การทดสอบระบบการเชื่อมต่อเส้นทางอินเทอร์เน็ตสำรอง 3G/4G

TESTING 3G/4G INTERNET BACK-UP LINK

นางสาวฐิตาพร จุลเกษม

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีไทย-ญี่ปุ่น

พ.ศ. 2560

การทดสอบระบบการเชื่อมต่อเส้นทางอินเทอร์เน็ตสำรอง 3G/4G

TESTING 3G/4G INTERNET BACK-UP LINK

ฐิตาพร จุลเกษม

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย-ญี่ปุ่น
ปีการศึกษา 2560

คณะกรรมการสอบ

..... ประธานกรรมการสอบ
(อาจารย์ ชาญ จารุวงศ์รังสี)

..... กรรมการสอบ
(อาจารย์ ดร.สะพรั่งสิทธิ์ มฤทุสาธร)

..... อาจารย์ที่ปรึกษา
(อาจารย์ ดร.ปราณิสา อิศรเสนา)

..... ประธานสหกิจศึกษาสาขาวิชา
(อาจารย์ อมรพันธ์ ชมกลิ่น)

ชื่อโครงงาน	การทดสอบระบบการเชื่อมต่อเส้นทางอินเทอร์เน็ตสำรอง 3G/4G TESTING 3G/4G INTERNET BACK-UP LINK
ผู้เขียน	นางสาวฐิตาพร จุลเกษม
คณะวิชา	เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ
อาจารย์ที่ปรึกษา	อาจารย์ ดร.ปราณิสา อิศรเสนา
พนักงานที่ปรึกษา	คุณพลอยแก้ว เรืองศรีสิริ
ชื่อบริษัท	NTT Communications (Thailand) Co., Ltd
ประเภทธุรกิจ	Network service provider

บทสรุป

จากการที่ได้สหกิจศึกษา ณ ที่บริษัท NTT Communications (Thailand) Co., Ltd ได้รับหมายหมายให้ทำการทดสอบระบบการเชื่อมต่อเส้นทางอินเทอร์เน็ตสำรอง 3G/4G เพื่อทดสอบว่าเส้นทางการเชื่อมโยงของอินเทอร์เน็ตสามารถเชื่อมต่อกันได้อย่างถูกต้อง และเมื่อเส้นทางหลักในการใช้อินเทอร์เน็ตเกิดการขัดข้องจนไม่สามารถใช้อินเทอร์เน็ตได้แล้วเส้นทางสำรองที่สร้างขึ้นมาจะสามารถสับเปลี่ยนมาใช้เส้นทางสำรองอัตโนมัติเพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง และเมื่อเส้นทางหลักสามารถกลับมาใช้งานได้ก็จะสับเปลี่ยนเส้นทางการใช้อินเทอร์เน็ตกลับมาใช้เส้นทางหลักเหมือนเดิม โดยหน้าที่ที่ได้รับมอบหมายอันดับแรกคือการไปติดตั้งอุปกรณ์Routerที่ไซต์งานของลูกค้าเพื่อทำการวางเส้นทางสำรองการใช้อินเทอร์เน็ตให้กับลูกค้า หน้าที่อันดับสองที่ได้รับมอบหมายคือการทดสอบระบบว่าเส้นทางการเชื่อมต่อสำรองอินเทอร์เน็ตที่ทางNTT ได้นำไปติดตั้งที่ไซต์งานของลูกค้าสามารถทำงานได้จริงตามไดอาแกรมที่วางเอาไว้หรือไม่ เพื่อความสะดวกและความต่อเนื่องในการใช้งานของลูกค้า ซึ่งผลที่ได้คือ ลูกค้าพึงพอใจในการบริการการสร้างระบบการเชื่อมโยงเส้นทางอินเทอร์เน็ตสำรองด้วย 3G/4G รวมไปถึงบริการหลังการให้บริการให้คำปรึกษาและการแก้ไขปัญหาเกี่ยวกับบริการในครั้งนี้

กิตติกรรมประกาศ

ในการที่ข้าพเจ้าได้มาสหกิจ ณ บริษัท เอ็นทีที คอมมิวนิเคชั่นส์ (ประเทศไทย) จำกัด ตั้งแต่วันที่ 29 พฤษภาคม พ.ศ. 2560 ถึงวันที่ 18 สิงหาคม พ.ศ.2560 ได้ทำให้ข้าพเจ้าเรียนรู้ประสบการณ์ต่างๆ ความรู้จากการทำงานจริง ซึ่งมีค่าอย่างมากมาย และส่งผลให้ข้าพเจ้าสามารถนำสิ่งต่างๆ เหล่านั้น มาใช้ในการพัฒนาทักษะของตนเอง สำหรับรายงานการปฏิบัติงานสหกิจในครั้งนี้ สามารถสำเร็จลุล่วงได้ด้วยดีจากการร่วมมือและการสนับสนุนจากหลายฝ่ายดังนี้

1. คุณศานิต เกษมสันต์ ณ อยุธยา (ผู้อำนวยการฝ่ายผลิตภัณฑ์และการบริการ บริษัท เอ็นทีที คอมมิวนิเคชั่นส์ (ประเทศไทย) จำกัด) ที่เห็นความสำคัญของการสหกิจศึกษา และได้ให้โอกาสที่มีคุณค่ายิ่งแก่ข้าพเจ้าในการเข้ามาสหกิจศึกษาที่บริษัทแห่งนี้

2. คุณพลอยแก้ว เรืองศรีสิริ (Manager Product and Service Department และ พนักงานที่ปรึกษา) ที่ได้ให้ความกรุณารับข้าพเจ้าเข้ามาเป็นส่วนหนึ่งของแผนก Product and Service (PS) ในการปฏิบัติงานสหกิจศึกษาในครั้งนี้

3. คุณพงลดา ธรรมขันธ์ และ คุณอภิชาติ เลาพันธกิจ ที่ให้การดูแล ให้คำปรึกษาและคำแนะนำเกี่ยวกับความรู้หรือการทำงานต่างๆ

และทุกคนในแผนก Product and Service (PS) รวมถึงบุคลลท่านอื่นๆ ที่มิได้กล่าวนามได้ให้คำแนะนำช่วยเหลือในการปฏิบัติงานสหกิจและจัดทำรายงานฉบับนี้ให้สำเร็จลุล่วงไปด้วยดี ขอขอบคุณไว้ ณ ที่นี้

นางสาวฐิตาพร จุลเกษม

ผู้จัดทำ

สารบัญ

หน้า

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูปภาพ

สารบัญรูปภาพ (ต่อ)

ภาพที่ **หน้า**

สารบัญรูปภาพ (ต่อ)

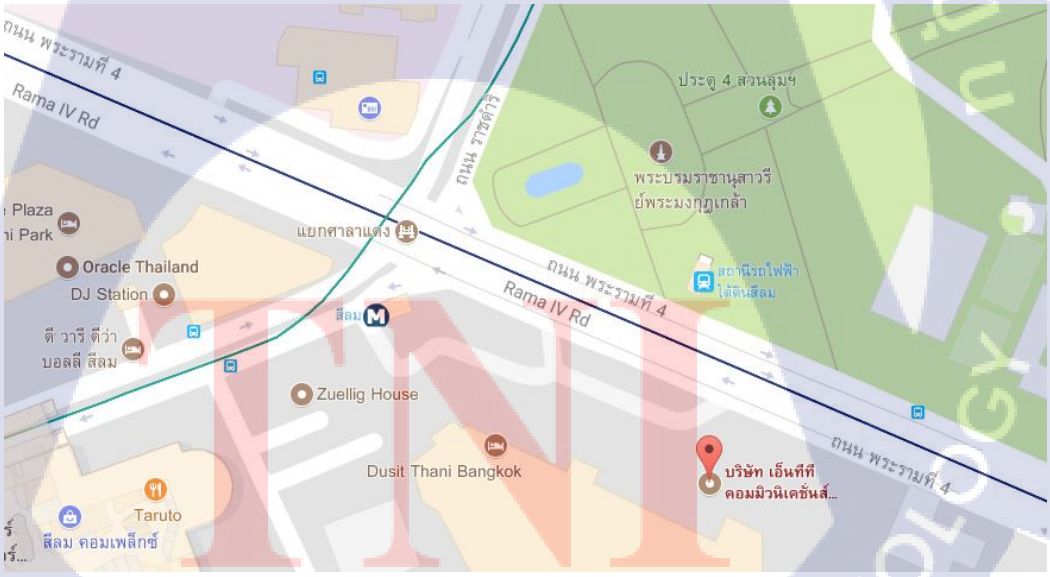
ภาพที่ **หน้า**

สารบัญรูปภาพ (ต่อ)

บทที่ 1
บทนำ

1.1 ชื่อและที่ตั้งของสถานประกอบการ

ชื่อสถานประกอบการ	:	บริษัท เอ็นทีที คอมมิวนิเคชั่นส์ (ประเทศไทย) จำกัด
ที่ตั้งสถานประกอบการ	:	946 ถนนพระราม 4 แขวงสีลม เขตบางรัก กทม. 10500
โทรศัพท์	:	0-2236-7227
โทรสาร	:	0-2236-6395



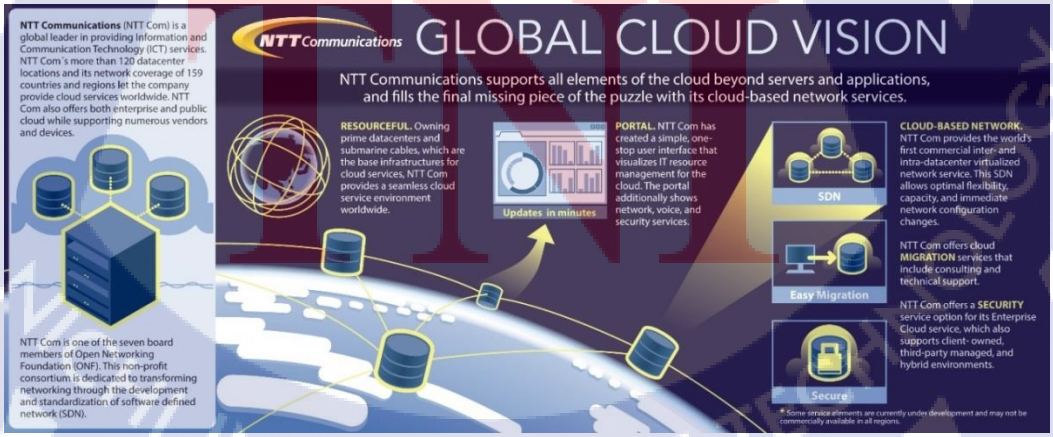
รูป 1.1 แผนที่ตั้ง บริษัท เอ็นทีที คอมมิวนิเคชั่นส์ (ประเทศไทย) จำกัด

1.2 ลักษณะธุรกิจของสถานประกอบการ หรือ การให้บริการหลักขององค์กร

เอ็นทีที คอมมิวนิเคชั่นส์ (ประเทศไทย) จำกัด คือ กลุ่มผู้นำในการให้บริการโซลูชั่นเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ระดับโลกและเป็นส่วนหนึ่งของ NTT Group ซึ่งเป็น บริษัท ที่ติดอันดับ 100 อันดับแรกใน Fortune Global 500 และเป็น บริษัทที่มีสาขาทั่วโลกในกว่า 120 เมืองในกว่า 40 ประเทศ / ภูมิภาคและการเชื่อมต่อเครือข่ายใน 196 ประเทศ

รูปที่ 1.2 แผนผังบริษัท NTT Communication (Thailand) Co., Ltd

NTT Communications เป็น บริษัทระหว่างประเทศที่ให้บริการและโซลูชั่นแก่ลูกค้าระดับองค์กรในระดับโลกและเราเป็นผู้นำด้านการให้บริการระบบคลาวด์เครือข่ายและข้อมูลเราใช้โครงสร้างพื้นฐานที่มีความปลอดภัย วิสัยทัศน์ที่ก้าวล้ำ และประวัติศาสตร์อันยาวนานของความสำเร็จเพื่อเสนอโซลูชั่นที่ดีที่สุดในหลายประเภท ด้วยเทคโนโลยีชั้นนำในอุตสาหกรรมและแนวคิดที่ก้าวหน้าเราเป็นพันธมิตรที่ดีที่สุดของคุณสำหรับโซลูชั่นการแก้ปัญหาด้านข้อมูลและการสื่อสารแบบปลายด้าน (ICT)



รูปที่ 1.3 Global Cloud Vision

ทาง NTT Communications ที่ให้บริการระดับโลกเพื่อช่วยให้ลูกค้าสามารถใช้งานได้อย่างครอบคลุมโดย “Transform Transcend” วิสัยทัศน์ทางธุรกิจของเราจะเปลี่ยนแปลงธุรกิจของลูกค้าและตลาดของลูกค้าเพื่อสร้างคุณค่าใหม่ๆ ที่เหนือกว่าความคาดหวังและจินตนาการที่เชื่อมโยงกับโลกที่จะก้าวข้ามอุปสรรคทั้งหมด โดย เอ็นทีที คอมมิวนิวนิเคชั่น ได้มีการให้บริการ ดังนี้

1.2.1 Network Innovation

นวัตกรรมเครือข่ายการสร้างเครือข่ายระบบคลาวด์ระดับโลกด้วยความมุ่งมั่นของญี่ปุ่นในการสร้างสรรค์นวัตกรรมด้านเครือข่ายที่มีคุณภาพนวัตกรรม NTT Communications มีข้อดีของเทคโนโลยีที่เป็นนวัตกรรมใหม่ที่เราสนับสนุนธุรกิจทั่วโลกด้วยบริการต่างๆทำให้เครือข่ายระบบคลาวด์ที่มีความน่าเชื่อถือสูงและมีการทำงานที่คล่องตัวสูง

รูปที่ 1.4 Network Innovation

1.2.2 Cloud Services

บริการระบบคลาวด์ทั่วโลกพร้อมโครงสร้างพื้นฐานระดับโลกแหล่งเดียวสำหรับบริการคลาวด์ที่ครอบคลุมซึ่งเป็นเอกลักษณ์เฉพาะของผู้ให้บริการโทรคมนาคม ทาง NTT Communications นำศูนย์ข้อมูลเครือข่ายและเซิร์ฟเวอร์มารวมกัน นอกจากนี้เรายังมีความยืดหยุ่นในการเชื่อมต่อกับบริการคลาวด์ของผู้ให้บริการรายอื่น ๆ ได้อีกด้วย

รูปที่ 1.5 Data Center ของ NTT Group สาขาอมตะนคร

1.2.3 IoT Platform

IoT Platform จะช่วยให้ลูกค้าแก้ปัญหาทางธุรกิจแบบ end-to-end โดยการให้บริการผ่าน Private Network และระบบคลาวด์และได้สร้างระบบนิเวศร่วมกับ บริษัท คู่ค้าที่นำไปสู่อุตสาหกรรมของตนเพื่อจัดหาโซลูชั่นแบบ end-to-end เพื่อแก้ปัญหาลูกค้า

รูปที่ 1.6 IoT Platform

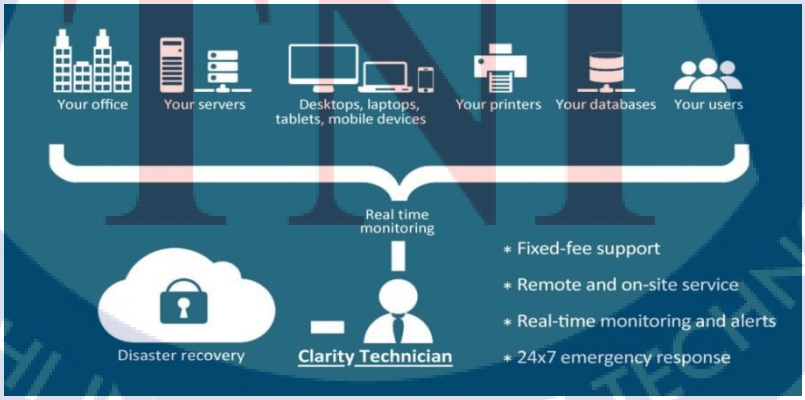
1.2.4 ICT Consulting

โซลูชั่น ICT สำหรับธุรกิจปล่อยให้ NTT Communication เป็นกรอบการทำงานแบบคลาวด์ที่ช่วยให้เกิดนวัตกรรม เรานำเสนอ ICT สำหรับการดำเนินงานแบบ bimodal ซึ่งมีความปลอดภัยและเชื่อถือได้สูงรวมถึงการประยุกต์ใช้และใช้งานได้ง่าย

รูปที่ 1.7 ICT Consulting

1.2.5 Managed Services

การบริการที่มีการจัดการซึ่งรวมการจัดการระบบ ICTในการบริการด้วย เราให้บริการแบบครบวงจรเพื่อให้การจัดการระบบไอซีทีรวม ไม่เพียงมีแต่รวมระบบเดิมที่เรานำเสนอเท่านั้นรวมถึงบริการที่มีให้โดย บริษัทอื่นๆ ด้วย



