักรยานยนต์ โดยให้บริการด้าน การขายส่งคอมพิวเตอร์อุปกรณ์ต่อพ่วงคอมพิวเตอร์และซอฟต์แวร์

Cloud and Infrastructure Modernization ในภูมิทัศน์ทางธุรกิจที่เปลี่ยนแปลงตลอดเวลาในปัจจุบัน เทคโนโลยีถือเป็นรากฐานสำคัญที่สนับสนุนการดำเนินงานทุกด้าน ระบบโครงสร้างพื้นฐานไม่ว่าจะอยู่ในคลาวด์หรือภายในองค์กร ในปัจจุบันทำหน้าที่เป็นแกนหลักที่สำคัญที่ช่วยให้มั่นใจได้ว่าการแสวงหาเทคโนโลยีจะก้าวหน้าอย่างราบรื่นและมั่นคง ในทางกลับกันรับประกันประสิทธิภาพที่ต่อเนื่องและมีประสิทธิภาพของแอปพลิเคชันทางธุรกิจและบริการดิจิทัลซึ่งเป็นส่วนสำคัญต่อความสำเร็จทางธุรกิจ โดยรับประกันว่าจะให้ผลตอบแทนจากการลงทุนสูงสุด

ยิบอินซอย เป็นผู้เชี่ยวชาญที่ได้รับการยอมรับในการนำเสนอโซลูชั่นไอทีแบบครบวงจรที่ปรับให้เหมาะกับองค์กรในประเทศไทย โดยมีประสบการณ์เชิงลึกในสาขานี้ พร้อมที่จะช่วยเหลือในการยกระดับโครงสร้างพื้นฐานด้านไอทีไปสู่ระดับใหม่ โดยสอดคล้องกับโมเดล Hybrid Multi-Cloud เพื่อตอบสนองความต้องการที่เปลี่ยนแปลงไปของภูมิทัศน์ธุรกิจในปัจจุบัน ครอบคลุมการปรับปรุงระบบคลาวด์และโครงสร้างพื้นฐานให้ทันสมัย ไม่เพียงแต่ใช้ประโยชน์จากเทคโนโลยีล้ำสมัยและแนวคิดที่เป็นนวัตกรรมใหม่เท่านั้น แต่ยังมาพร้อมกับทีมงานมืออาชีพที่มากประสบการณ์อีกด้วย ผู้เชี่ยวชาญเหล่านี้มีทักษะในการวางแผน ออกแบบ คัดเลือก นำไปใช้ บูรณาการ ฝึกอบรม และบำรุงรักษาระบบอย่างรอบคอบ เพื่อให้มั่นใจว่าระบบจะทำงานได้อย่างมีศักยภาพสูงสุด เราทุ่มเทเพื่อช่วยเหลือคุณในการบรรลุประสิทธิภาพและประสิทธิผลสูงสุดในการดำเนินงานด้านไอที



รูปภาพที่ 1 Cloud and Infrastructure Modernization

Cyber Security เพิ่มความปลอดภัยให้กับคลาวด์ ศูนย์ข้อมูล อุปกรณ์ และผู้ใช้ทั่วทั้งองค์กรด้วยโซลูชันและบริการที่ครอบคลุม ภัยคุกคามทางไซเบอร์ก่อให้เกิดความเสี่ยงต่อธุรกิจไม่ว่าจะเป็นองค์กรใดก็ตาม ความความเสี่ยงนี้เน้นย้ำถึงบทบาทสำคัญของระบบไอทีในการดำเนินธุรกิจและมูลค่าที่เพิ่มขึ้นของข้อมูลทางธุรกิจ ส่งผลให้การโจมตีทางไซเบอร์ในรูปแบบต่างๆ เริ่มปรากฏให้เห็น และการแพร่กระจายของการโจมตีดังกล่าวก็เกิดขึ้นในอัตราที่ไม่เคยเกิดขึ้นมาก่อน นอกจากนี้ การบังคับใช้กฎหมายและข้อกำหนดด้านกฎระเบียบที่เข้มงวดยังเพิ่มความจำเป็นในการปรับปรุงมาตรการรักษาความปลอดภัยขององค์กรอีกด้วย ปัจจัยทั้งหมดเหล่านี้ทำให้องค์กรต่างๆ ต้องเร่งความพยายามในการเสริมสร้างโครงสร้างพื้นฐานด้านความปลอดภัย ซึ่งเป็นขั้นตอนพื้นฐานในการรับประกันความก้าวหน้าที่ยั่งยืน

ยิบอินซอย ผู้ให้บริการชั้นนำด้านไอทีและบริการดิจิทัลแบบครบวงจรในประเทศไทย ที่มีประสบการณ์อย่างเชิงลึกในการปกป้องระบบไอทีสำหรับธุรกิจ องค์กร และภาครัฐ พร้อมที่จะช่วยเหลือ ความเชี่ยวชาญของยิบอินซอยครอบคลุมการเพิ่มประสิทธิภาพการรักษาความปลอดภัยสำหรับระบบคลาวด์ โครงสร้างพื้นฐานด้านไอที แอปพลิเคชันทางธุรกิจ ข้อมูลธุรกิจ และอุปกรณ์ที่ผู้บริหารและพนักงานของคุณใช้ นำเสนอโซลูชั่นที่ครอบคลุมจากผู้ผลิตที่มีชื่อเสียงหลายรายและการสนับสนุนเฉพาะของวิศวกรความปลอดภัยทางไซเบอร์ทุกวันตลอด 24 ชั่วโมง เพื่อให้มั่นใจในความปลอดภัยและความมั่นคง

รูปภาพที่ 2 Cyber Security

Digital Business Solutions พลิกโฉมสู่ Digital Business และก้าวสู่ Digital Transformation อย่างมั่นใจกับ ยิบอินซอย การนำ Digital Transformation มาใช้อย่างต่อเนื่องภายในภาคธุรกิจขององค์กรนั้นคาดว่าจะยังคงมีอยู่ตราบใดที่โลกยังคงเห็นความก้าวหน้าและนวัตกรรมใหม่ๆ ความก้าวหน้าล่าสุดในเทคโนโลยี AI ได้ก้าวไปสู่ระดับที่การใช้งานจริงเป็นไปได้อย่างรวดเร็วในสถานการณ์ต่างๆ ในชีวิตจริง ความก้าวหน้านี้ได้กลายเป็นแรงผลักดันสำคัญในการส่งเสริมนวัตกรรม การพัฒนาผลิตภัณฑ์ใหม่ และการแนะนำบริการใหม่ๆ ภายในภาคธุรกิจขององค์กร ยิบอินซอย พร้อมเป็นพันธมิตรที่คุณไว้วางใจในการชี้นำธุรกิจไทยผ่านการเปลี่ยนแปลงที่ราบรื่นนี้ ด้วยการใช้ความรู้ที่กว้างขวางและประสบการณ์ที่ต่อเนื่องของเรา เรามีความเข้าใจอย่างลึกซึ้งทั้งในด้านธุรกิจและเทคโนโลยีในอุตสาหกรรมที่หลากหลาย ชุดบริการที่ครอบคลุมของเราประกอบด้วยการให้คำปรึกษา การพัฒนาซอฟต์แวร์ การออกแบบและการใช้งานโครงสร้างพื้นฐานคลาวด์หรือไอที และมาตรการรักษาความปลอดภัยที่ครอบคลุม

รูปภาพที่ 3 Digital Business Solutions

Data & Analytic Solutions เปลี่ยนข้อมูลธุรกิจให้เป็นมูลค่า วางรากฐานการจัดการข้อมูล สร้างสรรค์นวัตกรรมเพื่อการเติบโตทางธุรกิจที่ยั่งยืน ในภาพรวมธุรกิจปัจจุบัน ข้อมูลมีบทบาทสำคัญในการดำเนินงานของทุกองค์กร การเติบโตที่ยั่งยืนไม่เพียงแต่ขึ้นอยู่กับการจัดการหรือการดำเนินงานที่มีประสิทธิผลเท่านั้น แต่ยังรวมถึงการจัดการและการใช้ข้อมูลอย่างเชี่ยวชาญด้วย การใช้ข้อมูลอย่างเหมาะสมจะพัฒนาธุรกิจให้กลายเป็นธุรกิจดิจิทัลเต็มรูปแบบ พร้อมสำหรับการซึมซับ AI ซึ่งเป็นเทคโนโลยีที่อาศัยข้อมูลจำนวนมหาศาลสำหรับการพัฒนาและการดำเนินงานในอนาคต ยิบอินซอย นำความเชี่ยวชาญที่ครอบคลุมในการจัดการ การวิเคราะห์ และการใช้ข้อมูล ในฐานะหน่วยงานที่เชื่อถือได้ซึ่งได้รับความไว้วางใจให้ดูแลข้อมูลปริมาณมหาศาลทั่วทั้งภาครัฐและภาคการเงิน เราพร้อมที่จะขับเคลื่อนธุรกิจของคุณไปข้างหน้าด้วยการใช้ประโยชน์จากสินทรัพย์ข้อมูลของคุณ เพื่อให้มั่นใจว่าพื้นที่จัดเก็บและการใช้ประโยชน์ข้อมูลมีการจัดการที่มีประสิทธิภาพ เหมาะสม และปลอดภัย นอกจากนี้เรายังรับประกันการปฏิบัติตามข้อกำหนดในการปกป้องข้อมูล รวมถึงการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เพื่อปกป้องข้อมูลของคุณ

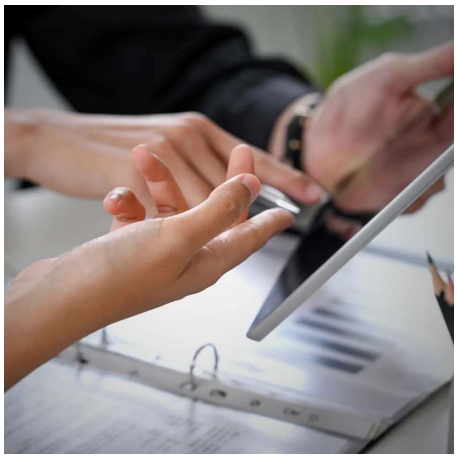
รูปภาพที่ 4 Data & Analytic Solutions

Professional Service รับประกันความคล่องตัวอย่างต่อเนื่องในการจัดการและบำรุงรักษาระบบไอทีของคุณด้วยบริการที่ครอบคลุมตลอด 24 ชั่วโมงทุกวันของ ยิบอินซอย การจัดการและบำรุงรักษาระบบไอทีและเทคโนโลยีที่ใช้โดยธุรกิจมีความสำคัญมากขึ้นท่ามกลางคลื่นแห่งการเปลี่ยนแปลงทางดิจิทัล แม้แต่ปัญหาเล็กๆ น้อยๆ ของระบบหรือการหยุดทำงานก็อาจส่งผลให้เกิดการสูญเสียยอดขายอย่างมาก กัดกร่อนความไว้วางใจของลูกค้า และทำให้ชื่อเสียงของบริษัทเสื่อมเสีย การขยายตัวอย่างรวดเร็วของระบบไอทีภายในภาคส่วนนี้ทำให้การบำรุงรักษา