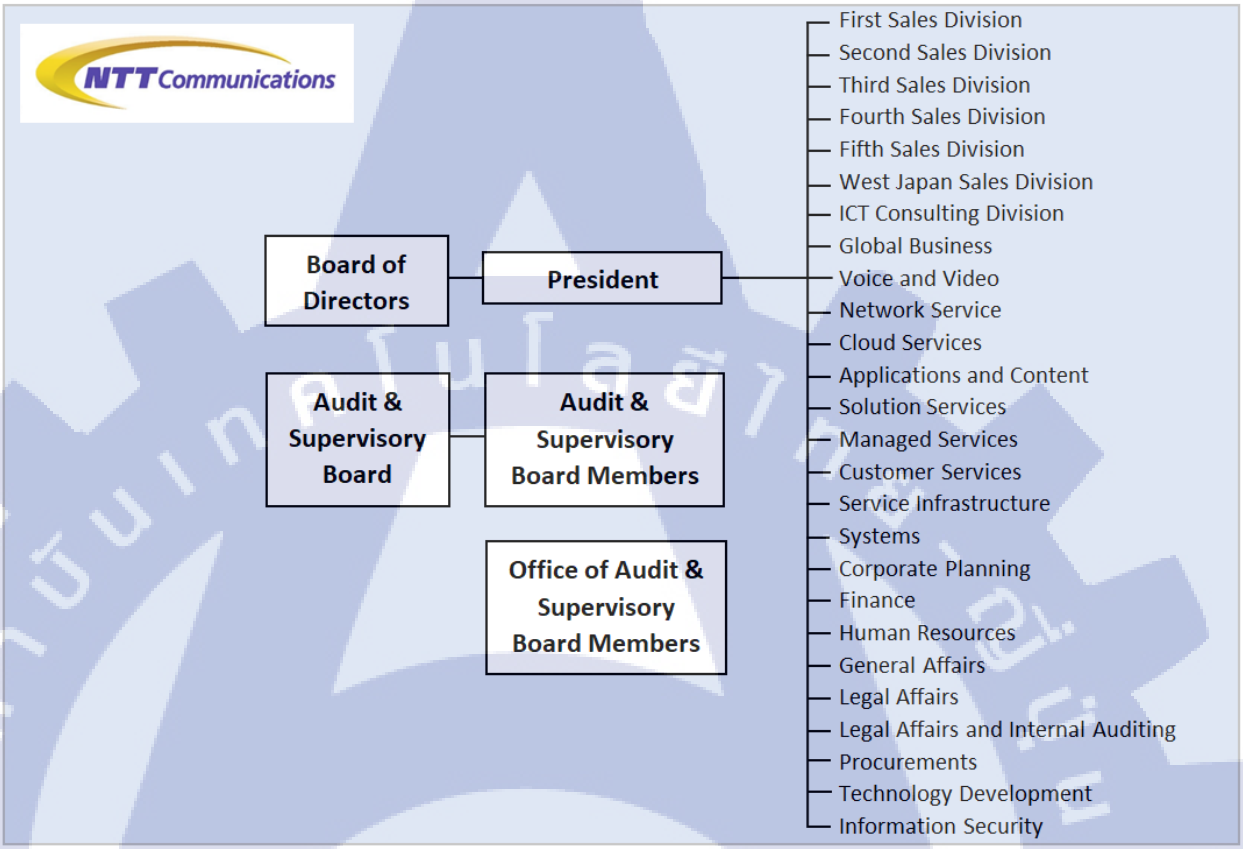
รูปที่ 1.8 Managed Services

1.2.6 ICT Operation

พอร์ทัล และ API Gateway สำหรับสภาพแวดล้อมการดำเนินงานพอร์ทัลของเราทำให้ลูกค้าสามารถเปลี่ยนการตั้งค่าและเข้าถึงบริการที่จำเป็นตามความต้องการ API Gateway ช่วยให้การดำเนินงานของลูกค้าและพันธมิตรไอซีทีอย่างมีประสิทธิภาพ

รูปที่ 1.9 ICT Operation

1.3 รูปแบบการจัดองค์กรและบริหารองค์กร



รูปที่ 1.10 แผนผังการบริหารของบริษัท

1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับมอบหมาย

ตำแหน่ง : Manage Service

หน้าที่ : ดูแล Service MDM (Mobile Device Management)

ดูแล Project 3G/4G Internet Back-up Link

จัดทำเอกสารประกอบการประชุม

แปลเอกสาร(Japanese / English)

1.5 พนักงานที่ปรึกษา และ ตำแหน่งของพนักงานที่ปรึกษา

พนักงานที่ปรึกษา	:	คุณพลอยแก้ว เรืองศรีสิริ
ตำแหน่ง	:	Manager
โทรศัพท์	:	083-5404359
Email	:	ploykaew.ru@ntt.co.th

1.6 ระยะเวลาที่ปฏิบัติงาน

เริ่มปฏิบัติงาน	:	วันที่ 29 พฤษภาคม 2560
สิ้นสุดการปฏิบัติงาน	:	วันที่ 18 สิงหาคม 2560
ระยะเวลา	:	3 เดือน

1.7 วัตถุประสงค์หรือจุดมุ่งหมายของการปฏิบัติงานหรือโครงงานที่ได้รับหมอบหมายให้ปฏิบัติงานสหกิจ

1.) เพื่อการเรียนรู้ทำงานจริงในสายงานด้านผู้ให้บริการเครือข่าย

2.) เพื่อนำความรู้ที่ได้เรียนรู้มาประยุกต์ใช้ในการปฏิบัติงานจริง

3.) เพื่อรู้จักการปรับตัวในการทำงานร่วมกับผู้อื่น

4.) เพื่อฝึกความเป็นระเบียบ รู้จักมีความรับผิดชอบในงานที่ตนได้รับมอบหมาย และ การตรงต่อเวลา

1.8 วัตถุประสงค์หรือจุดมุ่งหมายของโครงงาน

1.) เพิ่มเส้นทางสำรองอินเทอร์เน็ตให้แก่ลูกค้า

2.) เพื่อรักษาความต่อเนื่องในการดำเนินธุรกิจของลูกค้า

3.) เพิ่มความปลอดภัยทางด้านข้อมูล

1.9 ผลที่คาดว่าจะได้รับจากการปฏิบัติหรือโครงงานที่ได้รับมอบหมาย

1.) ได้รับความรู้เกี่ยวกับการติดตั้งและการตั้งค่าอุปกรณ์Router

2.) ได้รับความรู้เกี่ยวกับควบคุมอุปกรณ์ในระยะไกล

3.) ได้รับความรู้เกี่ยวกับการใช้คำสั่งในการทดสอบระบบและการเขียนรายงานเพื่อทำบันทึกให้แก่บริษัท

4.) ได้รับประสบการณ์ในการทำงานจริง ในการลงไซต์งานของลูกค้า การเข้า Data Center และเรียนรู้การเข้าถึงสังคมในการที่ทำงาน ซึ่งเป็นประโยชน์ต่อการทำงานในอนาคต

1.10 นิยามศัพท์เฉพาะ

MDM (Mobile Device Management) = ซอฟท์แวร์ที่ใช้ในการจัดการกับอุปกรณ์พกพา (Mobile Device) ในองค์กร

บทที่ 2

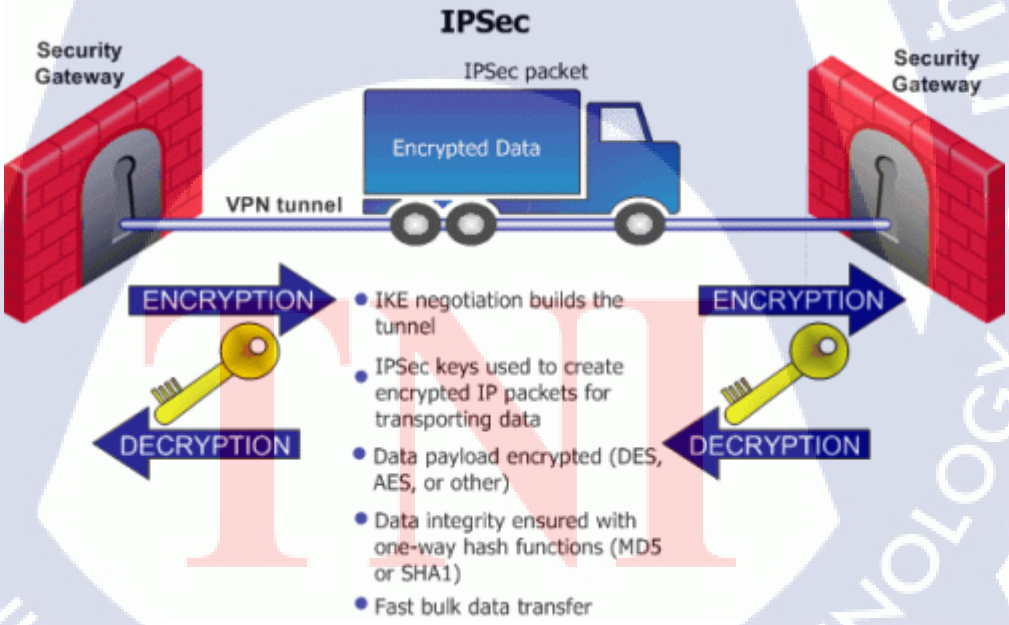
ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน

ในการปฏิบัติงานสหกิจศึกษาครั้งนี้ เป็นการนำความรู้ด้านทฤษฎีและเทคโนโลยีมาใช้ในการปฏิบัติงานทุกส่วนตลอดการปฏิบัติงานสหกิจศึกษา ซึ่งเป็นการนำความรู้ทั้งที่เคยเรียนมาประยุกต์ใช้และเป็นการศึกษาเรียนรู้สิ่งใหม่

2.1 ทฤษฎีที่ใช้ในการปฏิบัติงาน

2.1.1 IPSec (ตัวช่วยเพิ่มความปลอดภัยให้กับโปรโตคอล IP)

Internet Protocol security (IPSec) คือ ชุดโปรโตคอลเพิ่มเติมของโปรโตคอล IP เพื่อให้การติดต่อสื่อสารมีความปลอดภัยมากขึ้น โดยสิ่งที่เพิ่มเติมที่ทำให้มีความปลอดภัยนั่นคือ มีการทำ authentication และการ encryption ในข้อมูล IP packet ที่รับส่งกัน



รูปที่ 2.1 Encrypted Data by IPSec

ชุดโปรโตคอล IPSec นี้รวมถึงโปรโตคอลที่ใช้ในการทำ authentication ระหว่างกันเพื่อสร้าง session ที่ใช้ในการติดต่อสื่อสารและ โปรโตคอลที่ใช้เจรจา key ที่ใช้เข้ารหัสข้อมูลระหว่างการติอต่อสื่อสารของ session เราสามารถใช้ IPSec ป้องกันข้อมูลในการติดต่อสื่อสารได้ทั้งระหว่าง host กับ host (computer user or server) ระหว่าง security gateway กับ security gateway (router or firewall) หรือระหว่าง security gateway และ host โดย IPSecสามารถนำไปประยุกต์ใช้งานได้หลากหลายมาก เนื่องจากมันทำงานใน layer ที่ต่ำ (internet layer ใน TCP/IP model) ทำให้ Application ต่างๆ ไม่ต้องทำสิ่งใดเพิ่มเติมเพื่อให้ทำงานร่วมกับ IPSec ได้ ไม่เหมือนกับโปรโตคอลด้านความปลอดภัยตัวอื่น เช่น TLS/SSL ที่จะต้องออกแบบ Application ให้ทำงานร่วมกันกับมันได้

IPSec ประกอบด้วยโปรโตคอล ที่ทำหน้าที่หลักต่างๆกันดังนี้

1. Internet Key Exchange (IKE) เป็นโปรโตคอลที่ใช้สำหรับการจัดตั้ง Security Association (SA) ที่ใช้เป็นช่องทางการสื่อสารระหว่างกัน และเป็นโปรโตคอลที่ใช้เจรจาว่าจะใช้โปรโตคอลใดและ algorithm ใด ทีจะใช้สร้าง key สำหรับ encrypt ข้อมูลและทำ authentication ระหว่างกัน

2. Authentication Header (AH) เป็นโปรโตคอลที่ทำหน้าที่รักษาความถูกต้องสมบูรณ์ (integrity) ของข้อมูล เพื่อเป็นการยืนยันว่าข้อมูลที่ได้รับนั้นไม่ได้ถูกแก้ไขระหว่างทาง โดยการใช้ Hash Message Authentication Code (HMAC) ที่สร้างจาก algorithm เช่น MD5 หรือ SHA เป็นต้น

3. Encapsulation Security Payload (ESP) เป็นโปรโตคอลที่ทำหน้าที่ในการรักษาความลับ (Confidentiality) ข้อมูลโดยการเข้ารหัส โดยใช้algorithm เช่น DES, 3DES หรือ AES เป็นต้น

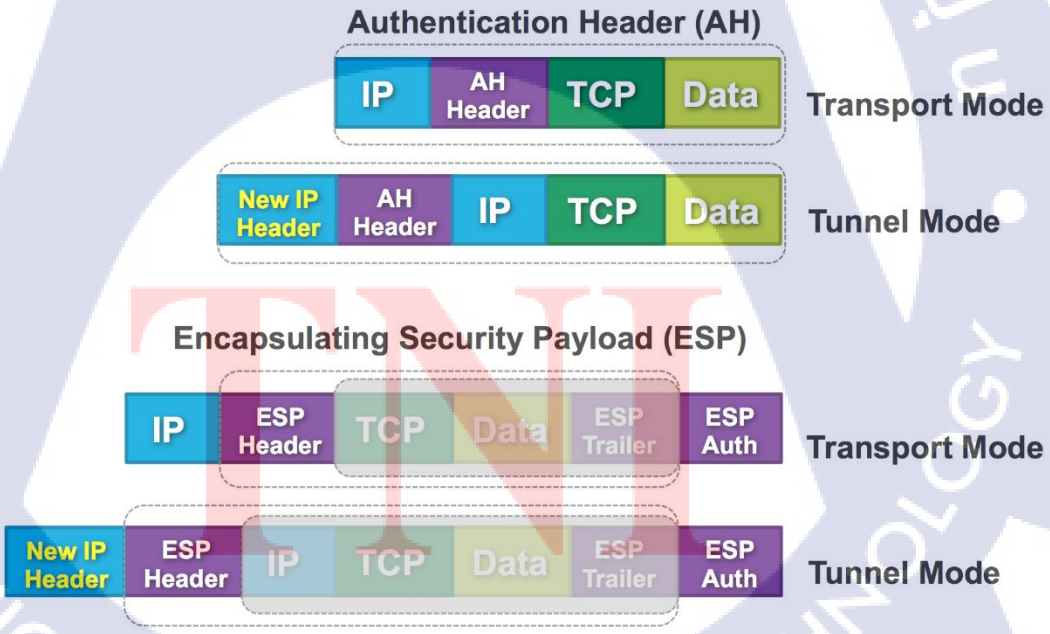
IPSec ทำงานอยู่ใน 2 mode ดังนี้

1. Transport mode ใน mode นี้ IPSec จะทำการ encrypt หรือ authenticate เฉพาะในส่วนข้อมูล (payload) ของ IP packet ที่จะส่ง แต่ไม่ทำในส่วนของ Header (หรือ IP Header) ของ IP packet

2. Tunnel mode ใน mode นี้จะทำการ encrypt หรือ authenticate ทั้ง IP packet (payload และ header) และสร้าง IP Header ขึ้นมาใหม่

ตัวอย่าง การตั้งค่า Router Cisco เพื่อใช้งาน IPSec โดยการตั้งค่า Router เพื่อใช้งาน IPSec มีขั้นตอนหลักๆ ดังนี้

- ตั้งค่า ISAKMP
- ตั้งค่า IPSec



รูปที่ 2.2 Mode ของ IPSec

การตั้งค่า ISAKMP

IKE (ISAKMP/Oakley) คือโปรโตคอลลูกผสมที่นำบางส่วนของโปรโตคอล Oakley และ ISAKMP แต่ใน Cisco IOS softwareโปรโตคอล IKE และ ISAKMP จะใช้สื่อความหมายถึงสิ่งเดียวกัน ดังนั้นการตั้งค่า ISAKMP ก็คือการตั้งค่า IKE โดยโปรโตคอล IKE นี้จะทำงานในช่วงการจัดตั้งSA สำหรับ IPSec และมันต้องมี policy ที่ใช้ในการเจรจาเพื่อสร้าง SA ระหว่าง router กันด้วย

การตั้งค่า ISAKMP มีด้วยกันอยู่ 2 วิธีดังนี้

1. ใช้วิธี pre-shared keys ซึ่งตั้งค่าได้ง่ายและสะดวก (ตัวอย่างจะใช้วิธีนี้)
2. ใช้วิธี CA เหมาะกับรองรับการขยายตัวในการใช้งาน

หมายเหตุ โปรโตคอล IKE ทำงานบน UDP 500, IPSec ทำงานบน IP protocol 50 และ 51 โดย port เหล่านี้จะต้องไม่ถูกปิดกั้นระหว่าง router ด้วยกัน

วิธี Pre-Shared Keys

การใช้วิธีนี้จะต้องตั้งค่าตามขั้นตอนดังนี้

- ตั้งค่า ISAKMP Protection Suite(s)
- ตั้งค่า ISAKMP key

ตั้งค่า ISAKMP Protection Suite(s)

คำสั่งนี้เป็นการสร้าง object ของ ISAKMP policy

```
RouterName(config)# crypto isakmp policy 1
RouterName(config-isakmp)#
```

คำสั่ง group ใช้เพื่อบอกขนาดจำนวน bit ของ modulus ที่ใช้ในวิธีการคำนวณใน Diffie-Hellman(เป็นวิธีการการจัดตั้ง(establishment)การ shared key ผ่านบนช่องทางที่ไม่ปลอดภัย) โดย group 1 หมายถึงมีขนาด 768 บิต group 2 หมายถึง มีขนาด 1024 บิต โดย default Cisco IOS จะเป็น group 1

RouterName(config-isakmp)# *group 2*

คำสั่ง hash ใช้เพื่อบอกว่าจะใช้ hash algorithm แบบใด โดย default ของ Cisco IOS จะเป็นแบบ SHA ที่มีความปลอดภัยมากกว่า MD5

RouterName(config-isakmp)# *hash md5*

คำสั่ง lifetime ใช้เพื่อบอกว่า SA จะมีเวลาอยู่เท่าใด ก่อนที่จะมีการเจรจาสร้าง SA ใหม่ โดย default จะมีค่าอยู่ที่ 86400 วินาทีหรือ 1 วัน

RouterName(config-isakmp)# lifetime *500*

คำสั่ง authentication ใช้เพื่อบอกว่าจะใช้ key อะไรในการยืนยันตัวตนของ router ทั้งฝั่ง

RouterName(config-isakmp)# *authentication pre-share*

ตั้งค่า ISAKMP key

คำสั่งที่จะแสดงต่อไปนี้ จะเป็นการบอกว่าค่า key เป็นอะไร และ ip ของ router ฝั่งตรงข้ามเป็นอะไร โดย key ที่ตั้งนี้จะต้องเหมือนกัน

RouterName(config-isakmp)# exit

RouterName(config-isakmp)# crypto isakmp key *Slurpee* address *192.168.10.38*

การตั้งค่า IPSec

มีขั้นตอนย่อยๆดังนี้

- สร้าง extended access list
- สร้าง IPSec transform(s)
- สร้าง crypto map
- นำ crypto map ไปใส่ใน interface เพื่อใช้งาน

การสร้าง extended access list

คำสั่งที่ใช้นี้เป็นการสร้าง access list สำหรับบอกว่า traffic ใดบ้างที่จะถูก encryption หรือไม่ถูก encryption โดยคำสั่ง permit เป็นเหมือนการบอกว่า trafficนั้นจะถูก encryption และ คำสั่ง deny เป็นเหมือนการบอกว่า traffic นั้นไม่ถูก encryption โดยมีการนำไปใช้อ้างอิงใน crypto map

RouterName(config)#*access-list 101 permit ip host 192.168.10.38 host 192.168.10.66*

หรือ RouterName(config)#*access-list 101 permit ip host 192.168.10.38 0.0.0.255 192.168.10.66 0.0.0.255*

การสร้าง IPSec transform(s)

คำสั่งนี้เป็นการสร้าง IPSec transform set เพื่อบอกว่าจะใช้วิธีการใดในการ encrypt ข้อมูล โดยมีการนำไปใช้อ้างอิงใน crypto map

RouterName(config)*crypto* ipsec *transform-set MamaBear ah-md5-hmac esp-des*

RouterName(cfg-crypto-trans)*exit*

การสร้าง Crypto Map

ใน Crypto map จะมีการตั้งค่าต่างๆ ประกอบด้วย การตั้งค่าเพื่อบอกว่า peer ที่จะคุยด้วยเป็น IP อะไรโดยใช้คำสั่ง set peer การตั้งค่า session key ว่าจะมีอายุใช้งานเท่าใดก่อนมีการสร้างขึ้นใหม่ โดยมีการกำหนดได้สองแบบคือกำหนดด้วยเวลาและกำหนดด้วยขนาดข้อมูล traffic ที่รับส่งกัน การตั้งค่าผูกโยงกับIPSec transform set ที่ได้มีการสร้างขึ้นมาก่อนหน้านี้ด้วยคำสั่ง set transform และการตั้งค่าอ้างอิงกับ access list ที่ได้สร้างขึ้นมาไว้ ด้วยคำสั่ง match address

RouterName(config)crypto map armadillo 10 ipsec-isakmp

RouterName(config-crypto-map)#set peer 192.168.10.38

RouterName(config-crypto-map)#set session-key lifetime seconds 4000

RouterName(config-crypto-map)#set transform-set MamaBear

RouterName(config-crypto-map)#match address 101

นำ crypto map ไปใส่ใน interface เพื่อใช้งาน โดยใช้คำสั่งนี้

RouterName(config)#interface serial 0/0

RouterName(config-if)crypto map armadillo

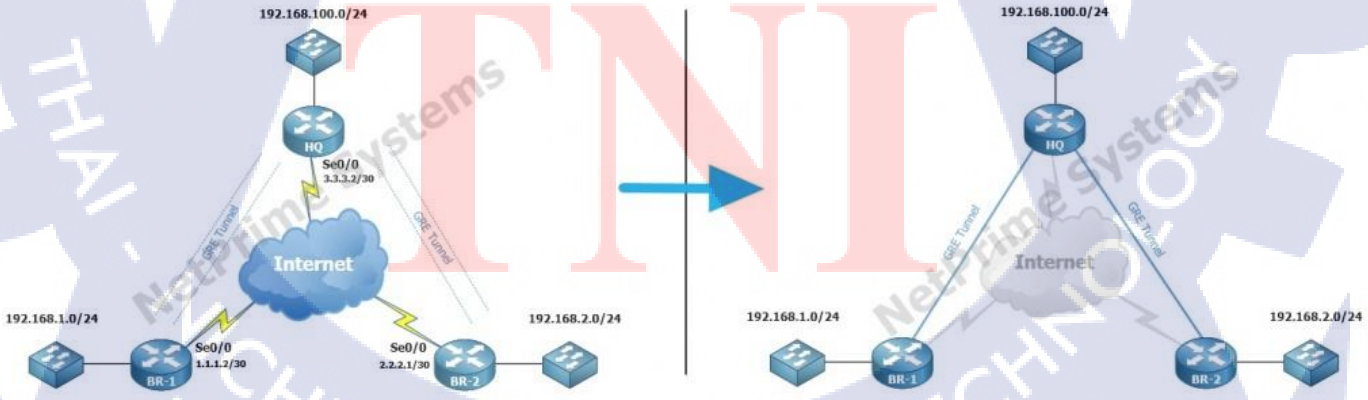
ตัวอย่างคำสั่งที่ใช้ตรวจสอบ IPsec เช่น

Show crypto isakmp sa	ใช้ดูตาราง ISAKMP(IKE) SA ถึงการมีอยู่ระหว่าง SA ของ router ทั้งสอง
Show crypto isakmp policy	ใช้ดู policy ของ ISAKMP ที่ได้ตั้งค่าต่างไว้
Show crypto ipsec sa	ใช้ดูค่าของ traffic ที่ถูก encrypt ฯลฯ

ตารางที่ 2.1 ตัวอย่างคำสั่งที่ใช้ตรวจสอบ IPSec

2.1.2 DYNAMIC MULTIPOINT VPN (DMVPN)

Dynamic Multipoint VPN (DMVPN) เป็นการทำ VPN โดยที่เราสามารถเชื่อมต่อหลายๆ Site เข้าหากันได้ ซึ่ง DMVPN จะใช้ topology แบบ Hub and Spoke และอย่างที่ทราบกันโดยปกติ ถ้า Spoke ต้องการจะคุยกับ Spoke แล้ว traffic จะต้องผ่าน Hub ก่อน แต่ถ้าเราต้องการให้ Spoke คุยกับ Spoke ได้โดยไม่ผ่าน Hub เราจำเป็นจะต้องมาสร้าง tunnel เอง แต่เมื่อเราใช้งาน DMVPN แล้ว มันจะทำการสร้าง tunnel ระหว่าง Spoke กับ Spoke ขึ้นมาให้อัตโนมัติ โดยที่เราไม่ต้องไปตั้งค่าแบบ manual



รูปที่ 2.3 Dynamic Multipoint VPN

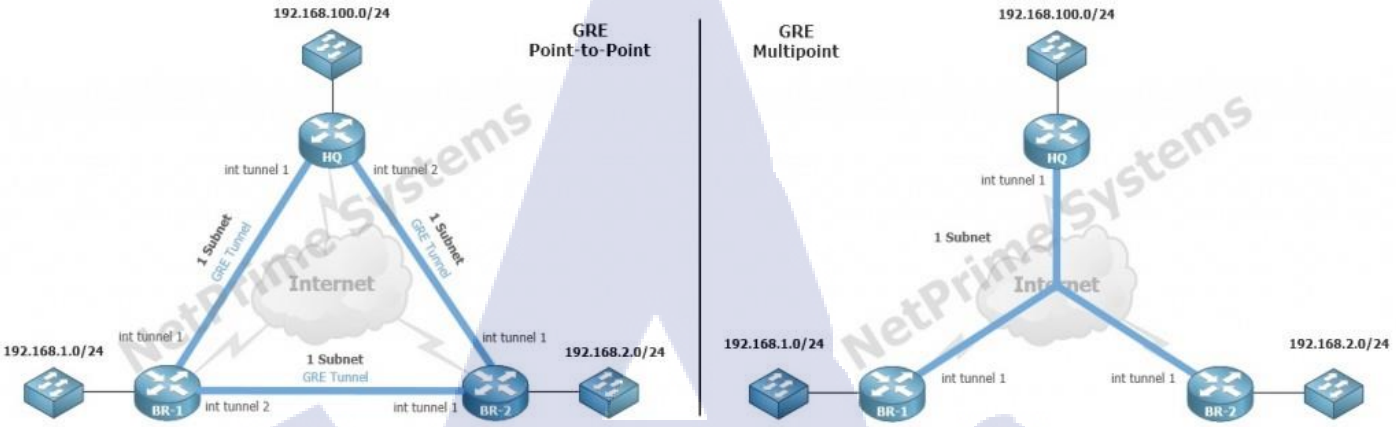
ปกติแล้ว ถ้าเราต้องการจะเชื่อมต่อหลายๆ Site เข้าหากัน ขอแค่แต่ละ Site มี internet ของตัวเอง (ไม่ต้องไปเสียเงินเช่า private link ราคาแพงๆ) แล้วเราก็ทำ VPN โดยใช้ GRE เพื่อให้แต่ละ Site เชื่อมต่อกันได้ เปรียบเสมือน Router ของแต่ละ Site มีสายต่อกันตรงๆ

ในการเชื่อมต่อระหว่าง Site (Hub to Spoke หรือ Spoke to Spoke) โดยใช้แบบ Point-to-Point เราจะต้องสร้าง GRE ตามจำนวน Site ทั้งฝั่ง Hub และ Spoke และอนาคตถ้ามี Site (Spoke) เพิ่มขึ้น เราก็ต้องเข้าไปสร้าง GRE tunnel ทั้งฝั่ง HQ (Hub) และ Branch (Spoke) ขึ้นมาใหม่ หรือ ถ้าต้องการให้สามารถคุยกันระหว่าง Site ได้ (Spoke to Spoke) ก็ต้องไปตั้งค่าเพื่อสร้าง GRE tunnel ขึ้นมาอีก ทำให้เกิดความยุ่งยากเมื่อมีการเพิ่ม Site หรือ ต้องการจะให้ traffic ระหว่าง Site คุยกันได้

ซึ่งการทำ DMVPN นั้น จะใช้หลายๆ เทคโนโลยีเข้ามาประกอบกัน ดังนี้

- mGRE (Multipoint GRE)
- Next Hop Resolution Protocol (NHRP)
- Dynamic Routing Protocol (OSPF , EIGRP etc.)
- IPSec (ถ้าต้องการ encryption ข้อมูล)
- Cisco Express Forwarding (CEF)

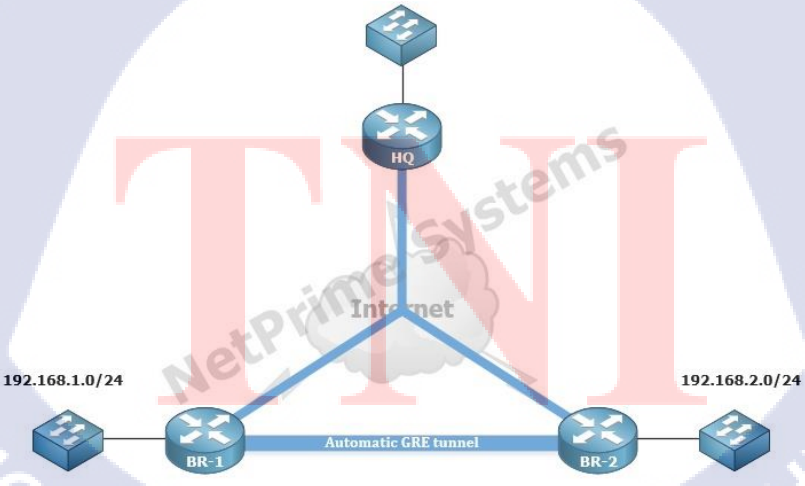
พอเราต้องการจะทำ DMVPN แล้ว GRE ที่เราจะใช้จะเป็น Multipoint GRE (MGRE) ไม่ใช่ Point-to-Point แบบที่ผมพูดถึงในตอนแรกแล้ว การทำ Multipoint มีข้อดีคือ ไม่ว่าเราจะเพิ่ม Router เข้ามาอีกกี่ Site ก็ตาม โครงข่ายตรงกลางที่เราทำ Tunneling จะใช้เพียง subnet เดียว ไม่เหมือนกับ Point-to-Point ที่ต้องใช้ 1 subnet ต่อ 1 tunnel ซึ่งสามารถทำให้ง่ายต่อการเพิ่มขยาย



รูปที่ 2.4 Multipoint GRE (MGRE) เปรียบเทียบแบบ Point-to-Point กับ Multipoint

จะเห็นว่าถ้าทำ Point-to-Point เราจะมี subnet และ interface tunnel ตามจำนวน tunnel ที่เกิดขึ้น แต่ถ้าเป็น multipoint บน Router แต่ละตัว จะมี Interface tunnel เดียวเท่านั้น

และเมื่อเป็น DMVPN ในส่วนของ traffic ที่คุยกันระหว่าง Site (Spoke-to-Spoke) โดยตรง มันจะสร้าง GRE tunnel แบบ Point-to-Point ให้อัตโนมัติเลย (ถ้าไม่ใช้ DMVPN แล้วเราอยากให้ Spoke คุยกับ Spoke เราก็จะต้องไปทำการตั้งค่า GRE ระหว่าง Site นั้นเองแบบ manual



รูปที่ 2.5 Traffic ระหว่าง BR-1 กับ BR-2

จากรูป ถ้า traffic จาก BR-1 ต้องการจะส่งไปฝั่ง BR-2 แล้ว DMVPN จะทำการสร้าง GRE tunnel ระหว่าง BR-1 กับ BR-2 ขึ้นมาให้โดยอัตโนมัติ

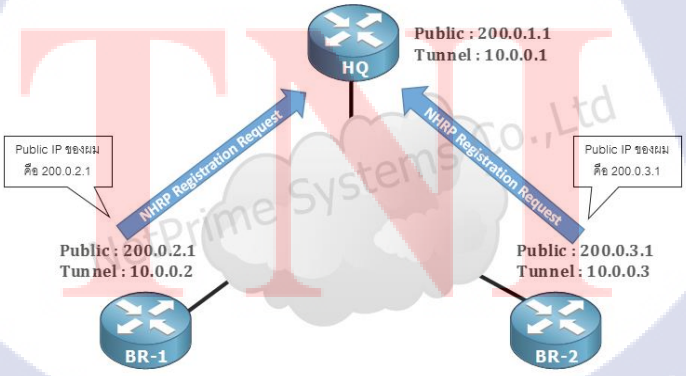
ในส่วนต่อมา ถ้าใช้ DMVPN แล้ว traffic ที่ต้องการคุยกันระหว่าง Site (Spoke-to-Spoke) จะทำการสร้าง GRE tunnel ให้อัตโนมัตินั้น จะมีกลไลและวิธีการสร้าง โดยใช้งานผ่าน Next Hop Resolution Protocol (NHRP)

2.1.3 NEXT HOP RESOLUTION PROTOCOL (NHRP)

คือ โปรโตคอลที่ใช้งานบน DMVPN ทำงานคล้าย ARP ที่ใช้ในการหา IP address ของอุปกรณ์ที่อยู่บนโครงข่ายแบบ NBMA (Non Broadcast Multi-Acces) ซึ่งจะมีการทำงานดังนี้

การทำงานเป็นแบบ Client – Server

- Router ที่ถูกกำหนดเป็น Hub จะทำหน้าที่เป็น NHRP Server (Static Public IP)
- Router ที่ถูกกำหนดเป็น Spoke จะทำหน้าที่เป็น NHRP Client (Static หรือ Dynamic Public IP)
- NHRP Client จะไป register กับ NHRP Server
- NHRP Server จะเก็บข้อมูลของ Client ที่มา register ไว้ใน NHRP Database