ด้วยตนเองไม่สามารถทำได้ นอกจากนี้ การจ้างบุคลากรด้านไอทีใหม่ถือเป็นเรื่องท้าทายเนื่องจากการขาดแคลนผู้เชี่ยวชาญด้านไอทีทั่วโลก การจัดการกับความซับซ้อนที่เพิ่มขึ้นของระบบไอทีจำเป็นต้องได้รับบริการระดับมืออาชีพ ยิบอินซอย พร้อมที่จะรับมือกับความท้าทายด้วยทีมวิศวกรมืออาชีพของเราที่พร้อมให้บริการตลอด 24 ชั่วโมงเพื่อให้มั่นใจว่าระบบของคุณทำงานได้อย่างราบรื่น

รูปภาพที่ 5 Professional Service

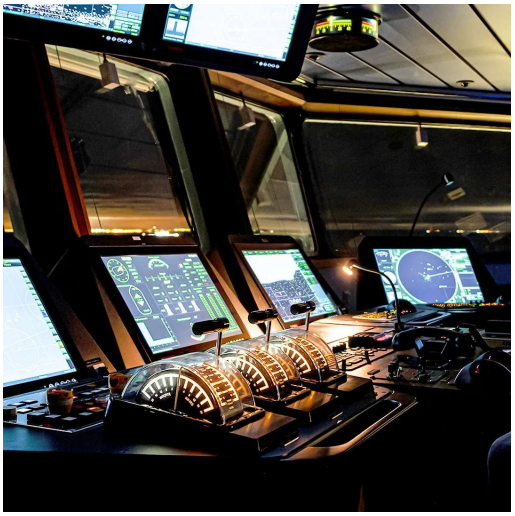
Financial & Banking Services ปลดล็อคศักยภาพธุรกิจทางด้านการเงินและการธนาคาร ขยายการเข้าถึงบริการอย่างไร้รอยต่อ ปลดล็อคศักยภาพของธุรกิจการเงินและการธนาคาร ขยายการเข้าถึงบริการอย่างไร้รอยต่อ



รูปภาพที่ 6 Financial & Banking Services

CNS : Communication Navigation Surveillance ระบบสื่อสาร ระบบเดินอากาศและระบบตรวจตราอากาศยาน เป็นระบบที่จำเป็นสำหรับนักบินและผู้ควบคุมการจราจรทาง

อากาศ สิ่งเหล่านี้อำนวยความสะดวกในกระบวนการพิจารณาว่าเครื่องบินอยู่ที่ไหน เวลาใด และอย่างไรที่จะไปถึงจุดหมายปลายทาง แผนกเทคโนโลยี CNS ของบริษัทนำเสนอผลิตภัณฑ์และบริการคุณภาพสูงในด้านการสื่อสาร การนำทาง เทคโนโลยีกล้องวงจรปิด ตามความต้องการของลูกค้า ด้วยประสบการณ์ในอุตสาหกรรมที่แข็งแกร่ง ความสามารถ และทีมงานบริการที่มีทักษะ บริษัทมีความมุ่งมั่นอย่างสูงในการสร้างความพึงพอใจให้กับลูกค้า



รูปภาพที่ 7 CNS : Communication Navigation Surveillance

Media Innovation Virtual Reality Production เปิดโอกาสให้ผู้กำกับและโปรดิวเซอร์สร้างวิสัยทัศน์ที่กว้างและน่าเชื่อถือของทิวทัศน์และสัตว์ป่าจากแหล่งที่สร้างแรงบันดาลใจของพวกเขาเอง เป็นเทคนิคที่เติบโตอย่างรวดเร็วในอุตสาหกรรมภาพยนตร์และโทรทัศน์ซึ่งช่วยให้ผู้สร้างสามารถสร้างเนื้อหาที่น่าดึงดูดและมีประสิทธิภาพมากขึ้น ด้วยการรวมวิธีการผลิตภาพยนตร์แบบดั้งเดิม เช่น การจับภาพเคลื่อนไหวและการจดจำใบหน้าเข้ากับการผลิตภาพเสมือนจริง ช่วยให้ผู้กำกับและโปรดิวเซอร์สามารถสร้างทิวทัศน์ที่กว้างใหญ่ ทิวทัศน์อันกว้างใหญ่ที่เต็มไปด้วยสัตว์ป่าที่กระโดดออกมาจากจินตนาการของพวกมันเอง ในขณะที่ยังคงผลิตด้วยต้นทุนที่ลดลง และ เพิ่มประสิทธิภาพการผลิต ด้วยการผลิตเสมือนจริง ผู้สร้างสามารถปรับเปลี่ยนเสื้อผ้าและสภาพแวดล้อมได้อย่างรวดเร็วและง่ายดาย การผลิตแบบเสมือนจริงกำลังกลายเป็นเครื่องมือที่ขาดไม่ได้ที่ผู้สร้างทุกคนควรมี ยิบอินซอยพร้อมเป็นพันธมิตรกับผู้ผลิตภาพยนตร์ บริษัทผลิตภาพยนตร์ และ Virtual Production ทุกราย เพื่อช่วยคุณลดต้นทุนและเวลาในการผลิตและเพิ่มคุณภาพงานในขณะที่ยังคงสามารถสร้างเนื้อหาได้อย่างอิสระตามต้องการด้วยระดับโลกของเราโซลูชั่นที่สามารถตอบสนองความต้องการของคุณได้อย่างเต็มที่

รูปภาพที่ 8 Media Innovation

1.3 รูปแบบการจัดองค์กรและการบริหารงานขององค์กร

1.1.1 ผู้บริหาร

1.1.2 หัวหน้าวิศวกร

1.1.3 หัวหน้าช่าง

1.4 ตำแหน่งและลักษณะงานที่นิสิตได้รับมอบหมายให้รับผิดชอบ

ตำแหน่งงานที่ได้รับมอบหมาย Field Service Engineer (Network) มีหน้าที่หลายอย่างที่เกี่ยวข้องกับการติดตั้ง ดูแล และซ่อมบำรุงระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์เครือข่าย งานหลัก ๆ มีดังนี้

1. การติดตั้งอุปกรณ์เครือข่าย: รวมถึงการตั้งค่าและการติดตั้งอุปกรณ์ต่าง ๆ เช่น เราเตอร์ สวิตช์ ไวไฟ และเซิร์ฟเวอร์ในสถานที่ที่กำหนด

2. การบำรุงรักษาและซ่อมแซม: ทำการตรวจสอบระบบเครือข่ายเพื่อหาข้อผิดพลาด แก้ไขปัญหาที่เกิดขึ้น และทำการบำรุงรักษาอุปกรณ์ให้อยู่ในสภาพพร้อมใช้งาน

3. การให้คำปรึกษาและช่วยเหลือผู้ใช้งาน: ให้คำแนะนำและช่วยเหลือผู้ใช้งานเกี่ยวกับการใช้ระบบเครือข่าย รวมถึงการแก้ไขปัญหาเฉพาะหน้าเมื่อผู้ใช้งานพบปัญหา

4. การอัปเดตและปรับปรุงระบบเครือข่าย: ดำเนินการอัปเดตซอฟต์แวร์ เฟิร์มแวร์ หรือการเปลี่ยนอุปกรณ์เพื่อให้ระบบเครือข่ายมีประสิทธิภาพและปลอดภัยมากยิ่งขึ้น

5. การตรวจสอบและประเมินผล: ตรวจสอบการทำงานของเครือข่ายเพื่อให้แน่ใจว่าระบบทำงานได้อย่างมีประสิทธิภาพ และเสนอแนะการปรับปรุงระบบให้ดียิ่งขึ้น

6. การจัดการเอกสารและรายงาน: จัดทำเอกสารการติดตั้ง การซ่อมบำรุง และรายงานการทำงาน รวมถึงการจัดทำแผนผังเครือข่าย

7. การฝึกอบรม: ให้การฝึกอบรมแก่ทีมงานหรือผู้ใช้งานเกี่ยวกับการใช้งานอุปกรณ์เครือข่ายและการดูแลระบบเบื้องต้น

Field Service Engineer (Network) จำเป็นต้องมีทักษะในการวิเคราะห์และแก้ไขปัญหา ความรู้เกี่ยวกับอุปกรณ์เครือข่ายและโปรโตคอลการสื่อสารต่าง ๆ รวมถึงทักษะในการสื่อสารและการทำงานเป็นทีม งานที่พวกเราทำไม่ได้มีอะไรมากเท่ากับคนที่มืออาชีพทำจริงๆอย่างที่กล่าวมาส่วนมากจึงเป็นการเรียนรู้พื้นฐานเพื่อนำไปต่อยอด

1.5 วิศวกรพี่เลี้ยง และตำแหน่งงานของวิศวกรพี่เลี้ยง

ชื่อ: ฐิติพงษ์ ลิ้มอุดมสุข

ตำแหน่ง: Service Manager

1.6 ระยะเวลาที่ปฏิบัติงาน

1 เมษายน พ.ศ. 2567 ถึง 14 มิถุนายน พ.ศ. 2567

บทที่ 2

วัตถุประสงค์ของการฝึกงานหรืองานที่ได้รับมอบหมาย

2.1 วัตถุประสงค์หรือจุดมุ่งหมายที่นิสิตหรือวิศวกรพี่เลี้ยง

2.1.1 เพื่อศึกษาข้อมูลเกี่ยวกับระบบเครือข่าย

2.1.2 เรียนรู้อุปกรณ์ทางเครือข่ายและวิธีใช้งาน

2.1.3 สามารถนำความรู้ไปต่อยอดขยายผลในการทำงานระดับมืออาชีพ

2.2 ผลที่คาดว่าจะได้รับจากการปฏิบัติงานหรือโครงงานที่ได้รับมอบหมาย

2.2.1 สามารถใช้งานอุปกรณ์เครือข่ายและเข้าใจหลักการทำงาน

2.2.2 มีประสบการณ์และความรู้ที่สามารถนำไปต่อยอดในระดับมืออาชีพได้

2.2.3 การทำงานร่วมมือกันแบบเป็นทีม

2.3 รายระเอียดงาน

ตามเวลาทำงาน ระยะเวลาเริ่มต้นคือเวลา 8.00 น. และสิ้นสุดเวลาคือเวลา 17.00 น. ช่วงเวลาพักตั้งแต่เวลา 12.00 น. ถึงเวลา 13.00 น. งานที่ได้รับมอบหมายส่วนใหญ่จะเป็นงานเกี่ยวกับการศึกษาความรู้และค้นคว้าด้วยตัวเองเรื่องการออกแบบเครือค่าย อุปกรณ์เครือค่ายและการตั้งค่าอุปกรณ์เพื่อปรับปรุงประสิทธิภาพของระบบเครือข่ายของจริง