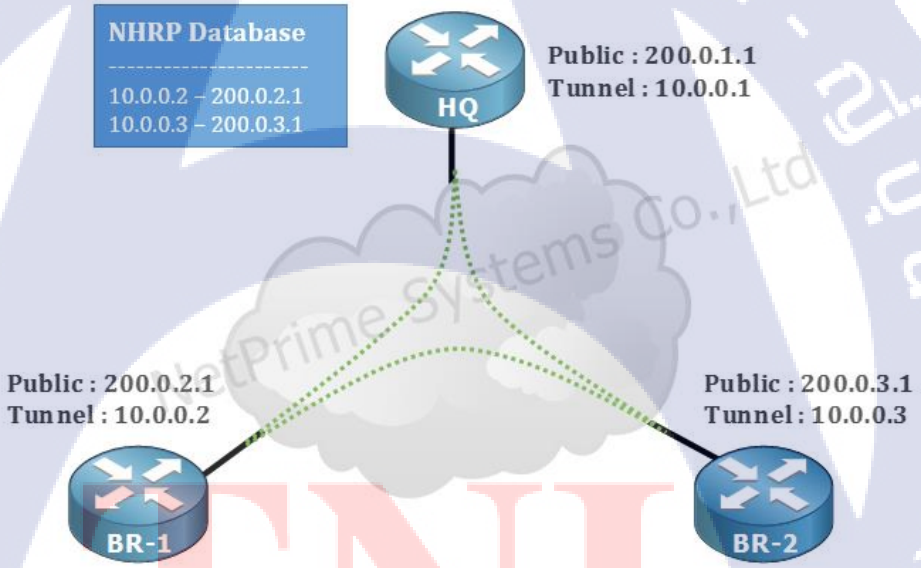
รูปที่ 2.6 การทำงานของ NHRP

จากรูปด้านบนกำหนดให้ HQ เป็น Hub และ BR-X เป็น Spoke

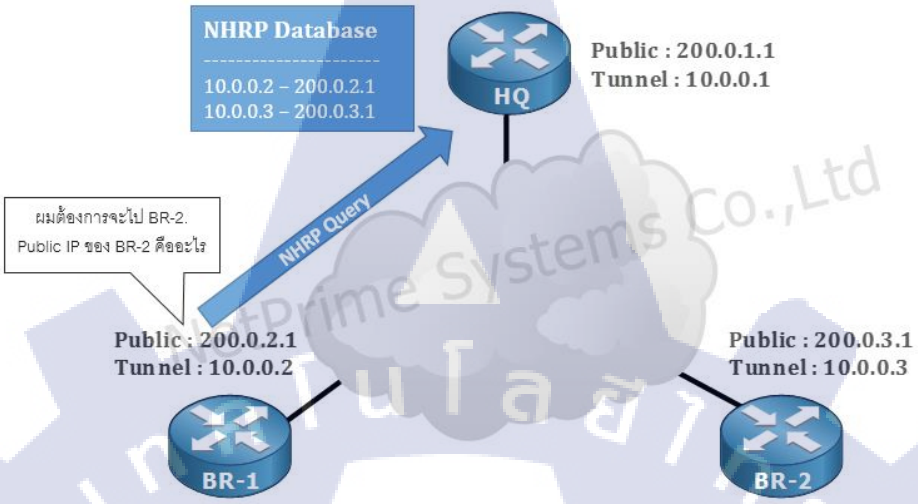
เมื่อมีการตั้งค่าใช้งาน NHRP บน HQ และ BR-X ฝั่ง BR-X (Spoke) จะทำการส่ง “NHRP Registration request” เพื่อลงทะเบียน และ รายงาน Public IP ของตัวเองไปให้ HQ (Hub)

Note: ดังนั้น Router ฝั่งที่เป็น Spoke ไม่จำเป็นที่จะต้องใช้ Public IP แบบ Static ก็ได้ เราสามารถใช้ Public IP แบบ Dynamic ได้เลย เพราะในกระบวนการ NHRP Registration จะเห็นว่าฝั่งที่เป็น Spoke จะรายงาน Public IP ของตัวเองไปให้ Hub รู้จักอยู่แล้ว

เมื่อ HQ (Hub) ได้รับมาแล้ว ก็จะทำการสร้าง Tunnel ขึ้นมา และเก็บข้อมูล Public IP กับ Tunnel IP ของฝั่ง BR-X (Spoke) ทั้ง 2 ตัว เอาไว้ใน Database (Cache)



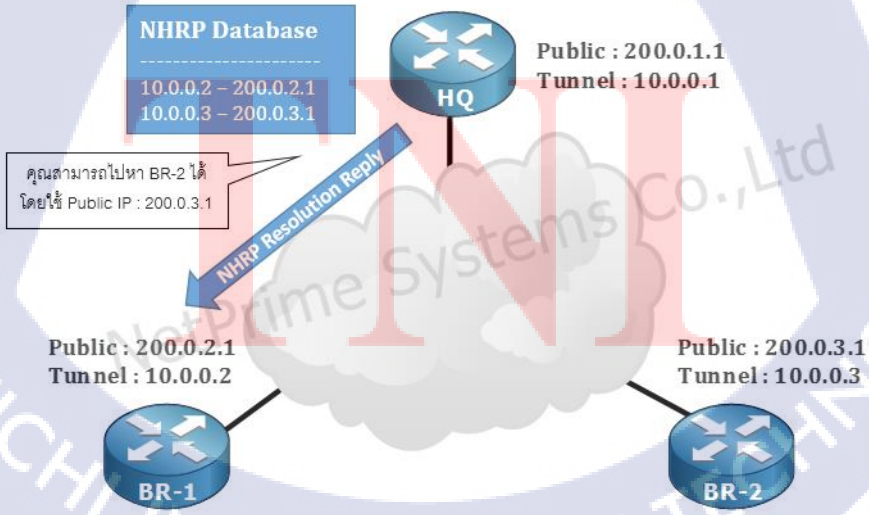
รูปที่ 2.7 เมื่อ HQ (Hub) ได้รับมาแล้วทำการสร้าง Tunnel ขึ้นมา และเก็บข้อมูล



รูปที่ 2.8 BR-1 ส่งข้อมูลไปยัง BR-2 ด้วย NHRP Query เพื่อถาม Public IP

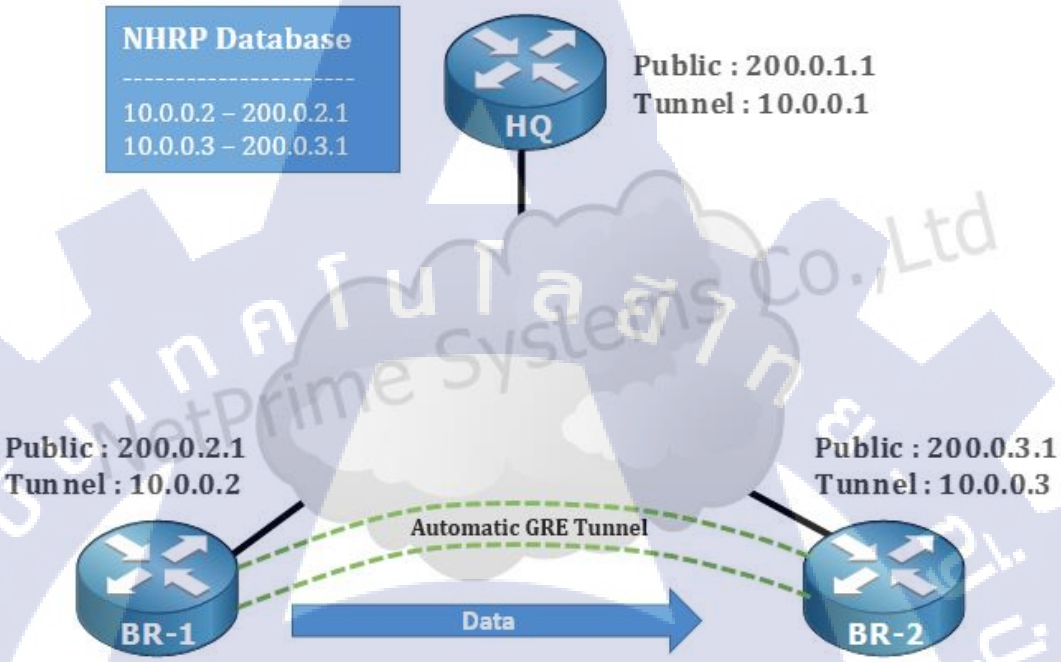
เมื่อฝั่ง BR-1 (Spoke1) ต้องการจะส่งข้อมูลไปฝั่ง BR-2 (Spoke2)

ฝั่ง BR-1 (Spoke1) จะทำการส่ง “NHRP Resolution Request (Query)” ไปหา HQ (Hub) เพื่อถามว่า Public IP ของ BR-2 (Spoke2) คืออะไร



รูปที่ 2.9 BR-2 ตอบกลับ BR-2 โดยการส่ง Public IP กลับไปยัง BR-1

HQ (Hub) จะตอบกลับ BR-1 (Spoke1) ด้วย “NHRP Resolution Reply” โดยการส่ง Public IP ของ BR-2 (Spoke2) กลับไปให้ BR-1 (Spoke1)



รูปที่ 2.10 ระหว่าง BR-1 และ BR-2 สร้าง Tunnel ขึ้นระหว่างกัน

เมื่อ BR-1 รู้ Public IP ของ BR-2 แล้ว ก็สามารถสร้าง Tunnel ระหว่างกัน ได้โดยอัตโนมัติ และทำการส่งข้อมูลหากันได้โดยตรง โดยที่ไม่ต้องไปวิ่งผ่าน HQ (Hub) ก่อนนั่นเองครับ

สรุปทั้งหมดคือ คือ กระบวนการทำงานของ NHRP ที่เราจะนำมาใช้งานบน DMVPN ต่อไป

DMVPN จะใช้งานอยู่ทั้งหมด 3 Phases ด้วยกัน ดังนี้

- Phase 1
- Phase 2
- Phase 3

Phase 1

- ฝั่ง Spoke ใช้ NHRP ในการ Registration กับ Hub
- ฝั่ง Hub ใช้งาน Tunnel แบบ Multi point (mGRE)
- ฝั่ง Spoke ใช้งาน Tunnel แบบ Point-to-Point (GRE)
- Spoke กับ Spoke ไม่สามารถคุยกันได้โดยตรง
- Spoke กับ Spoke จะคุยกัน traffic จะต้องวิ่งผ่าน Hub เท่านั้น

Phase 2

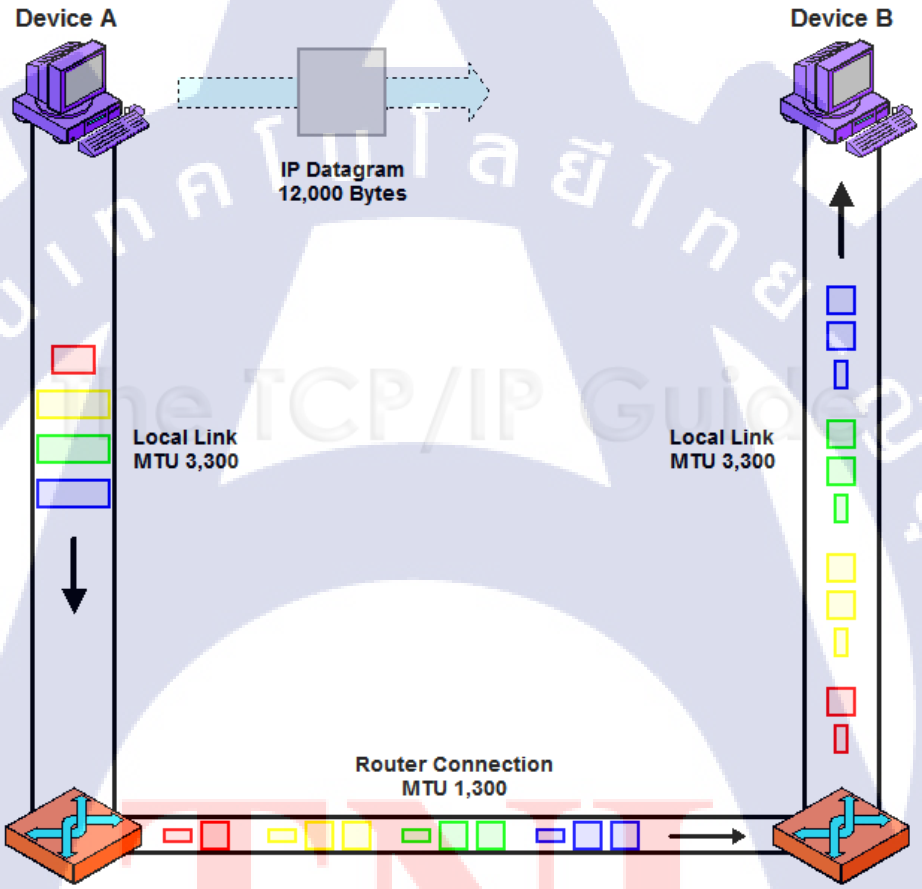
- ฝั่ง Spoke ใช้ NHRP ในการ Registration กับ Hub
- ฝั่ง Hub ใช้งาน Tunnel แบบ Multi point (mGRE)
- ฝั่ง Spoke ใช้งาน Tunnel แบบ Multi point (mGRE)
- Spoke กับ Spoke สามารถคุยกันได้โดยตรง ไม่ต้องวิ่งผ่าน Hub
- ไม่สามารถทำ summarization ที่ฝั่ง Hub เพื่อให้ส่ง summary route ไปหา Spoke ได้
- ใช้เทคนิคของ routing protocol เพื่อให้ฝั่ง Spoke เห็น Next-hop ซึ่งกันและกัน (จะกล่าวถึงในบทความการตั้งค่า DMVPN Phase 2)

Phase 3

- การทำงานของ NHRP จะแตกต่างออกไปจากเดิม
- เมื่อฝั่ง Spoke ต้องการจะส่งข้อมูลหากัน จะทำการส่ง traffic ไปหา Hub จากนั้น Hub จะทำส่ง NHRP Redirect ไปหา Spoke เพื่อบอกว่า ให้ Spoke สามารถคุยกันโดยตรงได้เลย
- เมื่อ Spoke ได้รับ NHRP Redirect จาก Hub มันจะส่ง NHRP Resolution ไปหา Public IP ของ Spoke ที่จะไปหา และทำการเพิ่มเส้นทางใหม่ (route) ลงใน routing table เพื่อติดต่อหากันโดยตรงระหว่าง Spoke to Spoke

2.1.4 MAXIMUM TRANSMISSION UNIT (MTU)

ในหน้าการตั้งค่าการเชื่อมต่ออินเตอร์เน็ต ฟีเจอร์หนึ่งบนRouterที่จะเห็นคือ MTU ซึ่งหากทำความเข้าใจกับ MTU ว่ามันมีประโยชน์อย่างไร ซึ่งถ้าใครใช้อินเตอร์เน็ตแล้วหลุดบ่อยหรือเข้าเว็บแล้วช้ารอนานเล่นเกมไม่เสถียร สาเหตุอาจจะเกิดจากค่า MTU ได้



รูปที่ 2.11 แผนผังการส่งค่า MTU

MTU หรือ Maximum Transmission Unit ก็คือค่าที่กำหนดปริมาณการรับส่งข้อมูลระหว่างเครื่องของเรากับ ผู้ให้บริการอินเตอร์เน็ต (ISP) ปกติจะมีค่า default = 1500 byte หรือถ้ายกตัวอย่างง่ายคือ ลองสุมมิตให้ MTU นี้คือขนาดของกล่องพัสดุที่สามารถบรรจุสิ่งของหรือข้อมูลได้จำนวนหนึ่ง ถ้าเราใส่ของที่มีขนาดใหญ่เกินกว่าที่กล่องจะรับได้มันก็จะปิดไม่ลงและส่งไม่ได้ ซึ่งแต่ละเครื่องเวลาจะส่งข้อมูลไปในอินเตอร์เน็ตก็ต้องเลือกกล่องที่สามารถบรรจุของได้มากที่สุดเท่าที่จะเป็นไปได้เพื่อ

ประหยัดเที่ยวในการขนส่ง ซึ่งถ้าต้องขนส่งหลายเที่ยวก็จะมีความเสี่ยงที่จะเกิดอุบัติเหตุระหว่างทาง และไม่สามารถขนส่งไปถึงได้ จึงจำเป็นต้องมาหาว่าค่า MTU เหมาะสมและถูกต้องเป็นเท่าไหร่เพื่อให้เราสามารถขนส่งของหรือข้อมูลได้มีประสิทธิภาพสูงสุด เพื่อลดความสูญเสียข้อมูลระหว่างทางและเพิ่มความเสถียรให้กับการใช้งานอินเตอร์เน็ต