หัวข้องาน		เดือนที่ 1				เดือนที่ 2				เดือนที่ 3			
1	Introduction to Networking	✓											
2	Implementing Ethernet LANs		✓										
3	Implementing VLANs and STP			✓									
4	IPv4 Addressing				✓								
5	IPv4 Routing Protocols					✓							
6	OSPF, BGP						✓						
7	IPv6							✓					
8	Wireless LANs								✓				
9	Access Control									✓			
10	NAT										✓		

ตารางที่ 1 แผนปฏิบัติงานฝึกงาน

เครื่องมือที่ใช้ในการฝึกงาน คือ Packet Tracer และ Xshell

รูปภาพ 9 โลโก้ Packet Tracer

โปรแกรม Packet Tracer เป็นเครื่องมือที่ใช้สำหรับจำลองและทดสอบเครือข่ายคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งในบริบทของเครือข่ายระดับนำทาง โปรแกรมนี้ได้รับความนิยมในการใช้งานภายในห้องเรียนและอุตสาหกรรมเนื่องจากความสามารถในการจำลองเครือข่ายอย่างสมจริงและการใช้งานที่สะดวกสบาย

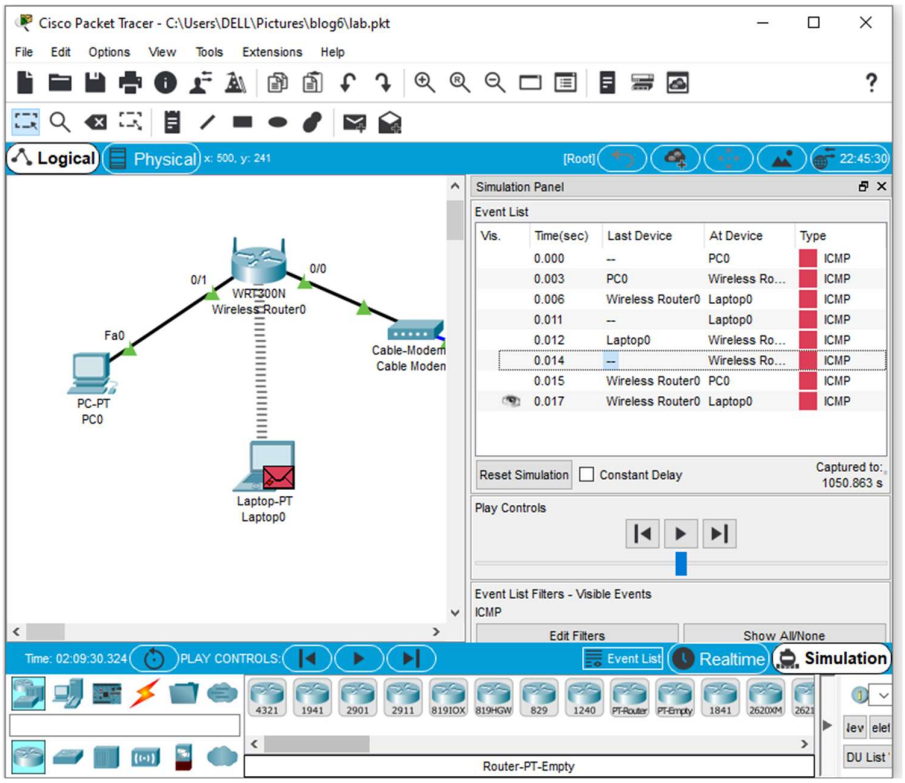
Packet Tracer ถูกพัฒนาโดย Cisco Systems ซึ่งเป็นบริษัทชั้นนำด้านเทคโนโลยีสารสนเทศและการสื่อสาร โปรแกรมนี้มีฟีเจอร์ที่มากมายเพื่อช่วยให้ผู้ใช้สามารถสร้างและทดสอบเครือข่ายได้อย่างสะดวก นอกจากนี้ยังเป็นเครื่องมือที่เหมาะสำหรับการศึกษาและการฝึกอบรมในด้านเครือข่ายคอมพิวเตอร์

คุณสมบัติหลักของ Packet Tracer ประกอบด้วย:

1. การจำลองเครือข่าย: ผู้ใช้สามารถสร้างเครือข่ายคอมพิวเตอร์ตามที่ต้องการได้โดยใช้อุปกรณ์และอุปกรณ์เครือข่ายต่าง ๆ ที่มีอยู่ในโปรแกรม และทดสอบการทำงานของเครือข่ายดังกล่าวได้โดยไม่ต้องมีอุปกรณ์ทางด้านจริง
2. Simulation: Packet Tracer มีแผนภาพต่าง ๆ และ Simulation ที่ช่วยให้ผู้ใช้เข้าใจการทำงานของเครือข่ายได้ง่ายขึ้น ซึ่งรวมถึงการจำลองการส่งข้อมูลผ่านเครือข่ายต่าง ๆ อย่างไร้ปัญหา
3. การสร้างและทดสอบการเชื่อมต่อ: ผู้ใช้สามารถสร้างและทดสอบการเชื่อมต่อเครือข่ายต่าง ๆ เช่น LAN, WAN, VLAN, และอื่น ๆ ได้อย่างง่ายดาย
4. การจำลองอุปกรณ์เครือข่าย: Packet Tracer มีอุปกรณ์เครือข่ายที่หลากหลายและครอบคลุมทุกระดับของชั้นของโครงข่าย เช่น สวิตช์, เราเตอร์, เซิร์ฟเวอร์, โปรโตคอลต่าง ๆ เป็นต้น

5. การศึกษาและการสอน: Packet Tracer เป็นเครื่องมือที่เหมาะสำหรับการใช้ในการศึกษาและการสอน เนื่องจากมีความสามารถในการสร้างสถานการณ์ที่เข้าใจง่ายและสะดวกสบายสำหรับการเรียนรู้เกี่ยวกับเครือข่ายคอมพิวเตอร์

Packet Tracer เป็นเครื่องมือที่มีความสำคัญสำหรับผู้เริ่มต้นในการศึกษาเกี่ยวกับเครือข่ายคอมพิวเตอร์ และเป็นเครื่องมือที่มีประสิทธิภาพสำหรับนักเชี่ยวชาญด้านเครือข่ายในการทดสอบและปรับปรุงเครือข่ายในสถานการณ์ที่ปลอดภัยและเสถียร



รูปภาพที่ 10 ตัวอย่างการออกแบบเครือข่ายในโปรแกรม Packet Tracer

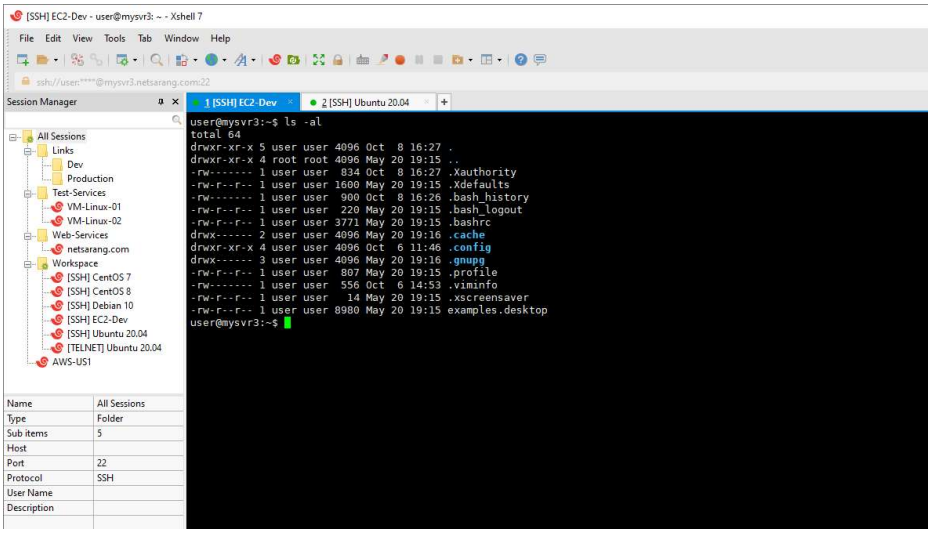
รูปภาพที่ 11 โลโก้โปรแกรม Xshell

Xshell เป็นโปรแกรมที่ใช้ในการจัดการและควบคุมอุปกรณ์เครือข่ายผ่านทางโปรโตคอล SSH (Secure Shell) โดยเฉพาะอย่างยิ่งสำหรับอุปกรณ์ที่ใช้ระบบปฏิบัติการ Unix หรือ Linux ซึ่งมักมีการใช้งาน SSH เพื่อเชื่อมต่อและจัดการผ่านทางเน็ตเวิร์กในลักษณะที่ปลอดภัย นอกจากนี้ Xshell ยังสามารถใช้งานร่วมกับโปรแกรมอื่น ๆ เช่น Xftp สำหรับการโอนย้ายไฟล์ผ่านทาง SSH ได้อีกด้วย

คุณสมบัติหลักของ Xshell ประกอบด้วย:

1. การเชื่อมต่อผ่านทาง SSH: Xshell มีความสามารถในการเชื่อมต่อกับอุปกรณ์เครือข่ายผ่านทางโปรโตคอล SSH โดยใช้การเข้ารหัสข้อมูลเพื่อความปลอดภัยขณะทำงาน ทำให้ผู้ใช้สามารถเชื่อมต่อกับอุปกรณ์เครือข่ายและทำงานร่วมกันได้อย่างปลอดภัย
2. การจัดการเซสชัน (Session Management): Xshell มีความสามารถในการจัดการเซสชันการเชื่อมต่อหลาย ๆ รายการพร้อมกัน ซึ่งช่วยให้ผู้ใช้สามารถเปิดหลายเซสชันและทำงานได้พร้อมกันโดยมีการจัดการที่มีประสิทธิภาพ
3. การแสดงผลแบบแบ่งหน้า (Tabbed Interface): โปรแกรมนี้มีการแสดงผลแบบแบ่งหน้าซึ่งช่วยให้ผู้ใช้สามารถเปิดหลายเซสชันและเครื่องคอมพิวเตอร์พร้อมกันได้ในหน้าต่างเดียว ทำให้การทำงานเป็นไปอย่างมีประสิทธิภาพและสะดวกสบาย
4. การตั้งค่าและปรับแต่ง: ผู้ใช้สามารถปรับแต่งการตั้งค่าต่าง ๆ ของ Xshell ให้เหมาะกับความต้องการและการใช้งานของตนเองได้ ซึ่งรวมถึงการปรับแต่งรูปแบบและสีของหน้าจอ การตั้งค่าการเชื่อมต่อ SSH, และการปรับแต่งคีย์บอร์ดเพื่อความสะดวกในการใช้งาน
5. การสนับสนุนเครื่องมืออื่น ๆ: Xshell สามารถทำงานร่วมกับเครื่องมืออื่น ๆ ที่ใช้ในการจัดการเครือข่ายและการเชื่อมต่ออื่น ๆ เช่น Xftp สำหรับการโอนย้ายไฟล์ผ่านทาง SSH และ Xlpd สำหรับการพิมพ์เอกสารผ่านทางเครือข่ายในรูปแบบที่ปลอดภัย

Xshell เป็นโปรแกรมที่มีประสิทธิภาพสำหรับผู้ที่ต้องการจัดการและควบคุมอุปกรณ์เครือข่ายผ่านทางเน็ตเวิร์กในลักษณะที่มีความปลอดภัยและมีประสิทธิภาพสูง



รูปภาพที่ 12 ตัวอย่างโปรแกรม Xshell

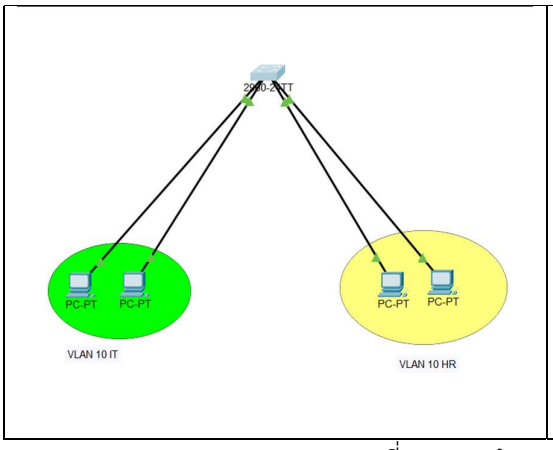
เนื้อหาการฝึกงาน และความรู้ที่ได้รับจากการฝึกงาน

การฝึกงานส่วนใหญ่จะเน้นการหาความรู้ด้วยตัวเองเกี่ยวกับการออกแบบเครือข่ายจำลองผ่านโปรแกรม Packet Tracer โดยจะศึกษาเกี่ยวกับการทำงานของอุปกรณ์รวมถึงการทำงานของโปรโตคอลแต่ละประเภทว่ามีรูปแบบการทำงานและการตั้งค่าอย่างไรให้ได้ประสิทธิภาพมากที่สุด

VLAN

VLAN(Virtual Local Area Network) คือเทคโนโลยีที่ใช้ในการแบ่งเครือข่าย LAN ให้ออกเป็นกลุ่มๆ ที่สามารถควบคุมการกระจายสัญญาณภายในเครือข่ายได้ โดยการแบ่งนี้จะเป็นการแบ่งขอบเขตของ การกระจายสัญญาณภายในอุปกรณ์หรือระบบเครือข่ายออกเป็นหลายๆ กลุ่ม (ที่เรียกว่า Broadcast Domain) ซึ่งการแบ่งนี้ทำในทางตรรกะ (Logical) ไม่ใช่ในทางกายภาพ (Physical) จึงเรียกว่า “Virtual” LAN หรือ VLAN

ตัวอย่างการกำหนดค่า VLAN




```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name IT
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name HR
Switch(config-vlan)#exit
Switch(config)#interface range f0/1-2
Switch(config-if-range)#switchport mode
access
Switch(config-if-range)#switchport access
vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range f0/3-4
Switch(config-if-range)#switchport mode
access
Switch(config-if-range)#switchport access
vlan 20
```

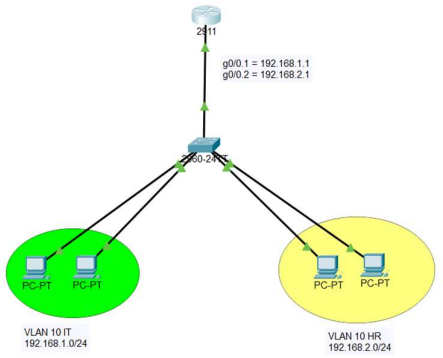
รูปภาพที่ 13 การกำหนดค่า VLAN บน Switch

Inter-VLAN (Inter-VLAN Routing) เป็นกระบวนการที่ช่วยให้การสื่อสารระหว่าง VLAN ต่างๆ ใน เครือข่ายสามารถเกิดขึ้นได้ โดยปกติแล้ว VLAN ต่างๆ จะไม่สามารถสื่อสารกันได้โดยตรง เนื่องจากแต่ละ VLAN มี Broadcast Domain ของตัวเอง เพื่อให้สามารถสื่อสารระหว่าง VLAN ได้ จำเป็นต้องใช้ Inter-VLAN Routing ซึ่งสามารถทำได้โดยใช้เราเตอร์หรือสวิตช์เลเยอร์ 3 (Layer 3 Switch)

การกำหนดค่า Inter-VLAN Routing

มีสองวิธีหลักในการตั้งค่า Inter-VLAN Routing

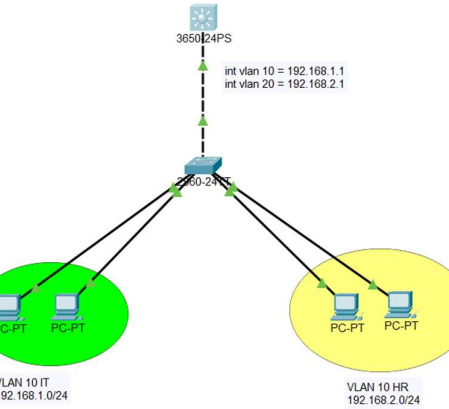
1. Router-on-a-Stick
   - ใช้เราเตอร์ที่มีการตั้งค่าพอร์ต 802.1Q Trunk
   - เราเตอร์จะรับเฟรมจากพอร์ต Trunk และทำการ Route ระหว่าง VLAN ต่างๆ
   - เหมาะสำหรับเครือข่ายขนาดเล็กหรือขนาดกลาง




```
Router(config)#interface g0/0.1
Router(config-subif)#encapsulation
dot1Q 10
Router(config-subif)#ip address
192.168.1.1 255.255.255.0
Router(config-subif)#exit
Router(config)#in g0/0.2
Router(config-subif)#encapsulation
dot1Q 20
Router(config-subif)#ip address
192.168.2.1 255.255.255.0
```

รูปภาพที่ 14 การกำหนดค่า Inter-VLAN บน Router

2. Layer 3 Switch
   - ใช้สวิตช์เลเยอร์ 3 ที่สามารถทำการ Route ได้ในตัว
   - ตั้งค่า SVI (Switched Virtual Interface) สำหรับแต่ละ VLAN บนสวิตช์
   - เหมาะสำหรับเครือข่ายขนาดใหญ่ที่ต้องการความเร็วและประสิทธิภาพสูง




```
Switch(config)#vlan 10
Switch(config-vlan)#name IT
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name HR
Switch(config-vlan)#in vlan 10
Switch(config-if)#ip add 192.168.1.1
255.255.255.0
Switch(config-if)#in vlan 20
Switch(config-if)#ip add 192.168.2.1
255.255.255.0
Switch(config-if)#ex
Switch(config)#ip routing
```

รูปภาพที่ 15 การกำหนดค่า Inter-VLAN บน Switch Layer 3

VTP

VTP (VLAN Trunking Protocol) เป็นโปรโตคอลของ Cisco ที่ใช้เพื่อจัดการและเผยแพร่ข้อมูล VLAN ในเครือข่ายสวิตช์ โดย VTP ช่วยลดความยุ่งยากในการกำหนดค่า VLAN บนสวิตช์หลายตัว และทำให้ การจัดการ VLAN เป็นไปอย่างมีประสิทธิภาพ

VTP Domain

VTP ใช้โดเมนเพื่อจัดกลุ่มสวิตช์ที่ต้องการแชร์ข้อมูล VLAN ร่วมกัน สวิตช์ในโดเมน VTP เดียวกันจะต้องมีชื่อโดเมน VTP และรหัสผ่านที่ตรงกัน

VTP Modes

- Server Mode: สามารถสร้าง, ลบ และแก้ไข VLAN และเผยแพร่ข้อมูล VLAN ไปยังสวิตช์อื่น
- Client Mode: รับข้อมูล VLAN จากสวิตช์ในโหมด Server และไม่สามารถสร้าง, ลบ หรือแก้ไข VLAN
- Transparent Mode: ไม่เข้าร่วมในการเผยแพร่ข้อมูล VLAN แต่ส่งผ่านข้อมูล VTP ไปยังสวิตช์อื่น

```
Switch> enable
Switch# configure terminal
Switch(config)# vtp domain mydomain
Switch(config)# vtp mode server
Switch(config)# vtp password mypassword
Switch(config)# exit
```

ในตัวอย่างนี้ เราได้กำหนดชื่อโดเมน VTP เป็น "mydomain" ตั้งค่าโหมดเป็น Server และกำหนดรหัสผ่าน เป็น "mypassword"

DTP

DTP (Dynamic Trunking Protocol) เป็นโปรโตคอลของ Cisco ที่ใช้ในการเจรจาต่อรองการตั้งค่า ลิงค์ระหว่างสวิตช์เพื่อกำหนดว่าลิงค์นั้นจะเป็นลิงค์ Trunk หรือ Access โดยจะส่งเฟรม DTP ไปยังสวิตช์ที่ เชื่อมต่อเพื่อแจ้งสถานะของพอร์ต DTP ช่วยให้การตั้งค่า Trunk เป็นไปอย่างอัตโนมัติและง่ายดาย

DTP Modes

- Dynamic Desirable: พยายามเจรจาต่อรองเพื่อสร้างลิงค์ Trunk กับพอร์ตปลายทาง
- Dynamic Auto: รับการเจรจาต่อรองจากพอร์ต Dynamic Desirable เพื่อสร้างลิงค์ Trunk
- Trunk: บังคับให้พอร์ตเป็นลิงค์ Trunk โดยไม่ต้องเจรจาต่อรอง
- Access: บังคับให้พอร์ตเป็นลิงค์ Access โดยไม่ต้องเจรจาต่อรอง

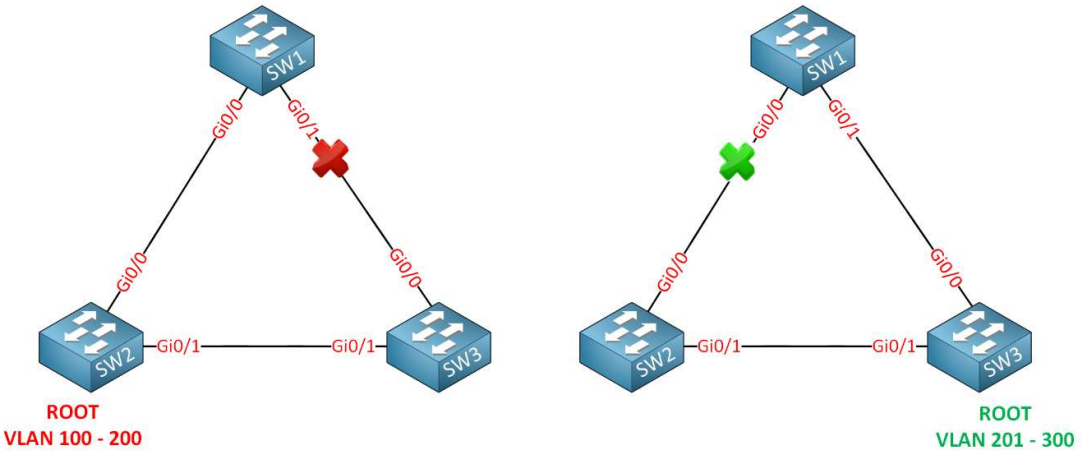
- Nonegotiate: ปิดการเจรจาต่อรอง DTP แต่สามารถกำหนดพอร์ตเป็น Trunk หรือ Access โดยตรง