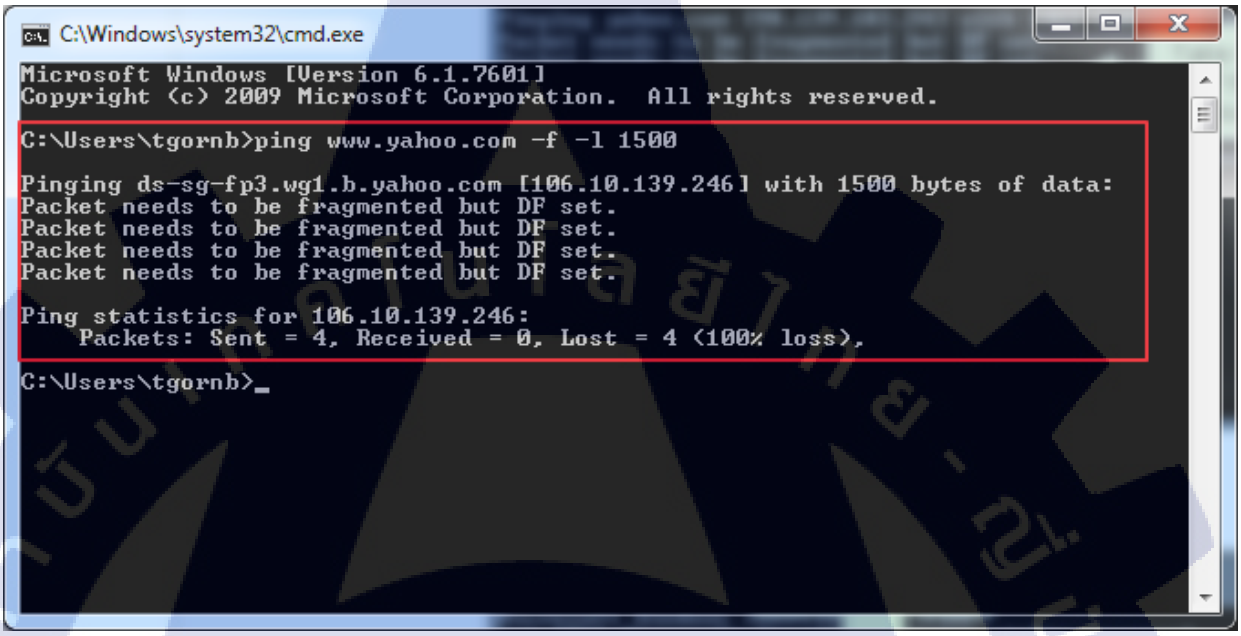
วิธีการหาค่า MTU ที่เหมาะสม (สำหรับผู้ที่ใช้ Windows)

1. ให้เปิด Command Prompt ขึ้นมา

รูปที่ 2.12 เปิดโปรแกรม Command Prompt

2. พิมพ์คำสั่งตามรูปแบบนี้ ping **[URL] [–f] [–l] [MTU Value]**

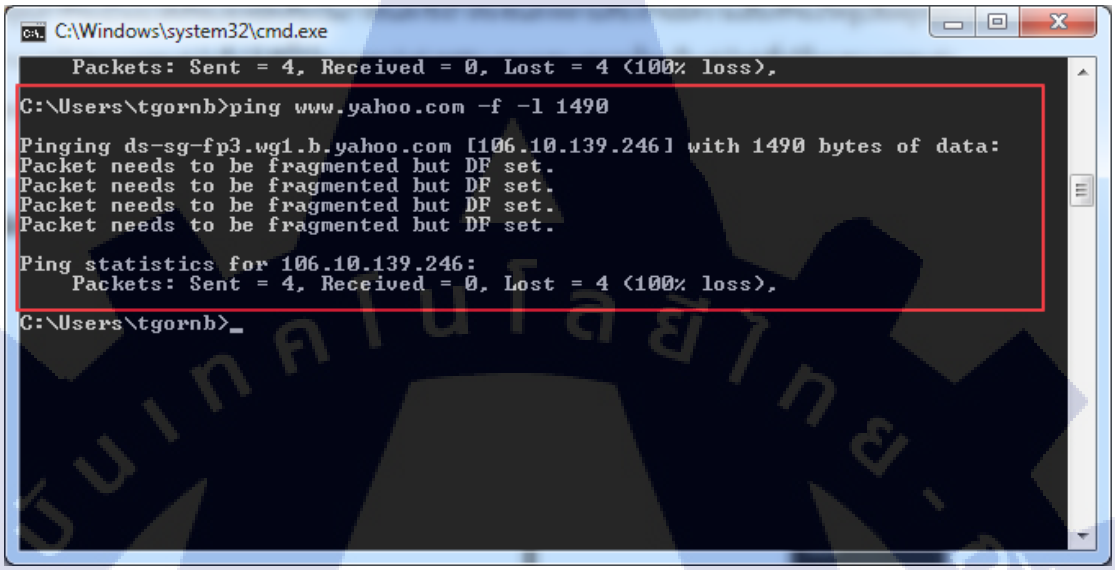
ตัวอย่างเช่น **ping www.yahoo.com –f –l 1500**



รูปที่ 2.13 พิมพ์คำสั่ง ping [URL] [–f] [–l] [MTU Value]

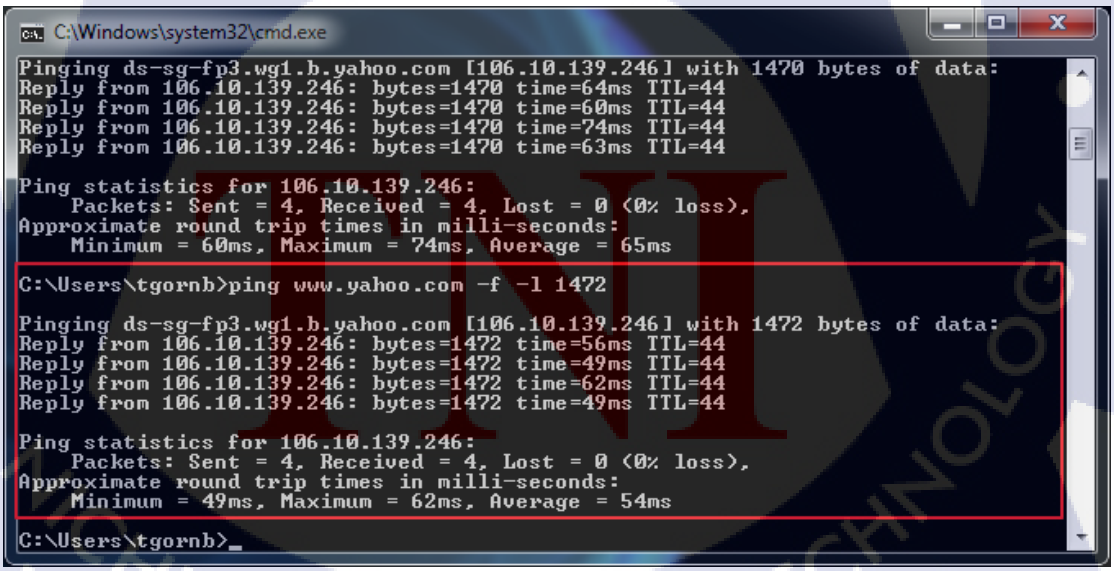
ถ้าขึ้น Packet needs to be fragmented but DF set. แสดงว่าค่า MTU หรือขนาดของข้อมูลที่เราใส่ไปมันใหญ่เกินไป ให้ลองปรับลงทีละ 10

3. ทดลองปรับค่า MTU ลงอีก 10 ใช้คำสั่ง **ping www.yahoo.com –f –l 1490** หากยังขึ้นข้อความเดิมอีกก็ลองปรับลงอีก



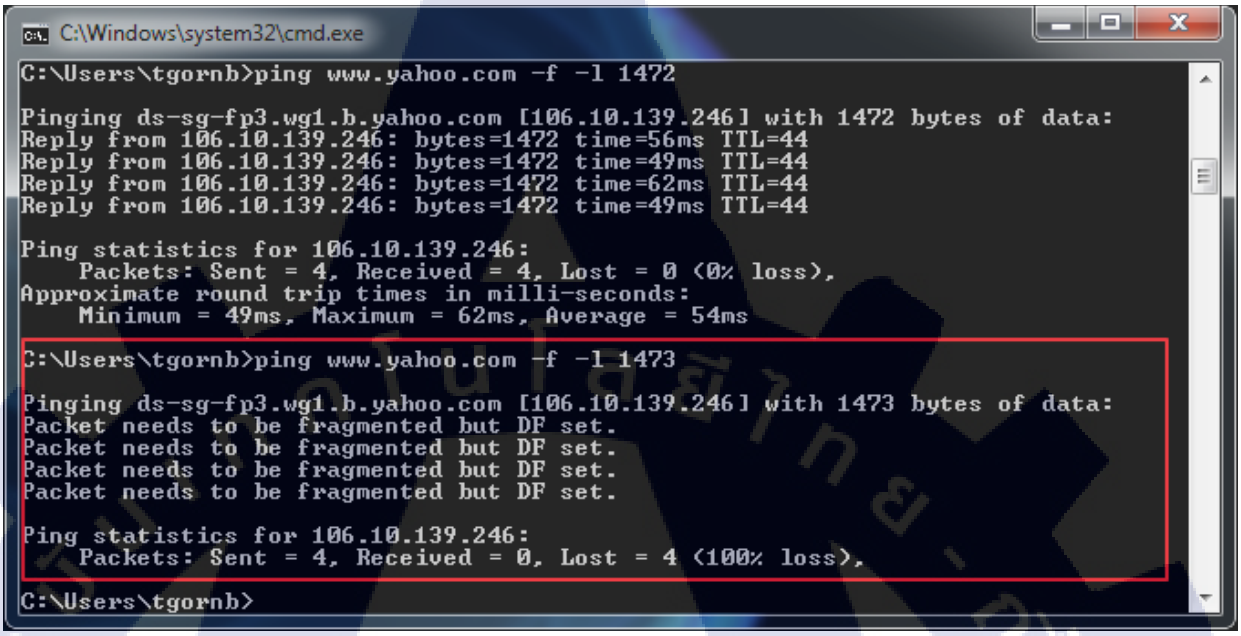
รูปที่ 2.14 ปรับค่า MTU ลง 10

4. ทดลองปรับจนเหลือค่า MTU = 1472 byte



รูปที่ 2.15 ปรับค่า MTU = 1472 byte

5.ในรูปนี้ทดลอง ปรับ MTU = 1473 byte จะเห็นได้ว่าเริ่มใช้ไม่ได้แล้ว



รูปที่ 2.16 ทดลองปรับค่าMTU = 1473 byte

จะเห็นได้ว่าค่า MTU = 1472 byte เป็นค่าที่เหมาะสมแต่ไม่ใช่ค่าที่ถูกต้องที่เราจะมากำหนดให้ที่ตัวRouter ในความเป็นจริงจำเป็นต้องเผื่อเอาไว้สักเล็กน้อยโดยการบวกเพิ่มอีก 28 byte (20 byte คือ จำนวนของ IP header และอีก 8 byte คือ จำนวนของ ICMP header) สรุปแล้วเราจะได้ค่า MTU ที่ถูกต้องเพื่อไปกำหนดให้Router คือ **1472+28 = 1500** ครับเมื่อได้ค่า MTU ที่ถูกต้องแล้วก็สามารถนำค่านี้ไปSetting Router ได้อย่าถูกต้อง

*** หรืออีกทางเลือกหนึ่งไม่อยากทำตามขั้นตอนเหล่านี้ก็สามารถใช้ค่า MTU ที่เป็นค่า default ของผู้ให้บริการได้ตามนี้

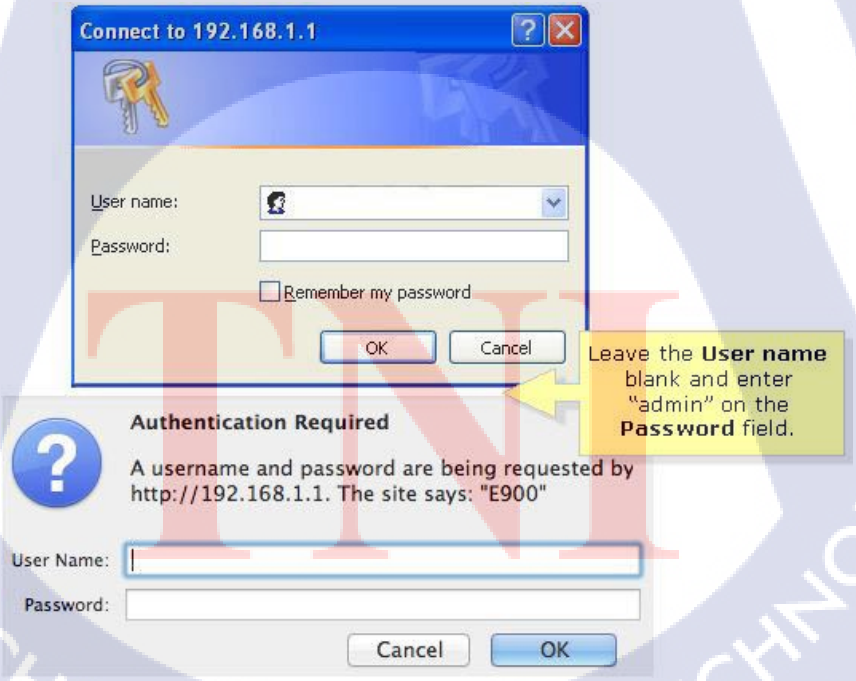
- TOT = 1492
- TRUE = 1492
- 3BB = Auto

วิธีการเซ็ตค่า MTU บนเร้าเตอร์ Linksys

1. เปิดเบราเซอร์ เช่น **Internet Explorer**,**Firefox**,**Chrome** หรือ **Safari** เข้าหน้าการตั้งค่าเร้าเตอร์โดยพิมพ์ 192.168.1.1 ในช่อง address bar แล้วกด Enter

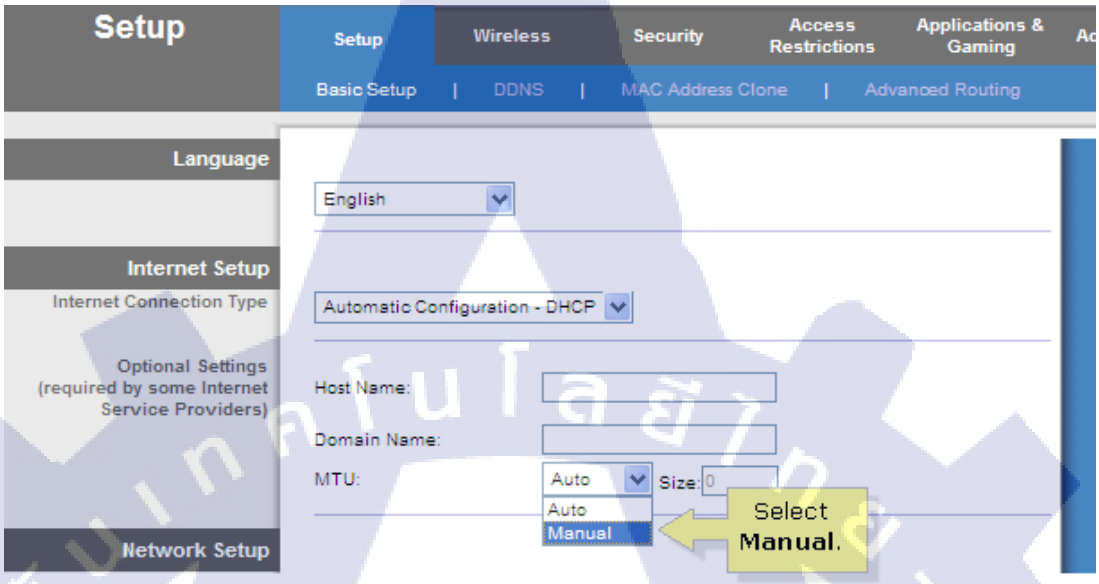
รูปที่ 2.17 เข้าหน้าการตั้งค่าเร้าเตอร์โดยพิมพ์ 192.168.1.1

2. จะมีหน้าต่างขึ้นมาให้ใส่ Username: **admin** และ Password : **admin** (หรือ password ที่คุณตั้งไว้)



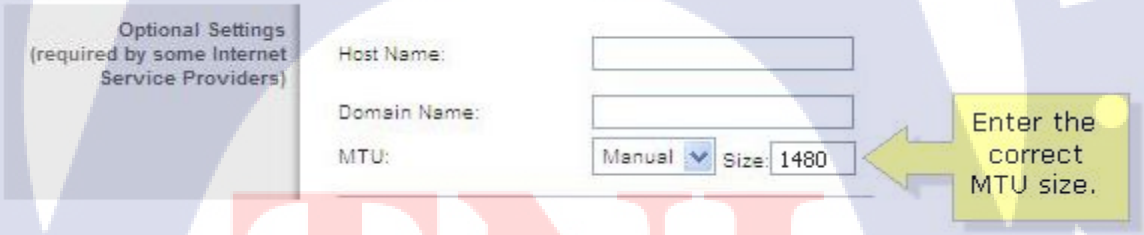
รูปที่ 2.18 ใส่ Username & Password

3. ไปที่แท็บ Basic Setup แล้วเลือก MTU เป็น Manual



รูปที่ 2.19 เลือก MTU เป็น Manual

4. ในช่อง Size ให้ใส่ค่า MTU ที่ถูกต้องลงไป *(สูงสุดไม่เกิน 1500)*



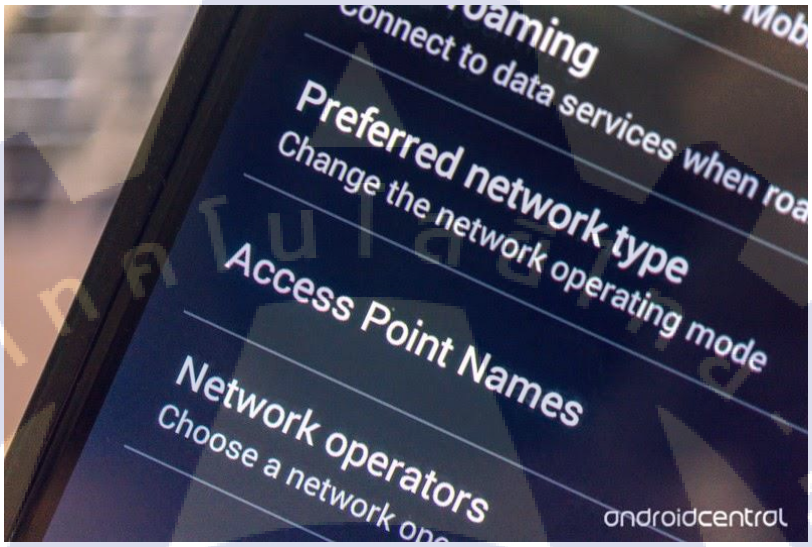
รูปที่ 2.20 ใส่ค่า MTU ที่ถูกต้อง

5. จากนั้นกดปุ่มSave Settingsเพื่อบันทึกการตั้งค่า

รูปที่ 2.21 ปุ่ม Save Settings

2.1.5 Access Point Name (APN)

APN (Access Point Name) เป็นชื่อของเกตเวย์ระหว่างเครือข่ายโทรศัพท์มือถือ GSM, GPRS, 3G หรือ 4G และเครือข่ายคอมพิวเตอร์อื่นซึ่งมักเป็นอินเทอร์เน็ตสาธารณะ