ตาราง DTP Modes

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access

ตารางที่ 2 แสดง DTP เมื่อเปิดใช้งานทั้งสองด้าน

Spanning Tree Protocol



รูปภาพที่ 16 ตัวอย่างการเกิด Spanning-Tree Protocol

Spanning-Tree Protocol (STP) เป็น Protocol ที่ใช้ป้องกันลูป (Loop) ใน Layer 2 โดยการทำงานคือจะ Blocking Port เพื่อไม่ให้รับส่งข้อมูลจนกว่าเส้นทางหลักจะมีปัญหา และยังช่วยเสริมให้มีเส้นทาง สำรอง เช่น สมมุติว่าเรามีจุดหมายปลายทางอยู่จุดหนึ่งแล้วเส้นทางนี้เกิดมีปัญหาทำให้ระบบใช้งานไม่ได้เลย ก็ ทำให้ระบบทั้งหมดมีปัญหาไปด้วย ตัว Spanning Tree มันก็จะมีระบบช่วยป้องกันไม่ให้ระบบหยุดการทำงาน ถ้าเส้นทางหนึ่งมีปัญหาก็สามารถไปใช้เส้นทางอื่นได้ Redundancy ของ Spanning

Tree มันทำให้ระบบมี เสถียรภาพ เพราะใช้ตลอดเวลาก็ไม่ Down ถึงแม้เส้นทางใดเส้นทางหนึ่งใช้ไม่ได้ก็ตาม Spanning tree ก็จะมี เส้นทางขึ้นมาใช้แทนโดยรวมทำให้มีเสถียรภาพมากขึ้น

หลักการทำงานของ STP

1. เลือก Root Bridge คือใน 1 Network จะมี Switch เพียง 1 ตัวที่เป็น Root Bridge พิจารณาจาก Switch ที่มี Bridge ID น้อยที่สุด (Bridge ID = Priority + MAC Address) และขาของ Bridge ID เป็น Designated Port
2. เลือก Root Port พิจารณาจาก Port ที่มีค่า Path Cost ไปหา Root Bridge ต่ำสุดถ้า Path Cost เท่ากันให้พิจารณาจาก Bridge ID โดย Switch จะมี Root Port ได้เพียง 1 ตัวเท่านั้น
3. เลือก Design Port ใน Link ระหว่าง Switch กับ Switch หรือที่เรียกว่า Segment ต้องมี 1 Designated Port โดยพิจารณาจาก Path Cost ไป Root Bridge ต่ำสุด หากเท่ากันให้พิจารณาจาก Bridge ID ต่ำสุด ถ้า Bridge ID เท่ากัน ให้พิจารณาจาก Port ID ต่ำสุด และ port ที่เหลือจาก Root Port และ Designated Port คือ Block Port

คำสั่งที่เกี่ยวข้องกับ STP บน Cisco Switch

คำสั่ง	คำอธิบาย
`Switch(config)# spanning-tree mode {pvst | rapid-pvst | mst}`	เปิดใช้งาน STP บนสวิตช์
`spanning-tree vlan <vlan-id> priority <priority>`	กำหนด Priority ให้กับ VLAN ที่ระบุ (ค่า Priority เป็นทวีคูณของ 4096)
`show spanning-tree`	แสดงข้อมูลเกี่ยวกับ Root Bridge, Priority, Path Cost และ สถานะของพอร์ตต่างๆ
`spanning-tree cost`	กำหนดค่า Path Cost ให้กับพอร์ตที่กำหนด
`spanning-tree guard root`	กำหนด Root Guard เพื่อป้องกันไม่ให้พอร์ตที่กำหนดกลายเป็น Root Port
`spanning-tree bpduguard enable`	กำหนด BPDU Guard เพื่อปิดพอร์ตที่รับ BPDU ที่ไม่คาดหวัง
`spanning-tree portfast`	กำหนด PortFast สำหรับพอร์ตที่เชื่อมต่อกับอุปกรณ์ปลายทาง เพื่อเร่งกระบวนการเชื่อมต่อ
`spanning-tree mst portfast edge`	กำหนดพอร์ตให้เป็น Edge Port ใน MST (ระบุหมายเลข MST instance)

ตารางที่ 3 คำสั่งที่เกี่ยวข้องกับ STP บน

EtherChannel

EtherChannel เป็นเทคโนโลยีที่ช่วยในการรวมลิงก์หลายๆ ลิงก์เข้าเป็นลิงก์เดียว (Logical Link) เพื่อเพิ่มแบนด์วิดท์และเสริมความเสถียรในการเชื่อมต่อระหว่างอุปกรณ์เครือข่าย เช่น สวิตช์กับสวิตช์ หรือ สวิตช์กับเราเตอร์เมื่อใช้งาน EtherChannel, ลิงก์หลายเส้นจะถูกมองเป็นลิงก์เดียว (Logical Link) โดย STP ทำให้ STP มองเห็น EtherChannel เป็นพอร์ตเดียวในการคำนวณและกำหนดเส้นทาง ทำให้ลดจำนวนพอร์ตที่ STP ต้องจัดการและลดโอกาสในการเกิดลูป การรวมลิงก์เหล่านี้ทำให้สามารถใช้ลิงก์หลายเส้นพร้อมกันโดย ที่เครือข่ายยังคงมองเห็นเป็นลิงก์เดียว ซึ่งช่วยเพิ่มความเร็วในการรับส่งข้อมูลและลดปัญหาจากการที่ลิงก์ใดลิงก์หนึ่งมีปัญหา (Link Redundancy)

การทำงานของ EtherChannel

- EtherChannel สามารถทำงานได้ทั้งในโหมด Static (กำหนดเอง) และ Dynamic (อัตโนมัติ) โดยใช้ โปรโตคอลช่วยในการจัดการ
- PAgP (Port Aggregation Protocol): โปรโตคอลที่ใช้โดย Cisco สำหรับการสร้าง EtherChannel โดยจะเจรจาและกำหนดค่าลิงก์ระหว่างสวิตช์
- LACP (Link Aggregation Control Protocol): โปรโตคอลมาตรฐาน IEEE 802.3ad ที่ใช้ในการสร้าง EtherChannel โดยสามารถใช้งานกับอุปกรณ์เครือข่ายจากผู้ผลิตต่างๆ ได้

Routing Protocol

Routing เป็นกระบวนการที่เราเตอร์ใช้ในการส่งต่อแพ็กเกจจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง โดยมีวิธีการกำหนดเส้นทางอยู่สองประเภทหลักๆคือ Static Routing และ Dynamic Routing

Static Route

Static Route คือการกำหนดเส้นทางในเครือข่ายโดยการตั้งค่าที่ชัดเจนและตายตัว โดยผู้ดูแลระบบเครือข่ายจะกำหนดเส้นทางนี้เพื่อให้แน่ใจว่าแพ็กเก็ตจะถูกส่งไปยังปลายทางผ่านเส้นทางที่กำหนดไว้

การกำหนดค่า Static Route บนอุปกรณ์ Cisco

การกำหนดค่า Static Route บน Cisco Router สามารถทำได้ด้วยคำสั่ง ip route ซึ่งจะกำหนดเส้นทางไปยังเครือข่ายปลายทาง (destination network) โดยใช้ next-hop IP address หรือ exit interface

Dynamic Routing

Dynamic Routing คือกระบวนการที่อุปกรณ์เครือข่ายเช่น Router ใช้โปรโตคอลเพื่อแลกเปลี่ยนข้อมูลเส้นทางในเครือข่ายอัตโนมัติ โดยอุปกรณ์เหล่านี้จะแชร์ข้อมูลเกี่ยวกับเส้นทางในเครือข่ายเพื่อให้สามารถ เลือกเส้นทางที่เหมาะสมสำหรับการส่งข้อมูลไปยังปลายทางได้

IGP (interior Gateway Protocol)

IGP คือโปรโตคอลการเรียนรู้เส้นทางที่ใช้อยู่ภายในเครือข่ายเดียวกัน ซึ่งมีหน้าที่ในการกำหนดเส้นทาง ภายในเครือข่ายและควบคุมการส่งข้อมูลในเครือข่ายดังนั้นจะมีการใช้งานอยู่ในโปรโตคอลดังนี้

- RIP (Routing Information Protocol) โปรโตคอลที่ใช้วิธีการนับจำนวนกระโดด (hop count) ในการเลือกเส้นทางที่ดีที่สุด

การกำหนดค่า RIP

1. เลือกระบุเวอร์ชันของ RIP ที่ใช้ (Version 1 หรือ Version 2)
2. ระบุเครือข่ายที่เป็น RIP networks ที่ต้องการให้เรียนรู้เส้นทาง
3. กำหนดให้แนวทางเป็น passively เพื่อไม่ให้ส่งข้อมูล RIP ผ่าน interface นั้น

```
router rip
version 2
network <network-address>
passive-interface <interface>
```

- EIGRP (Enhanced Interior Gateway Routing Protocol) โปรโตคอลที่เป็นเอกสารผสมระหว่าง Distance Vector และ Link-State และเน้นความเร็วในการเรียนรู้เส้นทาง

การกำหนดค่า EIGRP

1. ระบุ Autonomous System (AS) number ที่ใช้กับ EIGRP
2. ระบุเครือข่ายที่ต้องการให้ EIGRP ใช้เรียนรู้เส้นทาง
3. กำหนดให้แนวทางเป็น passively เพื่อไม่ให้ส่งข้อมูล EIGRP ผ่าน interface นั้น
4. ตั้งค่า metrics เช่น bandwidth, delay, reliability เพื่อใช้ในการคำนวณเส้นทางที่เหมาะสม
5. กำหนดการกระจายเส้นทางจากโปรโตคอลอื่นเข้ามาใน EIGRP

```
router eigrp <AS-number>
network <network-address>
passive-interface <interface>
```

- OSPF (Open Shortest Path First) โปรโตคอลที่ใช้วิธีการคำนวณเส้นทางที่สั้นที่สุดโดยใช้ Dijkstra's algorithm