รูปที่ 2.22 APN บน Smartphone

ต้องกำหนดค่าโทรศัพท์มือถือที่ทำการเชื่อมต่อข้อมูลด้วย APN เพื่อนำเสนอให้กับผู้ให้บริการ ผู้ให้บริการจะตรวจสอบตัวระบุนี้เพื่อกำหนดประเภทของการเชื่อมต่อเครือข่ายตัวอย่างเช่นควรกำหนดที่อยู่ IP ให้กับอุปกรณ์ไร้สายวิธีการรักษาความปลอดภัยที่ควรใช้และวิธีการหรือควรเชื่อมต่อกับเครือข่ายลูกค้าภาคเอกชนบางส่วน

โดยเฉพาะอย่างยิ่ง APN ระบุเครือข่ายข้อมูลแพคเก็ต (PDN) ที่ผู้ใช้ข้อมูลมือถือต้องการสื่อสารด้วย นอกเหนือจากการระบุ PDN แล้ว APN อาจถูกใช้เพื่อกำหนดประเภทของบริการ (เช่นการเชื่อมต่อไปยังเซิร์ฟเวอร์ WAP (Wireless Application Protocol), บริการข้อความมัลติมีเดีย (MMS)) ที่จัดเตรียมโดย PDN , APN ใช้ในเครือข่ายการเข้าถึงข้อมูล 3GPP เช่น General Packet Radio Service (GPRS), evolved packet core (EPC)

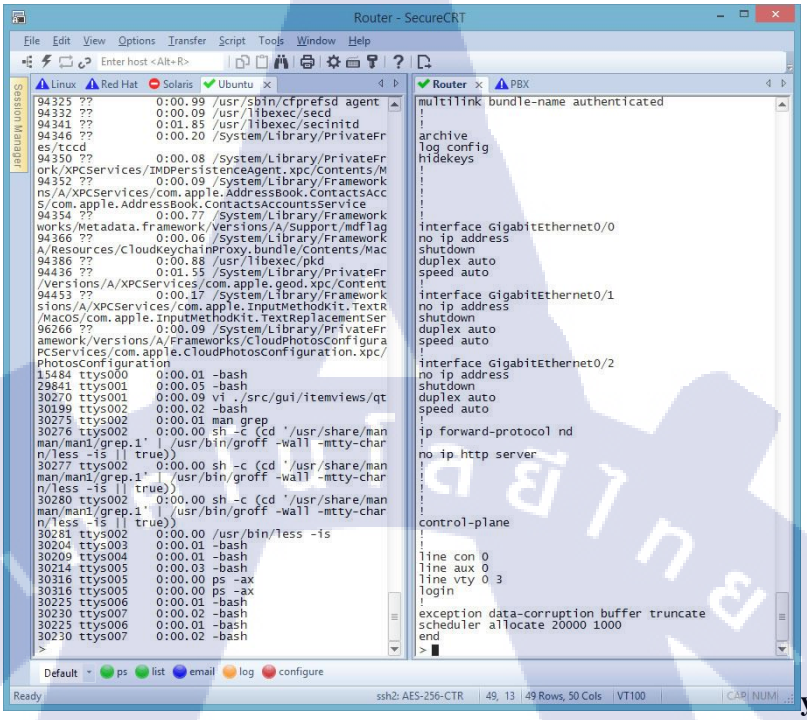
2.2 เทคโนโลยีที่ใช้ในการปฏิบัติงาน

2.2.1 SecureCRT

SecureCRT (โปรแกรมป้องกันข้อมูล ป้องกันการรับส่งข้อมูล): โปรแกรม SecureCRT เป็น **โปรแกรมป้องกันข้อมูล** ต่างๆ อาทิเช่นเอาไว้ สำหรับป้องกันรหัสผ่าน (Password) ชื่อผู้ใช้ (User Account) และข้อมูลสำคัญๆ ต่างๆ ด้วยการรวมเอาการจำลองเครื่อง Terminal ที่มีการเข้ารหัสข้อมูล ในการรับส่งข้อมูล ระหว่างเครื่องต้นทาง ไปยังเครื่องปลายทาง ในการใช้ โพรโตคอล Secure Shell (SSH) เข้าไว้ด้วยกัน

โปรแกรมนี้สามารถทำงานได้หลายวัตถุประสงค์ ทั้งวัตถุประสงค์ ทั้งนำไปใช้ในทางธุรกิจ การจัดการเครือข่าย หรือ การรักษาความปลอดภัยของข้อมูล และงานพัฒนา การเข้าถึงโปรแกรมหลัก และการ Admin Server เพื่อให้สามารถเข้าถึง ทรัพยากรหลัง Firewall อย่างเช่น E-mail, File และเครื่องพิมพ์ได้อย่างปลอดภัย โปรแกรมนี้เค้ามี Interface แบบ Multi-Session Tab พร้อมด้วยคุณสมบัติในการจัดการ ได้อีกด้วย

รูปที่ 2.23 ไอคอน โปรแกรม SecureCRT



yy

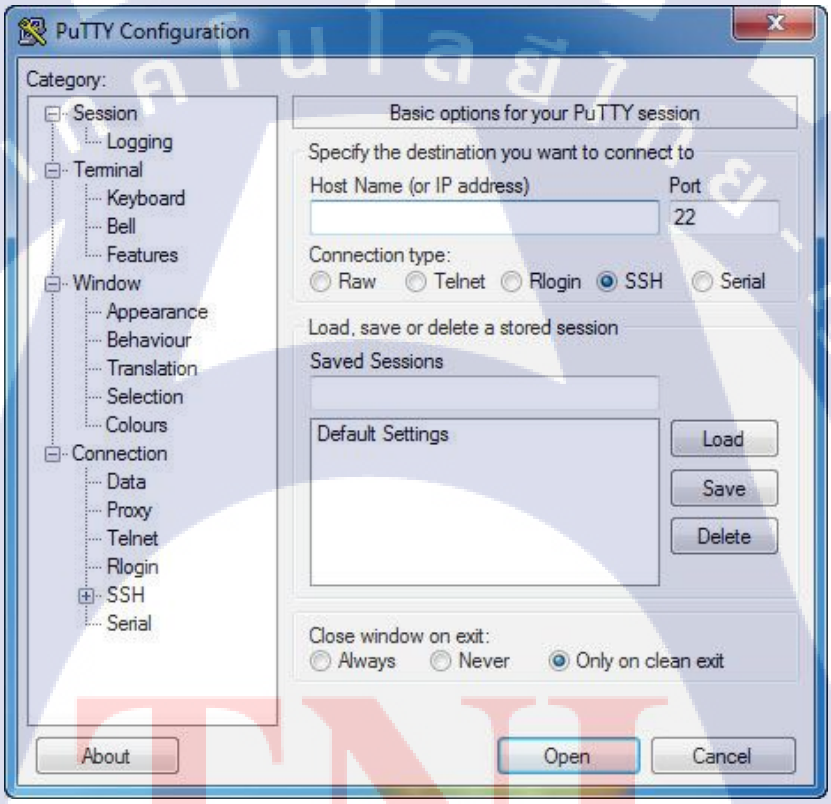
รูปที่ 2.24 หน้าตาโปรแกรม SecureCRT

2.2.2 Putty

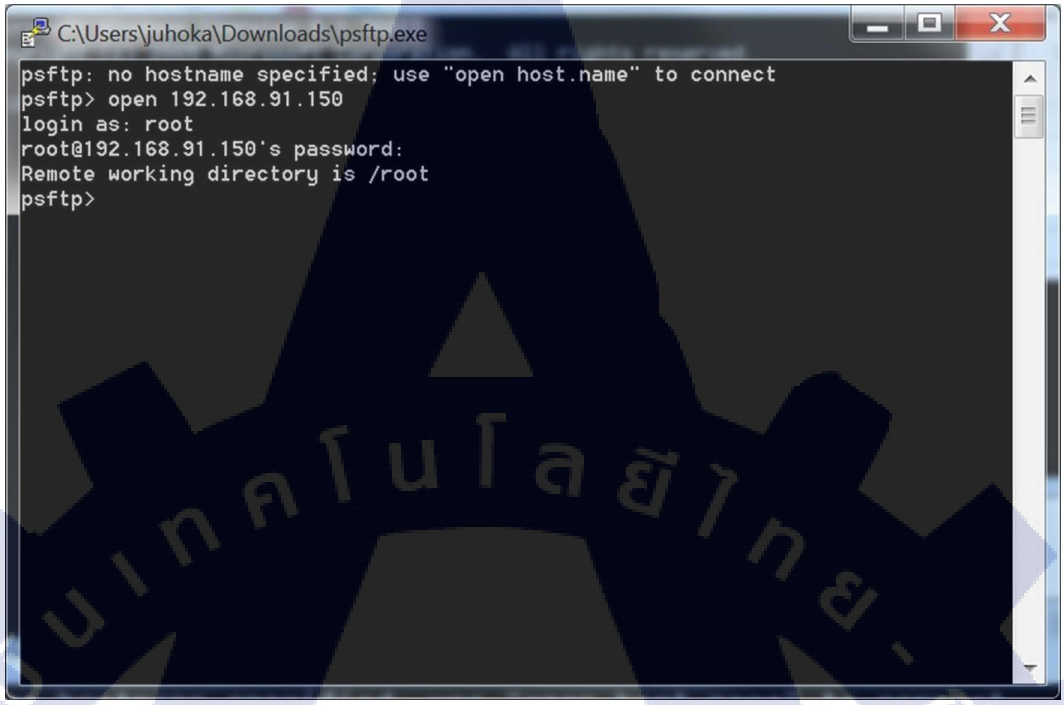
Putty เป็นโปรแกรมสำหรับเหล่าบรรดาผู้ดูแลระบบ (System Administrator) ทั้งหลายเพื่อนำไปใช้ในการเชื่อมต่อหรือremote จากเครื่องคอมพิวเตอร์ตัวเอง (Windows) เข้าไปยังเครื่องServerที่ส่วนมากแล้วจะใช้ระบบปฏิบัติการ Linux ที่ต้องการจะเชื่อมต่อ ได้อย่างง่ายๆ

โปรแกรมนี้ที่ถือกำเนิดตั้งแต่ปี ค.ศ.1997 จนถึงปัจจุบัน เป็นโปรแกรมที่มีหน้าที่เอาไว้ ใช้ในการ Remote หรือติดต่อ เชื่อมต่อ ไปยังเครื่องคอมพิวเตอร์อีกเครื่องหนึ่ง โดยวิธีการ Telnet หรือ Secure Shell (SSH) จากเครื่องลูก (Client) เข้าไปจัดการ พิมพ์คำสั่ง หรือส่งคำสั่ง ในเครื่องแม่ (Server) ด้วยระบบ Command-line Interface (ใช้พิมพ์คำสั่ง) โดยให้ความรู้สึกเหมือนนั่งอยู่บนหน้าเครื่องServer (เครื่องแม่) จริงๆ โดยไม่ต้องเดินทางไปนั่งหน้าเครื่องนั้นจริงๆ โดยอยู่ที่ไหนในโลกก็สามารถเข้าไปได้ และถึงแม้จะเป็นเพียงเป็นข้อความ แต่คุณสามารถเปลี่ยนฟ้อนต์ ปรับเปลี่ยนขนาด สีพื้นหลัง สีตัวอักษรต่างๆ ได้ตามใจชอบ ให้เหมาะกับการใช้งานของตัวเองได้

รูปที่ 2.25 ไอคอน โปรแกรมPutty



รูปที่ 2.26 หน้าตาของโปรแกรม Putty รูปที่1



รูปที่ 2.27 หน้าตาของโปรแกรม Putty รูปที่2

2.2.3 Microsoft Office Visio 2016

Visio เป็นโปรแกรมที่ถูกสร้างขึ้นมาเพื่อช่วยในการสร้างFlow Chart หรือ Diagram ของงานในสาขาต่างๆ ให้ทำได้ง่ายขึ้น ลักษณะที่สำคัญอย่างหนึ่งของการสร้าง Flow Chart บน Visio คือ มีรูปไดอะแกรมพื้นฐานต่างๆ จัดเตรียมไว้ให้

ข้อดีของโปรแกรม Visio คือ เป็นโปรแกรมที่ถูกสร้างให้สนับสนุนการทำงานกับโปรแกรมออฟฟิศอื่นๆได้ เป็นอย่างดี โดยเฉพาะ Microsoft Office

ซอฟต์แวร์ Visio เป็นซอฟต์แวร์ที่ช่วยสร้างกราฟฟิกและแผนภูมิได้ง่ายดายอย่างมีประสิทธิภาพเพื่ออำนวยความสะดวกให้กับองค์กรที่ต้องใช้กราฟฟิก แผนภูมิ แผนผัง และตารางต่างๆ ในการนำเสนองานรวมทั้งการสร้างบนเว็บไซต์

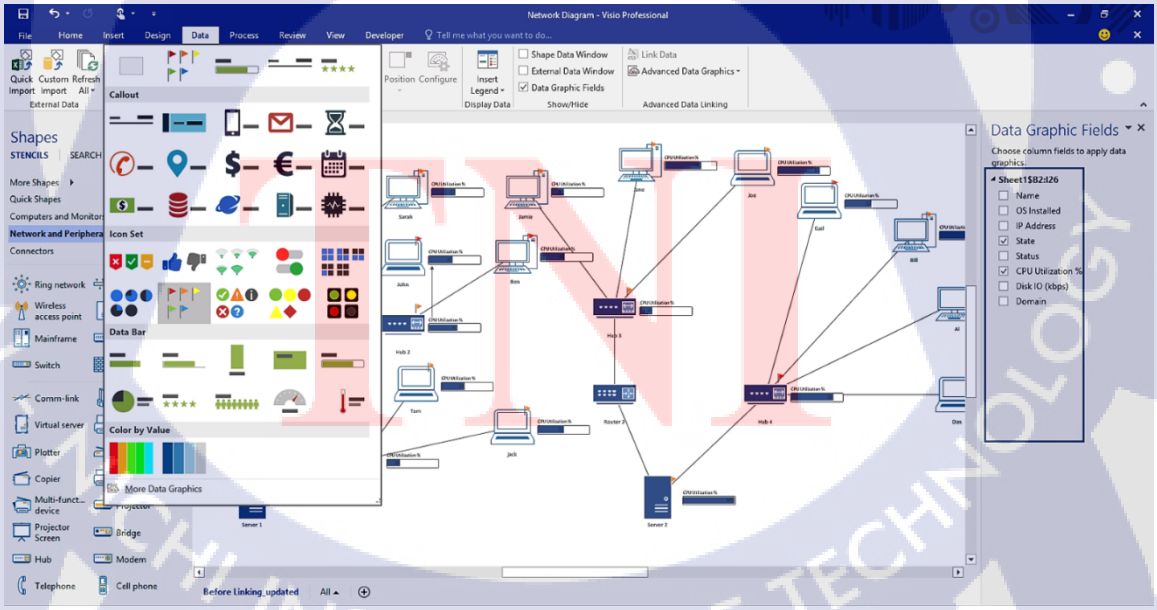
รูปที่ 2.28 ไอคอน โปรแกรม Microsoft Office Visio 2016

Visio เป็นเครื่องมือที่เสริมการทำงานของ Microsoft Office ในการช่วยให้สร้างแผนภูมิ แผนผัง ตารางแสดงโครงสร้างองค์กร แผนภูมิทางการตลาด ตารางเวลา และอื่นๆ ได้อย่างง่ายดาย รวมทั้งช่วยเพิ่มประสิทธิภาพในการสื่อสารโดยช่วยให้แต่ละแผนกสามารถดูแผนภูมิหรือตารางในรูปแบบไฟล์ที่แตกต่างกันตามต้องการได้ เช่น ไฟล์ที่ส่งทางอี-เมล์, ระบบอินทราเน็ต และ อินเทอร์เน็ต เป็นต้น และยังช่วยให้ผู้จัดทำเอกสารสร้างภาพกราฟฟิกใหม่ๆ แปลกๆ ได้สะดวก เพื่อเพิ่มสีสัน ความชัดเจนให้กับข้อมูลต่างๆ ได้เป็นอย่างดี และที่สำคัญก็คือ Visio 2016 ช่วยประหยัดเวลาในการสร้างเอกสารหรือไฟล์เหล่านี้ได้ถึงหนึ่งเท่าตัว