การกำหนดค่า OSPF

1. กำหนดเขต (Area) ใน OSPF เพื่อแบ่งเครือข่ายเป็นพื้นที่ต่างๆ
2. ระบุเครือข่ายที่ต้องการให้ OSPF ใช้เรียนรู้เส้นทาง
3. กำหนด Router ID สำหรับตัวเราใน OSPF
4. กำหนดประเภทของเขต OSPF เช่น Backbone Area, Stub Area, Not-So-Stubby Area (NSSA) ฯลฯ
5. ตั้งค่าการตรวจสอบความถูกต้อง (Authentication) เครือข่าย OSPF

```
router ospf <process-id>
network <network-address> <wildcard-mask> area <area-id>
passive-interface <interface>
```

EGP (Exterior Gateway Protocol)

EGP คือโปรโตคอลการเรียนรู้เส้นทางที่ใช้อยู่ระหว่างเครือข่ายหรือ AS (Autonomous Systems) ต่างๆ โดยใช้โปรโตคอลหลักคือ BGP (Border Gateway Protocol) ซึ่งมีหน้าที่ในการกำหนดเส้นทางระหว่าง AS และควบคุมการส่งข้อมูลข้าม AS ดังนั้นจะมีการใช้งานอยู่ในโปรโตคอลดังนี้

- BGP (Border Gateway Protocol) เป็นโปรโตคอลในการสื่อสารระหว่างเครือข่ายขนาดใหญ่ โดยเฉพาะเครือข่าย ISP (Internet Service Provider) และองค์กรขนาดใหญ่ โปรโตคอล BGP มี ลักษณะเป็นโปรโตคอล Path Vector ซึ่งหมายความว่า BGP ไม่เพียงแค่ระบุเส้นทางที่ดีที่สุด แต่ยังให้ ข้อมูลเพิ่มเติมเกี่ยวกับเส้นทาง เช่น ข้อมูลเริ่มต้นของเส้นทาง, AS-PATH (Autonomous System Path), NEXT-HOP และการเลือกเส้นทางตามนโยบายการเชื่อมต่อ (Policy-based routing) โดย BGP มีการใช้ AS Number เพื่อระบุเครือข่ายอิสระที่ไม่สามารถถูกแบ่งออกเป็นเครือข่ายย่อยได้

การกำหนดค่า BGP

1. กำหนด IP address ของ BGP neighbor เพื่อเชื่อมต่อและแลกเปลี่ยนข้อมูล BGP
2. ระบุ Autonomous System (AS) number ของตัวเอง
3. ระบุเครือข่ายที่ต้องการแจกจ่ายข้อมูล BGP
4. กำหนดนโยบายในการกรองข้อมูล BGP ที่จะรับหรือส่ง
5. ระบุเส้นทางหรือ prefixes ที่ต้องการแจกจ่ายหรือรับรู้

```
router bgp <AS-number>
neighbor <neighbor-IP> remote-as <neighbor-AS>
network <network-address>
```

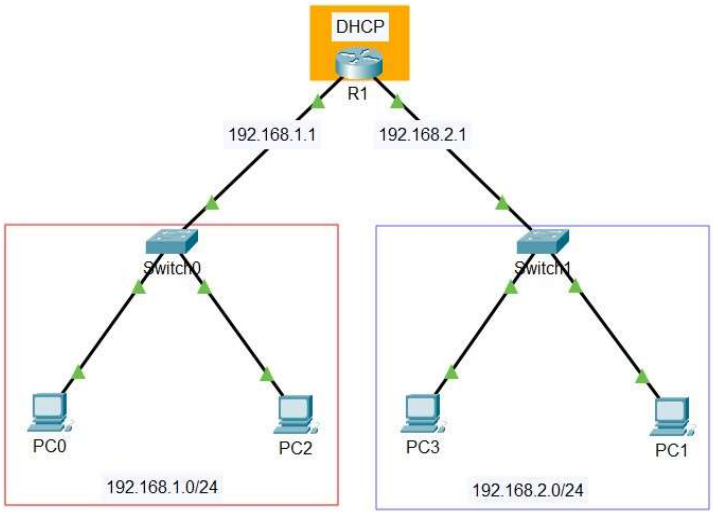
Redistribute

Redistribute เป็นกระบวนการในการนำเส้นทางหรือข้อมูลเครือข่ายจากโปรโตคอลหรือโปรโตคอล อื่นๆ มาแจกจ่ายหรือใช้ในโปรโตคอลอื่น เช่น การใช้ข้อมูลจาก RIP และ EIGRP ใน BGP หรือการใช้ข้อมูลจาก OSPF ใน EIGRP

DHCP (Dynamic Host Configuration Protocol)

DHCP เป็นโปรโตคอลที่ช่วยให้อุปกรณ์เครือข่ายที่เชื่อมต่อกับโครงข่ายได้รับการกำหนดค่า IP Address, Subnet Mask, Default Gateway, DNS Server และอื่นๆ โดยอัตโนมัติจากเซิร์ฟเวอร์ DHCP โดย ไม่ต้องกำหนดค่าด้วยตนเอง เมื่ออุปกรณ์เครือข่ายเชื่อมต่อกับโครงข่ายหรือเปิดเครื่องขึ้นมา จะส่งข้อความ DHCP Discover ไปยังเซิร์ฟเวอร์ DHCP ซึ่งเป็นการขอข้อมูลการกำหนดค่า จากนั้นเซิร์ฟเวอร์ DHCP จะตอบ กลับด้วยข้อมูลการกำหนดค่า DHCP Offer และอุปกรณ์เครือข่ายจะขอข้อมูลการกำหนดค่าด้วย DHCP Request และเซิร์ฟเวอร์ DHCP จะส่งข้อมูลการกำหนดค่า DHCP Acknowledge กลับไป บนเซิร์ฟเวอร์ DHCP ใช้คำสั่ง dhcpd และบนอุปกรณ์เครือข่ายใช้คำสั่ง ip dhcp

ตัวอย่างการใช้ DHCP บน Router



รูปภาพที่ 17 จำลองการทำ DHCP

ชื่ออุปกรณ์	คำสั่ง
R1	ip dhcp excluded-address 192.168.1.253 192.168.1.254 ip dhcp excluded-address 192.168.2.253 192.168.2.254 ip dhcp excluded-address 192.168.1.1 192.168.1.50 ip dhcp excluded-address 192.168.2.1 192.168.2.50

	ip dhcp pool LanA network 192.168.1.0 255.255.255.0 default-router 192.168.1.254 dns-server 192.168.1.253 ip dhcp pool LanB network 192.168.2.0 255.255.255.0 default-router 192.168.2.254 dns-server 192.168.1.253 interface FastEthernet0/0 ip address 192.168.1.254 255.255.255.0 interface FastEthernet1/0 ip address 192.168.2.254 255.255.255.0
PC (ทั้งหมด)	Ipconfig /renew

ตารางที่ 4 การกำหนดค่า DHCP ตามภาพที่ 17

DNS (Domain Name System)

DNS เป็นโปรโตคอลที่แปลงชื่อโดเมน (Domain Name) เป็นที่อยู่ IP (Internet Protocol) เพื่อให้ เครื่องคอมพิวเตอร์สามารถระบุและเชื่อมต่อกับเว็บไซต์ แอปพลิเคชัน หรือเครือข่ายอื่นๆที่ใช้ชื่อโดเมนเป็นตัวบ่งชี้เมื่อมีคำขอการแปลงชื่อโดเมนเป็นที่อยู่ IP ส่งเข้ามาที่เซิร์ฟเวอร์ DNS โดยเซิร์ฟเวอร์ DNS จะตอบกลับด้วยที่อยู่ IP ที่เกี่ยวข้องกับชื่อโดเมนนั้น บนเซิร์ฟเวอร์ DNS ใช้คำสั่ง named และบนเครื่องคอมพิวเตอร์ใช้คำสั่ง nslookup หรือ dig ในการตรวจสอบการแปลงชื่อโดเมน

FHRP

First Hop Redundancy Protocol (FHRP) เป็นโปรโตคอลที่ใช้ในเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่เป็นข้อมูลสำรองสำหรับเกตเวย์เริ่มต้นบนเครือข่ายย่อย เกตเวย์เริ่มต้นคือเราเตอร์ที่เชื่อมต่อเครือข่ายย่อยกับเครือข่ายอื่น เช่น อินเทอร์เน็ต ในกรณีที่เกตเวย์เริ่มต้นล้มเหลวเครือข่ายย่อยจะสูญเสียการเชื่อมต่อกับเครือข่ายอื่น ซึ่งทำให้เกิดการหยุดชะงักและการหยุดทำงานของเครือข่ายเพิ่มเติม

เพื่อหลีกเลี่ยงปัญหานี้ FHRP จะอนุญาตให้เราเตอร์หลายตัวแชร์ IP เสมือนเดียวและที่อยู่ MAC เสมือนซึ่งทำ หน้าที่เป็นเกตเวย์เริ่มต้นสำหรับโฮสต์ภายในเครือข่ายย่อยการรับส่งข้อมูลทั้งหมดที่เข้าและออกจากเครือข่ายย่อยจะถูกส่งผ่านหนึ่งในเราเตอร์เหล่านี้ ซึ่งระบุว่าเป็นเราเตอร์ที่ใช้งานอยู่เราเตอร์อื่นๆ เป็นตัวสำรองข้อมูลที่ คอยจับตาดูเราเตอร์หลักเพื่อเข้าควบคุมหากจำเป็น

ประเภทของ First Hop Redundancy Protocol (FHRP)

- Hot Standby Router Protocol (HSRP)

- มาตรฐานเริ่มต้นและเป็นกรรมสิทธิ์ของ Cisco – Virtual Router Redundancy Protocol (VRRP)
- โปรโตคอลมาตรฐานแบบเปิด – Gateway Load Balancing Protocol (GLBP) – มาตรฐานที่เป็นกรรมสิทธิ์ล่าสุดจาก Cisco ที่ อนุญาตให้มีการทำโหลดบาลานซ์

HSRP

Hot Standby Router Protocol หรือ HSRP เป็นโปรโตคอลสำรองเราเตอร์ที่เป็นกรรมสิทธิ์ของ Cisco ซึ่งช่วยให้กลุ่มเราเตอร์ทำงานร่วมกันเพื่อให้มีเครือข่ายสำรองได้ เราเตอร์ทั้งหมดภายในกลุ่มจะมีที่อยู่ IP เสมือนและที่อยู่ Mac เสมือนเดียวกัน