รูปที่ 2.29 โปรแกรม Microsoft Office Visio 2016

ซอฟต์แวร์ดังกล่าวแบ่งเป็น 4 ประเภทหลัก คือ Visio Standard Edition สำหรับผู้ใช้และองค์กรทั่วไป, Visio Professional Edition สำหรับองค์กรที่ทำงานบนระบบเครือข่ายคอมพิวเตอร์ที่ไม่ซับซ้อนมากนัก, Visio Enterprise Edition สำหรับองค์กรขนาดใหญ่ที่มีระบบเครือข่ายซับซ้อน หรือผู้พัฒนาซอฟต์แวร์, และ Visio Technical Edition สำหรับองค์กรที่ดำเนินธุรกิจด้านวิศวกรรม หรือการผลิต โดยเฉพาะ Visio 2016 เป็นแพลตฟอร์มที่ทรงพลัง คุ้มค่าที่อำนวยให้ผู้ใช้สามารถนำแผนภูมิภาพและกราฟฟิกที่ดูง่าย น่าใช้มาทำงานในการสื่อสารด้วยงานเอกสาร งานนำเสนอในองค์กรและระหว่างองค์กรได้ทุกวัน ดังนั้นการใช้ Visio 2016 ที่สามารถใช้งานร่วมกับโครงสร้างพื้นฐานของไอทีในองค์กรเดิมได้ เป็นอุปกรณ์นำเสนอมาตรฐานขององค์กรนั้นจึงจะทำให้องค์กรจะมีค่าใช้จ่ายโดยรวมลดลง

ประโยชน์ของMicrosoft Visio คือโปรแกรมสำหรับออกแบบภาพ Diagram ต่าง ๆ ไม่ว่าจะเป็นภาพแผนที่ ภาพกราฟฟิก แผนภาพต่าง ๆ สร้าง Flow Chart ของขั้นตอนการทำงาน หลักการคิด (Algorithm) ภาพห้องเรียน ภาพโครงสร้างเครือข่าย (Network Diagram) และแผนภาพอีกหลากหลาย เพื่อใช้อธิบายขั้นตอนการทำงานในชิ้นงานนั้น ๆ แสดงออกมาในรูปแบบของรูปภาพ



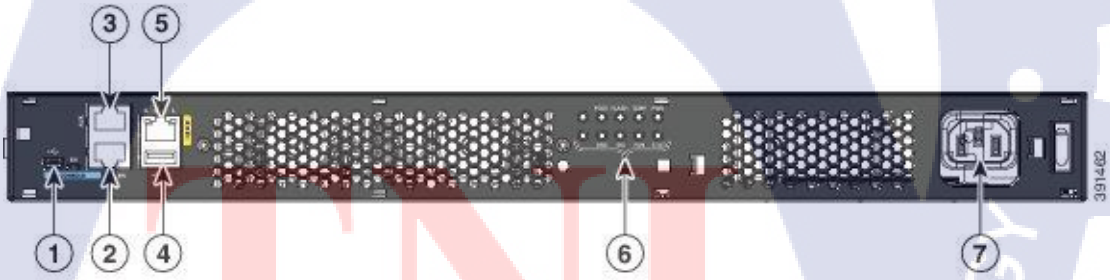
รูปที่ 2.30 ไอคอน โปรแกรม Microsoft Office Visio 2016

2.3 อุปกรณ์ที่ใช้ในการปฏิบัติงาน

2.3.1 Router (Cisco ISR4331-AX/K9)

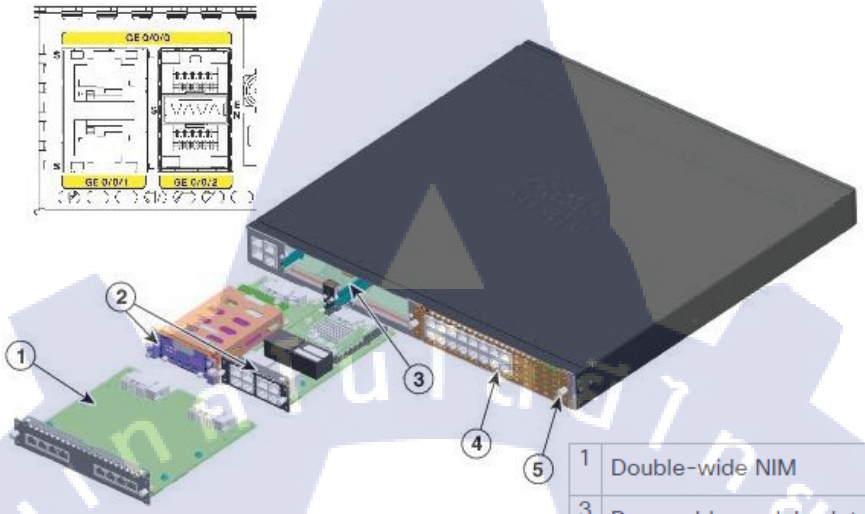
เราเตอร์ (router) เป็นอุปกรณ์คอมพิวเตอร์ที่ทำหน้าที่หาเส้นทางและส่ง(forward)แพ็กเกตข้อมูลระหว่างเครือข่ายคอมพิวเตอร์ ไปยังเครือข่ายปลายทางที่ต้องการ เราเตอร์ทำงานบนเลเยอร์ที่ 3 ตามมาตรฐานของ OSI Model

รูปที่ 2.31 Router รุ่น Cisco ISR4331-AX/K9



1	USB Type B mini port	2	Serial console port
3	AUX port	4	USB Type A port
5	Management port	6	LEDs
7	AC Power		

รูปที่ 2.32 รายละเอียดด้านหลัง Router รุ่น Cisco ISR4331-AX/K9



1	Double-wide NIM	2	NIMs
3	Removable module slot divider	4	SM-X slot
5	Ground connection		

รูปที่ 2.33 รายละเอียดด้านใน Router รุ่น Cisco ISR4331-AX/K9

เราเตอร์มีลักษณะการใช้งานคล้ายกับ สวิตช์ (Switch) ที่มีความสามารถแจกไอพีได้และเราเตอร์เชื่อมต่อเข้ากับสองเส้นทางหรือมากกว่าจากเครือข่ายที่แตกต่างกัน เมื่อแพ็คเก็ตข้อมูลเข้ามาจากเส้นทางหนึ่ง เราเตอร์จะอ่านข้อมูล address ที่อยู่ในแพ็คเก็ตเพื่อค้นหาปลายทางสุดท้าย จากนั้น, ด้วยข้อมูลในตารางเส้นทางหรือนโยบายการส่ง, จะส่งแพ็กเก็ตไปยังเครือข่ายข้างหน้าตามเส้นทางนั้น เราเตอร์จะดำเนินการ "กำกับการจราจร" บนเส้นทางนั้นด้วย แพ็คเก็ตข้อมูลโดยทั่วไปจะถูกส่งจากเราเตอร์หนึ่งไปยังอีกเราเตอร์หนึ่งผ่านเครือข่ายที่เป็น Internetwork จนกว่าจะถึงโหนดปลายทาง

เราเตอร์ประเภทที่คุ้นเคยมากที่สุดคือ เราเตอร์ที่บ้านและสำนักงานขนาดเล็ก ที่เพียงส่งผ่านข้อมูลเช่นหน้าเว็บ, อีเมล์, IM และวิดีโอระหว่างเครื่องคอมพิวเตอร์ที่บ้านและอินเทอร์เน็ต เราเตอร์ดังกล่าวอาจเป็นเคเบิลโมเด็มหรือ DSL โมเด็มที่เชื่อมต่อกับอินเทอร์เน็ตผ่าน ISP เราเตอร์ที่มีความซับซ้อนมากขึ้นเช่นเราเตอร์ขององค์กรธุรกิจเชื่อมต่อกับธุรกิจขนาดใหญ่หรือกับเครือข่ายผู้ให้บริการอินเทอร์เน็ต เข้ากับคอร์เราเตอร์กำลังสูงที่สามารถส่งข้อมูลไปข้างหน้าด้วยความเร็วสูงตามแนวเส้นใยแก้วนำแสงของอินเทอร์เน็ตแบ็คโบน

ในปัจจุบันเราเตอร์ได้ถูกพัฒนาให้มีความสามารถในการใช้งานมากยิ่งขึ้นซึ่งเมื่อก่อนถ้าจะใช้เราเตอร์ในการเชื่อมต่ออินเตอร์เน็ตเราจำเป็นต้องมี โมเด็มในการเชื่อมต่ออินเตอร์เน็ตเสียก่อนแล้วค่อยต่อสายนำสัญญาณมาที่เราเตอร์ และเราเตอร์ก็จะส่งข้อมูลต่างๆให้กับคอมพิวเตอร์ที่เป็นเครื่องลูกข่าย ซึ่งเราสามารถแบ่งเราเตอร์ตามความสามารถได้เป็น 4 ชนิดด้วยกัน

1. เราเตอร์ (Router) เราเตอร์ชนิดนี้เป็นเราเตอร์ที่ไม่สามารถเชื่อมต่ออินเตอร์เน็ตได้ด้วยตัวเอง การทำงานจำเป็นต้องมีอุปกรณ์อื่น ๆเสริมการทำงานด้วย แต่ข้อดีของเราเตอร์แบบนี้คือทำงานตามหน้าที่ได้อย่างเต็มที่และไม่ค่อยมีข้อผิดพลาดในการทำงาน

รูปที่ 2.34 อุปกรณ์ Router

2. โมเด็มเราเตอร์ (Modem Router/ ADSL Modem) โมเด็มประเภทนี้จะเห็นอยู่ในท้องตลาดอย่างมาก เป็นการผนวกความสามารถของโมเด็มและเราเตอร์ไว้ด้วยกัน ซึ่งทำให้สะดวกสบายในการใช้งาน โดยโมเด็มเราเตอร์นี้สามารถเชื่อมต่ออินเตอร์เน็ตความเร็วสูงได้ด้วยตัวเอง และกระจายข้อมูลต่าง ๆไปยังเครื่องคอมพิวเตอร์ที่ทำการเชื่อมต่ออยู่ได้ในทันที ส่วนมากแล้วโมเด็มเราเตอร์จะมี Port LAN มาให้ 4 ช่องด้วยกันซึ่งเป็นพื้นฐานของอุปกรณ์ชนิดนี้

รูปที่ 2.35 อุปกรณ์ Modem Router

3. ไวร์เลสโมเด็มเราเตอร์ (Wireless ADSL Modem Router) เราเตอร์ชนิดนี้จะทำงานได้เหมือนกับโมเด็มเราเตอร์ทุกประการ เพียงแต่มีความสามารถในการปล่อยสัญญาณ wireless ให้กับอุปกรณ์ที่สามารถรับ wireless ได้ โดยพื้นฐานของอุปกรณ์ชนิดจะมี Port LAN 4 พอร์ต และมีเสาสัญญาณที่ใช้ในการกระจายสัญญาณไวไฟจำนวน 2 เสา Router ประเภทนี้ถือว่ามีความสะดวกสบายมากและในปัจจุบันเป็นที่นิยมใช้งานกันมากในตลาด

รูปที่ 2.36 อุปกรณ์ **Wireless ADSL Modem Router**

4. ไวร์เลสเราเตอร์ (Wireless Router) เป็นเราเตอร์ที่ไม่สามารถเชื่อมต่ออินเตอร์เน็ตได้ด้วยตัวเองเหมือนกับประเภทแรก แต่เราเตอร์ประเภทนี้สามารถกระจายสัญญาณอินเตอร์เน็ตที่ได้รับด้วยระบบ wireless ได้และยังกระจายสัญญาณผ่านสายนำสัญญาณจาก Port Lan ทั้ง 4 พอร์ตที่มีการติดตั้งมากับตัวอุปกรณ์ด้วย นอกจากจะเป็น wireless Router แล้วเราเตอร์ประเภทยังสามารถเป็น Access Point ได้อีกด้วย

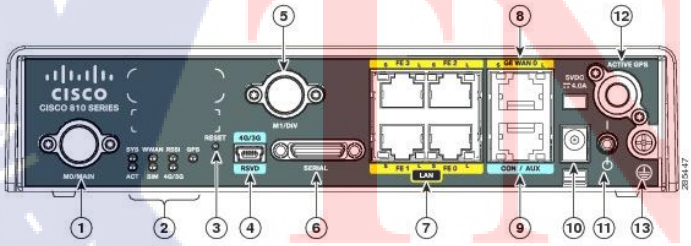
รูปที่ 2.37 อุปกรณ์ **Wireless Router**

2.3.2 3G/4G Router (Cisco 819G-4G-G-K9)

3G/4G Router มีคุณลักษณะทั้งหมดเหมือนกับ Wi-Fi Router มาตรฐาน เพียงแต่ไม่ได้เชื่อมต่ออินเทอร์เน็ตด้วยสายEthernet โดยการเชื่อมต่ออินเทอร์เนตจะเป็นแบบไร้สาย ภายในตัวอุปกรณ์ 3G/4G Router จะมีช่องสำหรับใส่SIM 3G/4G เพื่อรองรับสัญญาณ 3G/4G จากเครือข่ายโทรศัพท์ไร้สาย ซึ่งลักษณะคล้ายคลึงกับวิธีที่สมาร์ทโฟนในยุคปัจจุบันใช้งาน

ประโยชน์หลักของอุปกรณ์ชนิดนี้คือการพกพา คุณสามารถใช้อุปกรณ์ 3G/4G Router ในการสร้างเครือข่ายได้ทุกที่ที่มีสัญญาณ 3G/4G ซึ่งอุปกรณ์บางรุ่นอาจจะมีแหล่งจ่ายไฟในตัว(Battery) หรือไม่มี จึงจำเป็นต้องได้รับพลังงานจากเต้าเสียบ

รูปที่ 2.38 หน้าตา 3G/4G Router รุ่น Cisco 819G-4G-G-K9



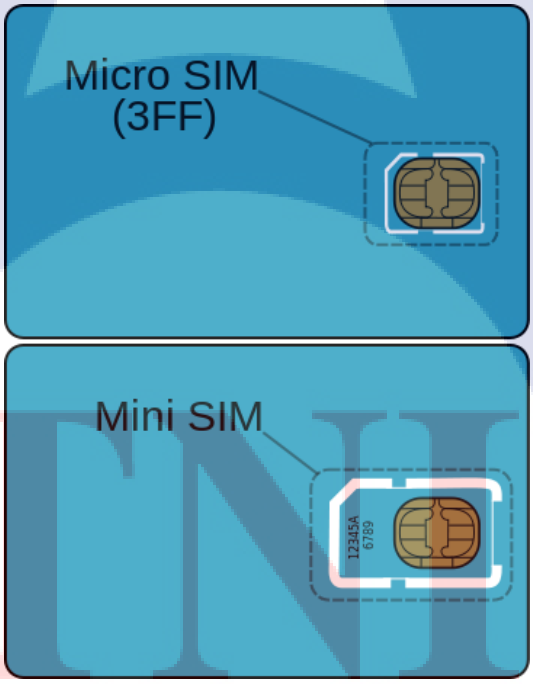
1	4G antenna connector–M0/MAIN	8	GE WAN port
2	LEDs	9	Console/Aux port
3	Reset button	10	Power input
4	4G/3G port	11	Power switch
5	4G antenna connector–M1/DIV	12	Active GPS antenna connector
6	Serial port	13	Ground
7	FE ports		

รูปที่ 2.39 รายละเอียดด้านหลัง 3G/4G Router รุ่น Cisco 819G-4G-G-K9

2.3.2 3G/4G SIM Card

ซิมการ์ด หรือ **Subscriber Identity Module** or **Subscriber Identification Module (SIM)** หมายถึง เกณฑ์ในการแสดงตัว หรือลักษณะเฉพาะของผู้ลงนาม (ผู้ออกเงิน) ซึ่งเก็บรวมรวมข้อมูลอย่างปลอดภัย ใช้พิสูจน์หรือระบุ ผู้ลงนาม บนระบบโทรศัพท์มือถือ ซิมการ์ดสามารถย้ายได้ ระหว่างโทรศัพท์มือถือเครื่องอื่นๆ ซิมการ์ดตัวแรก ผลิตในปี 1991 (พ.ศ. 2534) โดยบริษัท Giesecke & Devrient (G&D) ผู้ผลิตธนบัตร การเงิน smart cards และระบบการจัดการเงิน มีสำนักงานใหญ่ตั้งอยู่ที่เมืองมิวนิก ประเทศเยอรมนี และขาย 300 ซิมการ์ดแรกให้กับ Finnish wireless network operator Radiolinja ประเทศฟินแลนด์

ซิมการ์ดตัวแรก มีขนาดเฉกเช่นบัตรเครดิต (85.60 mm × 53.98 mm × 0.76 mm) ปัจจุบัน มีการพัฒนาทางวัตถุให้มีขนาดเล็กลงของซิมการ์ด เป็นมินิซิมการ์ด(Mini SIM Card) มีความหนาเท่าเดิม แต่มีความยาวและความกว้างลดลง (25 mm × 15 mm) และมีมุมที่ถูกตัดสั้น (trancated)