สถานะของเราเตอร์ทั้งสองของ Hot Standby Router Protocol (HSRP) คือ

- Active Router: เราเตอร์ที่ใช้งานอยู่(ค่าเริ่มต้น) ส่งและรับแพ็กเก็ตไปยังโฮสต์ภายในองค์กรคือเราเตอร์เกตเวย์เริ่มต้น จากกลุ่มของเราเตอร์ มีเพียงตัวเดียวเท่านั้นที่ถูกเลือกให้เป็นเราเตอร์ที่ใช้งานอยู่
- Standby Router: เราเตอร์ที่ในกรณีที่เราเตอร์ที่ใช้งานอยู่ในปัจจุบันออฟไลน์ ในบรรดาเรา เตอร์สแตนด์บายจะถูกเลือกให้เป็นเราเตอร์ที่ใช้งานอยู่
- คุณสมบัติ HSRP
- แลกเปลี่ยน Hello messages ทุกๆ 3 วินาที
- IP แบบหลายผู้รับสำหรับ HSRP เวอร์ชัน 1 = 224.0.0.2
- IP แบบหลายผู้รับสำหรับ HSRP เวอร์ชัน 2 = 224.0.0.102
- หมายเลขพอร์ต UDP = 1985 – หมายเลขกลุ่ม = 0-255
- ลำดับความสำคัญเริ่มต้นคือ 100 และช่วงคือ 0-255
- การเลือกเราเตอร์ที่ใช้งานอยู่ 35
- ลำดับความสำคัญสูงสุด
- หากลำดับความสำคัญเท่ากัน ที่อยู่ IP สูงสุดที่กำหนดค่าไว้บนอินเทอร์เฟซ
- ที่อยู่ MAC เสมือนของ HSRP คือ 0000.0c07.acxx

คำสั่ง	คำอธิบาย
`standby <group-number> ip <virtual-ip>`	กำหนด Virtual IP Address (VIP) สำหรับ HSRP
`standby <group-number> priority <priority>`	กำหนด Priority ของ HSRP

`Standby <group-number> preempt`	เปิดใช้ Preemption ให้หน่วยควบคุมหลักสามารถกลับมา ทำหน้าที่หลักได้หลังจากกลับมาทำหน้าที่สำรอง

ตารางที่ 5 การกำหนดค่า HSRP

VRRP

VRRP ย่อมาจากVirtual Router Redundancy Protocol เป็นโปรโตคอลสำรองที่เป็นกลางของผู้ขายที่จัดกลุ่มเราเตอร์ตั้งแต่สองตัวขึ้นไปเพื่อสร้างเราเตอร์เสมือนตัวเดียวใหม่ ช่วยให้มีความซ้ำซ้อนโดยการกำหนดที่อยู่ IP เกตเวย์เสมือนและที่อยู่ MAC เดียวกันให้กับเราเตอร์ทางกายภาพทั้งหมดในกลุ่ม VRRP

ปัจจุบัน VRRP อยู่ที่เวอร์ชัน 2 เกือบจะเป็นแนวคิดเดียวกับ HSRP ข้อแตกต่างเพียงอย่างเดียวคือบน VRRP การจองจะถูกเปิดใช้งานตามค่าเริ่มต้น ในขณะที่ HSRP จะต้องกำหนดค่าด้วยตนเอง

Virtual Router Redundancy Protocol (VRRP) สองสถานะคือ

- Master Router ปัจจุบันเป็นเกตเวย์เริ่มต้นขององค์กรสำหรับโฮสต์ทั้งหมดมีการส่งและรับแพ็กเก็ต เข้าและออกจากโฮสต์อย่างต่อเนื่อง
- Backup Router ในระหว่างที่เกิดข้อผิดพลาดหรือเมื่อเราเตอร์หลักออฟไลน์ เราเตอร์สำรองจะเข้ามาแทนที่เป็นเราเตอร์หลัก

การกำหนดค่า VRRP

คำสั่ง	คำอธิบาย
`vrrp <group-number> ip <virtual-ip>`	กำหนด Virtual IP Address (VIP) สำหรับ VRRP
`vrrp <group-number> priority <priority>`	กำหนด Priority ของ VRRP (ค่ามากสุดคือหน่วยควบคุมหลัก)
`vrrp <group-number> preempt`	เปิดใช้ Preemption ให้หน่วยควบคุมหลักสามารถกลับมาทำหน้าที่หลักได้หลังจากกลับมาทำหน้าที่สำรอง
`vrrp <group-number> track <interface> <decrement>`	กำหนดการตรวจสอบสถานะของ Interface และลด Priority ของ VRRP หาก Interface ดังกล่าวล่ม

ตารางที่ 6 การกำหนดค่า VRRP

GLBP

GLBP ย่อมาจาก Gateway Load Balancing Protocol ช่วยป้องกันความล้มเหลวจุดเดียว เช่น HSRP และ VRRP ถึงกระนั้นมันยังอนุญาตให้มีการแบ่งปันโหลดระหว่างกลุ่มของเราเตอร์ที่ซ้ำซ้อนเพื่อให้เราเตอร์ทั้งหมดมีส่วนร่วมในการส่งต่อแพ็กเก็ตและไม่มีการอัปลิงค์ใดที่จะไม่ถูกใช้งาน นี่เป็นคุณสมบัติเพิ่มเติมของโปรโตคอล GLBP ที่มีความซ้ำซ้อน

การดำเนินงานของ GLBP

- เราเตอร์ทั้งหมดที่เข้าร่วม GLBP จะรวมกลุ่มกัน หลังจากนั้นพวกเขาเลือกเราเตอร์หนึ่งตัวเพื่อทำหน้าที่เป็น AVG (เกตเวย์เสมือนที่ใช้งานอยู่) ของกลุ่ม
- สมาชิกคนอื่นๆ ในกลุ่มจะทำหน้าที่เป็นตัวสำรองสำหรับ AVG หากล้มเหลว
- AVG สามารถควบคุมสมาชิกกลุ่มทั้งหมดโดยกำหนดที่อยู่ MAC เสมือนให้กับแต่ละคน
- เราเตอร์แต่ละตัวมีหน้าที่รับผิดชอบในการส่งต่อแพ็กเก็ตที่ส่งไปยังที่อยู่ MAC เสมือนที่กำหนดโดย AVG
- สำหรับที่อยู่ MAC เสมือน เราเตอร์เหล่านี้เรียกว่า AVF (ตัวส่งต่อเสมือนที่ใช้งานอยู่)
- คำขอ ARP (Address Resolution Protocol)สำหรับที่อยู่ IP เสมือนได้รับการจัดการโดย AVG เช่นกัน สิ่งนี้มีความสำคัญอย่างยิ่งต่อการดำเนินงาน GLBP เนื่องจาก AVG ตอบสนองต่อคำขอ ARP จากโฮสต์ที่แตกต่างกันด้วยที่อยู่ MAC เสมือนที่แตกต่างกัน
- เมื่อไคลเอนต์ร้องขอที่อยู่ IP ของเกตเวย์เริ่มต้นผ่าน ARP AVG จะตอบกลับด้วยที่อยู่ MAC เสมือนของ AVF ตัวใดตัวหนึ่ง 38
- เมื่อไคลเอนต์อื่นส่งข้อความ ARP เพื่อแก้ไขที่อยู่เกตเวย์เริ่มต้น AVG จะตอบกลับด้วยที่อยู่ MAC เสมือนของ AVF ถัดไป เป็นผลให้ไคลเอนต์แต่ละรายได้รับที่อยู่ MAC เสมือนที่ไม่ซ้ำกันสำหรับที่อยู่ IP เสมือนเดียวกันกับเกตเวย์เริ่มต้น
- ด้วยเหตุนี้ แม้ว่าจะมีการกำหนดค่าเกตเวย์เริ่มต้นเหมือนกัน แต่ไคลเอ็นต์แต่ละเครื่องจะส่งการรับส่ง ข้อมูลไปยังเราเตอร์ที่แตกต่างกัน

คุณสมบัติ GLBP

- GLBP เป็นโปรโตคอลที่เป็นกรรมสิทธิ์ของ Cisco ซึ่งเปิดตัวในซอฟต์แวร์ Cisco IOSรุ่น 12.2(14) สำหรับเราเตอร์
- เราเตอร์ทั้งหมดในกลุ่มส่งต่อข้อมูล
- AVG (Active Virtual Gateway) ถูกกำหนดให้กับหนึ่งในเราเตอร์ในกลุ่ม
- เราเตอร์ที่มีลำดับความสำคัญสูงสุด

- หากลำดับความสำคัญเท่ากัน ที่อยู่ IP สูงสุดที่กำหนดค่าไว้บนอินเทอร์เฟซ
- จำนวน MAC เสมือนสูงสุดที่รองรับต่อกลุ่ม = 4
- หมายเลขกลุ่ม GLBP = 0 –1023
- ค่าลำดับความสำคัญ= 1-255
- สวัสดี Timer = 3 วินาที, Dead Timer = 10 วินาที
- ที่อยู่ IP แบบหลายผู้รับ=224.0.0.102
- ที่อยู่ MAC เสมือน = 0007.b4xx.xxyy

การกำหนดค่า GLBP

คำสั่ง	คำอธิบาย
`glbp <group-number> ip <virtual-ip>`	กำหนด Virtual IP Address (VIP) สำหรับ GLBP
`glbp <group-number> priority <priority>`	กำหนด Priority ของ GLBP (ค่ามากสุดคือหน่วยควบคุมหลัก)
`glbp <group-number> preempt`	เปิดใช้ Preemption ให้หน่วยควบคุมหลักสามารถ กลับมาทำหน้าที่หลักได้หลังจากกลับมาทำหน้าที่ สำรอง
`glbp <group-number> load-balancing <method>`	เลือกวิธีการ Load Balancing (Round-Robin, Host-Dependent, หรือ Weighted)
`glbp <group-number> track <interface> <decrement>`	กำหนดการตรวจสอบสถานะของ Interface และลด Priority ของ GLBP หาก Interface ดังกล่าวล่ม

ตารางที่ 7 การกำหนดค่า GLBP

Access control List (ACL)

Access Control List (ACL) คือกลไกการควบคุมที่ใช้ในเราเตอร์หรือสวิตช์ เพื่อกำหนดเงื่อนไขในการ อนุญาตหรือปฏิเสธการเข้าถึงทรัพยากรเครือข่าย ACL ช่วยในการควบคุมการไหลของข้อมูลเครือข่ายและเสริม ความปลอดภัย

ประเภทของ ACL

1. Standard ACL
    a. สนใจเฉพาะ Source IP Address เท่านั้น
    b. เหมาะสำหรับการควบคุมที่ไม่ต้องการความละเอียดสูง

2. Extended ACL
    a. สนใจทั้ง Source และ Destination IP Address
    b. สามารถระบุ Protocol และ Application ได้
    c. มีความละเอียดและความยืดหยุ่นสูงกว่า Standard ACL

วิธีการ Config ACL บน Router Cisco

1. Numbered ACLs ใช้หมายเลขในการกำหนด ACL – Standard ACL: หมายเลข 1 - 99 – Extended ACL: หมายเลข 100 - 199
2. Named ACLs ใช้ชื่อในการกำหนด ACL ให้ความยืดหยุ่นในการตั้งชื่อเงื่อนไข

NAT

NAT (Network Address Translation) เป็นกระบวนการที่ช่วยแปลง IP Address ในแพ็กเก็ตข้อมูลที่ส่งผ่านเราเตอร์หรือไฟร์วอลล์ NAT ช่วยให้สามารถใช้ IP Address ภายในเครือข่ายท้องถิ่น (Private IP Address) ร่วมกับ IP Address สาธารณะ (Public IP Address) เพื่อเข้าถึงอินเทอร์เน็ตหรือติดต่อกับ เครือข่ายอื่นๆ

ประเภทของ NAT

1. **Static NAT**
    - Static NAT หรือการแปลง IP Address แบบคงที่ เป็นการกำหนดการแปลง IP Address ภายใน (Private IP Address) ให้กับ IP Address ภายนอก (Public IP Address) แบบหนึ่งต่อหนึ่ง เหมาะสำหรับอุปกรณ์ที่ต้องการการเข้าถึงจากภายนอก เช่น เว็บเซิร์ฟเวอร์ หรืออีเมลเซิร์ฟเวอร์
2. **Dynamic NAT**
    - Dynamic NAT หรือการแปลง IP Address แบบไดนามิก เป็นการแปลง IP Address ภายในไปเป็น IP Address ภายนอกจากพูลของ IP Address ที่กำหนด เหมาะสำหรับเครือข่ายที่มีการใช้งาน IP Address ภายนอกหลายตัวและไม่ต้องการแปลงแบบคงที่
3. **PAT**
    - PAT หรือที่เรียกว่า NAT Overload เป็นการแปลง IP Address แบบหลายต่อหนึ่ง (many to-one) โดยการใช้หมายเลขพอร์ต (Port Number) เพื่อแยกแยะการเชื่อมต่อแต่ละอัน เหมาะสำหรับการแปลง IP Address ภายในหลายตัวไปเป็น IP Address ภายนอกเพียงตัวเดียว

IPsec (Internet Protocol Security)

IPsec เป็นชุดโปรโตคอลที่ช่วยให้การรับส่งข้อมูลผ่านเครือข่ายมีความปลอดภัยโดยการเข้ารหัสข้อมูล และการยืนยันตัวตน IPsec มักถูกใช้ใน VPN (Virtual Private Network) เพื่อสร้างการเชื่อมต่อที่ปลอดภัย ระหว่างสองเครือข่ายผ่านอินเทอร์เน็ต

ฟังก์ชันหลักของ IPsec

- Authentication Header (AH): ให้การยืนยันความถูกต้องของแพ็กเก็ตโดยการตรวจสอบความสมบูรณ์ของข้อมูล
- Encapsulating Security Payload (ESP): ให้การเข้ารหัสข้อมูลและการยืนยันความถูกต้องของแพ็ก เก็ต
- Internet Key Exchange (IKE): ใช้ในการสร้างและจัดการกุญแจเข้ารหัส

การกำหนดค่า IPsec บน Cisco Router

1. กำหนดการเชื่อมต่อ ISAKMP

```
Router(config)# cryto isakmp policy 10
Router(config-isakmp)# encryption aes
Router(config-isakmp)# hash sha256
Router(config-isakmp)# authentication pre-share
Router(config-isakmp)# group 14
```

2. กำหนดกุญแจการแชร์ล่วงหน้า (Pre-Shared Key)

```
Router(config)# crypto isakmp key <key> address <peer-ip>
```

3. กำหนดการตั้งค่า IPsec Transform Set

```
Router(config)# crypto ipsec transform-set MY_TRANSFORM_SET esp-
aes esp-sha-hmac
```

4. กำหนด Crypto Map

```
Router(config)# crypto map MY_CRYPTO_MAP 10 ipsec-isakmp
Router(config-crypto-map)# set peer <peer-ip>
Router(config-crypto-map)# set transform-set MY_TRANSFORM_SET
Router(config-crypto-map)# match address <access-list-number>
```

5. ประยุกต์ใช้ Crypto Map บน Interface

```
Router(config)# interface g0/1
Router(config)# crypto map MY_CRYPTO_MAP
```

GRE Tunnel

GRE (Generic Routing Encapsulation) เป็นโปรโตคอลการห่อหุ้มที่ใช้สำหรับสร้างการเชื่อมต่อแบบ Tunnel ระหว่างสองอุปกรณ์เครือข่าย GRE ช่วยให้สามารถส่งแพ็กเก็ตของโปรโตคอลที่แตกต่างกันภายในแพ็กเก็ต IP ได้

ฟังก์ชันหลักของ GRE

- การห่อหุ้ม (Encapsulation) ห่อหุ้มแพ็กเก็ตที่หลากหลายรวมถึง IP, IPX และ AppleTalk ภายใน แพ็กเก็ต IP
- การสร้าง Tunnel สร้างการเชื่อมต่อระหว่างสองอุปกรณ์เครือข่ายที่อยู่ห่างกัน

การกำหนดค่า GRE Tunnel บน Cisco Router

1. สร้างอินเทอร์เฟซ Tunnel

```
Router(config)# interface Tunnel 0
Router(config-if)# ip address 10.0.0.1 255.255.255.252
Router(config-if)# tunnel source g0/1
Router(config-if)# tunnel destination <peer-ip>
```

2. กำหนดเส้นทางสำหรับ Tunnel

```
Router(config)# ip route <remote-network> <subnet-mask> 10.0.0.2
```

IPv6 Translation and Tunneling Teachnologies

1. Dual Stack
   - วิธีนี้เป็นการติดตั้งทั้ง **IPv4** และ **IPv6** บนโครงสร้างเครือข่ายเดียวกัน ซึ่งช่วยให้เครื่องลูกข่ายสามารถใช้ทั้งสองโปรโตคอลได้ ง่ายต่อการบริหารจัดการ ช่วยให้การสื่อสารระหว่างโปรโตคอลเป็นไปได้ คำสั่งตัวอย่าง

```
interface GigabitEthernet0/0
ip address 192.0.2.1 255.255.255.0
ipv6 address 2001:db8::1/64
```

2. Tunneling
   - การห่อหุ้มแพ็กเก็ต IPv6 ภายในแพ็กเก็ต IPv4 เพื่อส่งผ่านเครือข่ายที่ยังไม่รองรับ IPv6 การใช้วิธีนี้เหมาะกับสถานการณ์ที่ยังไม่สามารถอัพเกรดโครงสร้างเครือข่ายทั้งหมดให้รองรับ IPv6 ได้ทันที

   ประเภทของ Tunneling

   1. 6to4 Tunnel: ใช้สำหรับการเชื่อมต่อ IPv6 ผ่านเครือข่าย IPv4 โดยไม่ต้องมีการตั้งค่า manual
   2. Manual Tunnel (GRE, IPIP): ต้องการการตั้งค่า manual แต่มีความยืดหยุ่นสูง

3. Translation
   - ใช้การแปลงแพ็กเก็ตจาก IPv6 เป็น IPv4 หรือจาก IPv4 เป็น IPv6 เพื่อให้การสื่อสารระหว่างโปรโตคอลเป็นไปได้ ช่วยให้เครื่องลูกข่าย IPv6 สามารถเข้าถึงทรัพยากรที่อยู่บน IPv4 ได้

ประเภทของ Translation

1. NAT64 แปลงจาก IPv6 เป็น IPv4
2. DNS64 ใช้กับ NAT64 เพื่อให้ชื่อโดเมน IPv6 ถูกแปลงเป็นที่อยู่ IPv4

คำสั่งตัวอย่าง

```
ipv6 nat64 prefix stateful 64:ff9b::/96
interface GigabitEthernet0/0
ip address 192.0.2.1 255.255.255.0
ipv6 address 2001:db8::1/64
```

บทที่ 3
สรุปผลการศึกษาหรือผลการปฏิบัติงาน

3.1 สรุปละวิเคราะห์ผลการปฏิบัติงาน

จากการเป็นนักศึกษาฝึกงานที่ได้รับการฝึกงานกับ บริษัท ยิบอินซอย จำกัด ข้าพเจ้าได้รับความรู้ความเข้าใจและประสบการณ์ในการทำงานจริงร่วมกับทีมพี่เลี้ยงวิศวกร การทำงานตามหัวข้อ และการวางแผนเพื่อทำให้งานที่ดีรับมอบหมายสำเร็จลุล่วงไปได้ด้วยดีตามจุดประสงค์ที่ตั้งไว้ ฝึกการทำงานเป็นทีมไม่ว่าจะเป็นคนช่วงวัยเดียวกันหรือคนต่างช่วงวัยอย่างราบรื่นรวมถึงการวางตัวเมื่ออยู่ร่วมกับผู้อื่น ความรู้เรื่องเครือข่าย อุปกรณ์เครือข่าย และการตั้งค่าการใช้งานอุปกรณ์ต่างๆรวมถึงซอฟแวร์ที่ใช้งานด้วย

3.2 ความรู้และประสบการณ์ที่ได้จากการฝึกงาน

3.2.1 ความรู้และความเข้าใจในอุปกรณ์ทางเครือข่ายโดยเฉพาะของ CISCO สามารถที่จะนำไปใช้งานได้อย่างถูกต้อง

3.2.2 ความรู้การออกแบบเครือข่ายให้เหมาะสมกับองค์กรแต่ละแบบ

3.2.3 การตั้งค่าอุปกรณ์เครือข่ายให้สามารถทำงานได้ เช่นการกำหนดไอพี หรือ การกำหนด โปรโตคอล

3.2.4 ประสบการณ์ทำงานร่วมกับคนในองค์กร

3.2.5 การทำงานให้สำเร็จลุล่วงตามระยะเวลาที่กำหนดอย่างราบรื่น

3.3 ปัญหาและอุปสรรคในการฝึกงาน

3.3.1 ความรู้ด้านพื้นฐานเกี่ยวกับระบบเครือข่ายไม่มากพอทำให้เสียเวลาในการทบทวนเนื้อหาจากเรื่องที่เรียนและต้องค้นหาข้อมูลเพิ่มเติมจากเรื่องที่ไม่รู้อีกเยอะพอสมควร ด้วยเหตุนี้จึงทำให้ระยะเวลาในการทำงานจริงๆน้อยลงไป หากมีเวลามากกว่านี้คาดว่าอาจจะได้รับประสบการณ์ทำงานที่มากกว่า

เอกสารอ้างอิง

CISCO Packet Tracer, เว็บไซต์ทางการของ CISCO ใช้ในการดาวน์โหลดโปรแกรมออกแบบเครือข่าย, สืบค้นวันที่ 14 เมษายน พ.ศ. 2567, จาก Cisco Packet Tracer - Networking Simulation Tool (netacad.com)

Netsarang, เว็บไซต์ทางการของ Netsarang Computer ใช้ในการดาวน์โหลดโปรแกรม Xshell, สืบค้นวันที่ 14 เมษายน พ.ศ. 2567, จาก XSHELL - The Industry's Most Powerful SSH Client (netsarang.com)

WENDELL ODOM, CCIE No. 1624 Emeritus (2020). Official Cert Guide Advance your IT career with hands-on learning CCNA 200-301 Volume 1. Cisco Press 221 River St. (3D11C) Hoboken, NJ 07030

WENDELL ODOM, CCIE No. 1624 Emeritus (2020). Official Cert Guide Advance your IT career with hands-on learning CCNA 200-301 Volume 2. Cisco Press 221 River St. (3D11C) Hoboken, NJ 07030