รูปที่ 2.40 Micro Sim และ Mini Sim

รุ่นใหม่ล่าสุดในปัจจุบัน คือ micro-SIM หรือ 3FF ขนาด 15 mm × 12 mmการ์ดส่วนใหญ่ จะมี 2 ขนาดอยู่ในการ์ดเดียวกัน คือขนาดบัตรเครดิต กับขนาดมาตรฐานที่เล็กกว่า เชื่อมกับพลาสติกเล็กๆ เพื่อง่ายในการหักออกมาใช้

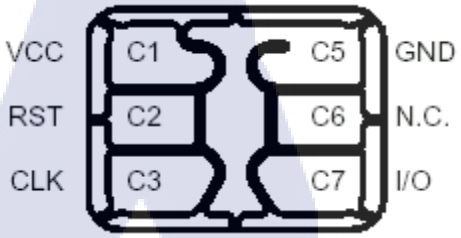
รูปที่ 2.41 Mini Sim กับ Micro Sim จากบริษัท Telia ประเทศสวีเดน

Micro Sim ถูกพัฒนาโดย สถาบันมาตรฐานโทรคมนาคมยุโรป (The European Telecommunications Standards Institute) คู่กันกับอีกหลายๆบริษัท สำหรับเตรียมความเหมาะสมในอุปกรณ์ที่ขนาดเล็กสำหรับ Mini Sim card

ซิมการ์ดมีการระบุ serial number (ICCID) ที่เป็นเอกลักษณ์ในระดับนานาชาติ เป็นหมายเลขเฉพาะที่ไม่ซ้ำกันของผู้ใช้มือถือ หลักการเหมือนกับหมายเลขประจำตัวนักเรียน ซึ่งเปลี่ยนไปตามจำนวนที่มากขึ้น รายการบริการผู้ใช้ ซึ่งต้องการมีการยอมรับ ผ่านสองรหัสผ่าน นั้นคือ

1. PIN (Personal identification number) สำหรับผู้ใช้ทั่วไป
2. PUK (Personal unblocking code) สำหรับเปิดใช้

ซึ่งในปัจจุบันในยุค 3G/4G จึงได้มีซิมการ์ดประเภท 3G/4G SIM Card ออกมาใช้ในปัจจุบัย เพื่อเชื่อมต่ออินเตอร์เน็ตด้วยความเร็วสูง โดยโครงสร้างของ SIM Card จะมีลักษณะเหมือนกับ Smart SIM ในบัตรประชาชน



Pin Definitions and Functions

Card Contact	Symbol	Function
C1	VCC	Supply voltage
C2	RST	Control input (Reset Signal)
C3	CLK	Clock input
C5	GND	Ground
C6	N.C.	Not connected
C7	I/O	Bi-directional data line (open drain)

รูปที่ 2.42 โครงสร้างหน้าสัมผัสของ SIM Card

บทที่ 3

แผนงานการปฏิบัติงาน

ตารางที่ 3.1 แสดงแผนงานการปฏิบัติงานสหกิจศึกษาเป็นเวลา 3 เดือน ประจำปีการศึกษา 2560

หัวข้องาน	เดือน พฤษภาคม				เดือน มิถุนายน				เดือน กรกฎาคม				เดือน สิงหาคม			
ศึกษาเรียนรู้การทำงาน และ Service ของบริษัท																
ปรึกษาโครงงานกับพนักงานที่ปรึกษา																
วางแผนการทำงาน																
ศึกษาอุปกรณ์และวงจรการทำงานของเครือข่าย																
เริ่มลงมือ																
ทำการทดสอบระบบและแก้ไข																
สรุปผลการทำงาน																

ตารางที่ 3.1 แผนงานปฏิบัติ

3.2 รายละเอียดงานที่นักศึกษาปฏิบัติในงานสหกิจ หรือ รายละเอียดโครงงานที่ได้รับมอบหมาย

3.2.1 งานที่ได้รับมอบหมายในส่วนบริการ 3G/4G Back-Up

3.2.1.1 ออกแบบ Network Diagram และนำเสนอในที่ประชุม

3.2.1.2 ติดตั้งและตั้งค่าอุปกรณ์

3.2.1.3 ทดสอบระบบ

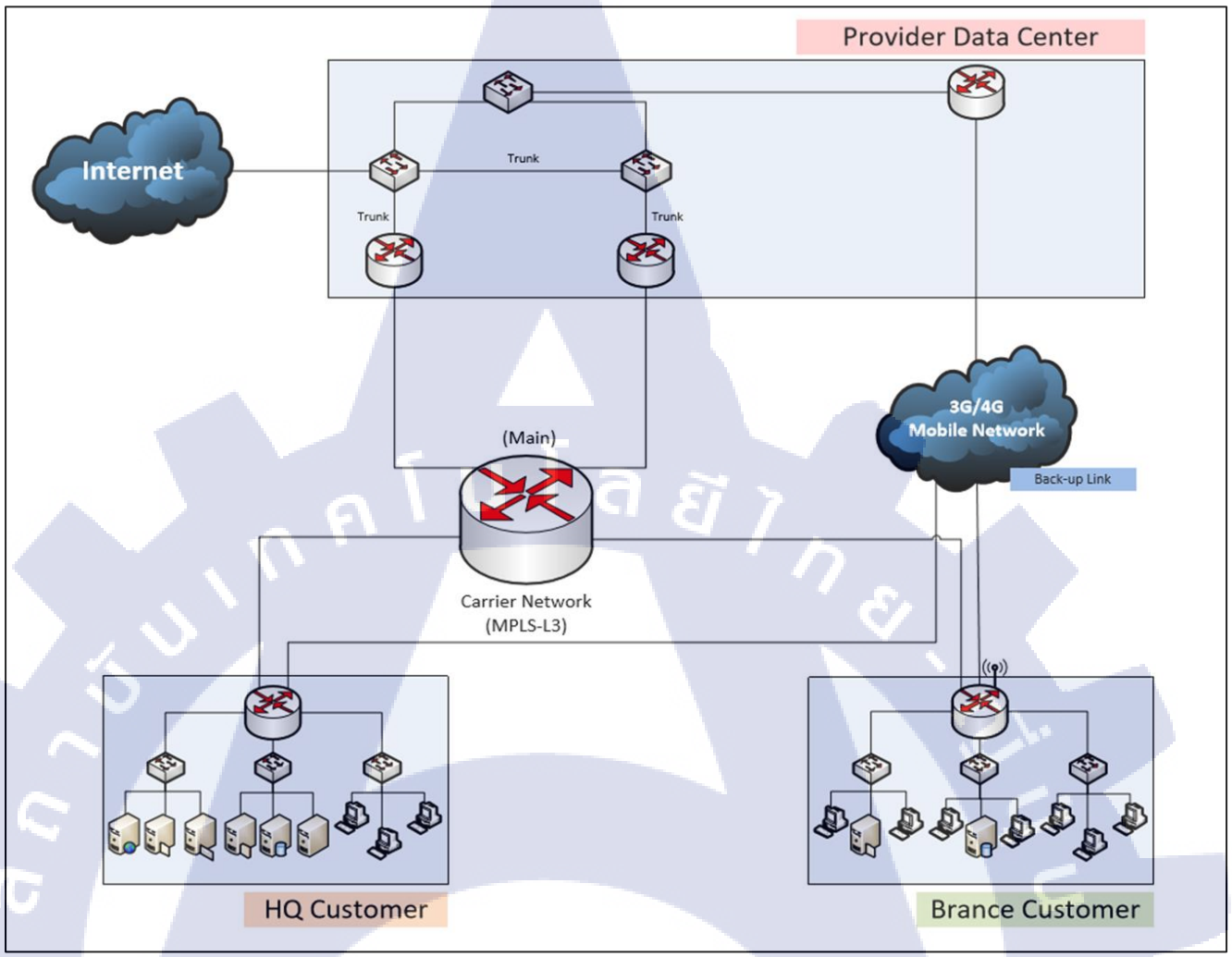
3.2.1.4 ติดตามการทำงานและสำรวจความพึงพอใจของผู้ใช้บริการ

3.3 ขั้นตอนการดำเนินงานที่นักศึกษาปฏิบัติงานหรือโครงงาน

3.3.1 ออกแบบ Network Diagram

เริ่มต้นจากการออกแบบ Network Diagram ของโครงงานว่าโครงสร้างโดยรวมของโครงงานเป็นอย่างไร โดยที่วาดไดอาแกรมโดยใช้โปรแกรม Microsoft Office Visio 2016 เพื่อใช้ในการทำงาน

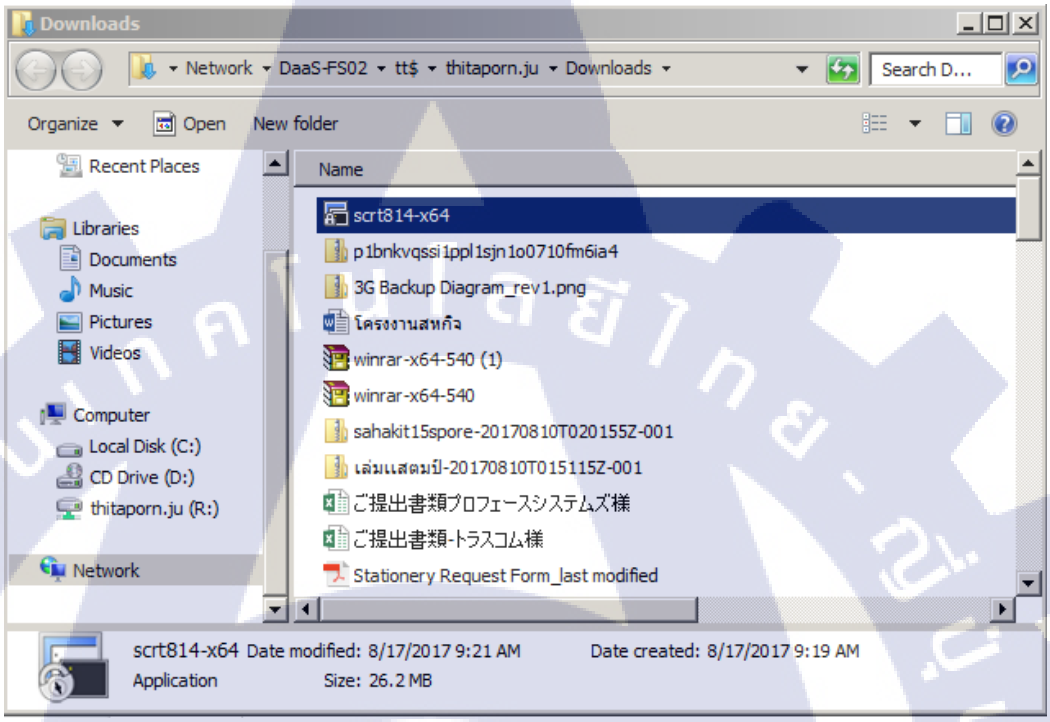
ภายในไดอาแกรม สามารถอธิบายว่า หากเมื่อเส้นทางหลักในการใช้อินเทอร์เน็ตของลูกค้าเกิดขัดข้อง (Down) หรือไม่สามารถใช้งานไปได้ชั่วขณะหนึ่ง การใช้อินเทอร์เน็ตจะถูกสับเปลี่ยนมาใช้เส้นทางสำรองที่ทางเราจัดเตรียมเราไว้เพื่อความต่อเนื่องในการดำเนินธุรกิจของลูกค้า ซึ่งเส้นทางสำรองเราก็ได้เตรียมเอาไว้สองเส้นทางเผื่อหากเส้นทางสำรองหมายเลขหนึ่งเกิดขัดข้องหรืองานไม่ได้ไม่ว่าด้วยสาเหตุอะไรก็จะยังมีเส้นทางสำรองเส้นที่สองที่จะสามารถใช้งานได้จนกว่าเส้นทางการใช้อินเทอร์เน็ตหลักจะกลับมาใช้งานได้ (Up) อีกครั้งหนึ่ง โดยอุปกรณ์ที่จะใช้ในการออกอินเทอร์เน็ตคือ 3G/4G Router โดยภายใน Router จะใส่ 3G/4G SIMS Card เอาไว้และตั้งค่าเพื่อให้สามารถออกอินเทอร์เน็ตได้



รูปที่ 3.1 Network Diagram เขียนโดย Microsoft Office Visio 2016

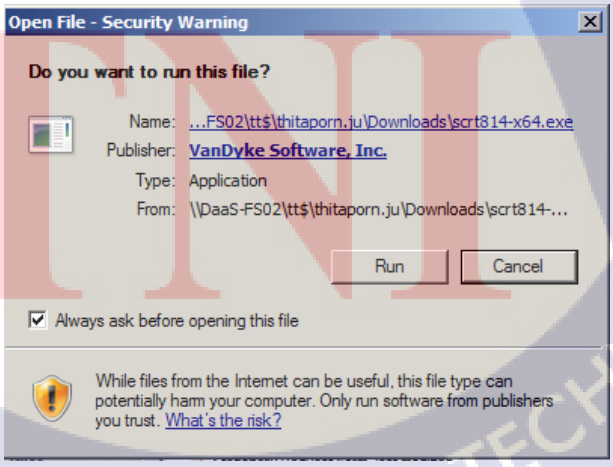
3.3.2 ติดตั้งโปรแกรม SecureCRT

3.3.2.1 ดับเบิ้ลคลิกที่ไฟล์ scrt814-x64.exe ที่ดาวน์โหลดมาเพื่อติดตั้งโปรแกรม



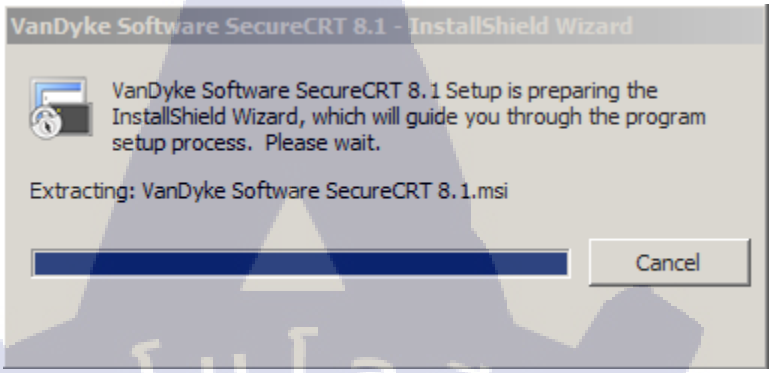
รูปที่ 3.2 เลือกไฟล์ scrt814-x64.exe

3.3.2.2 คลิก Run เพื่อติดตั้งโปรแกรม



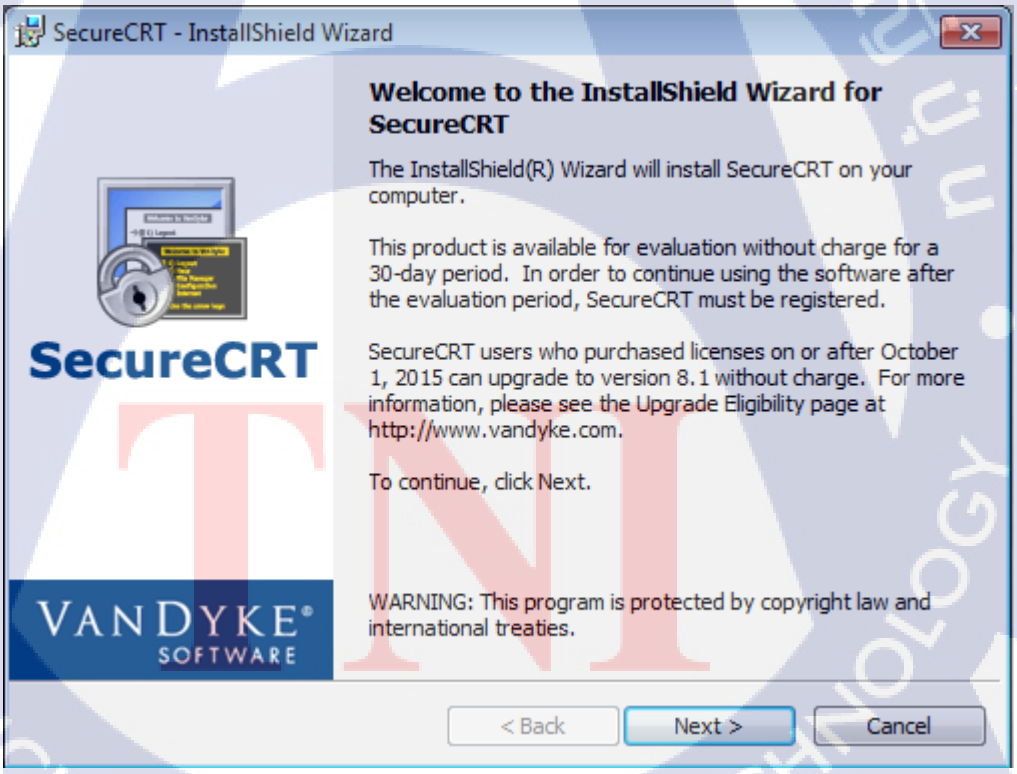
รูปที่ 3.3 คลิก Run เพื่อติดตั้งโปรแกรม

3.3.2.3 ระหว่างที่โปรแกรมกำลังเตรียมข้อมูลของตัวโปรแกรม อย่ากด Cancel เป็นอันขาด



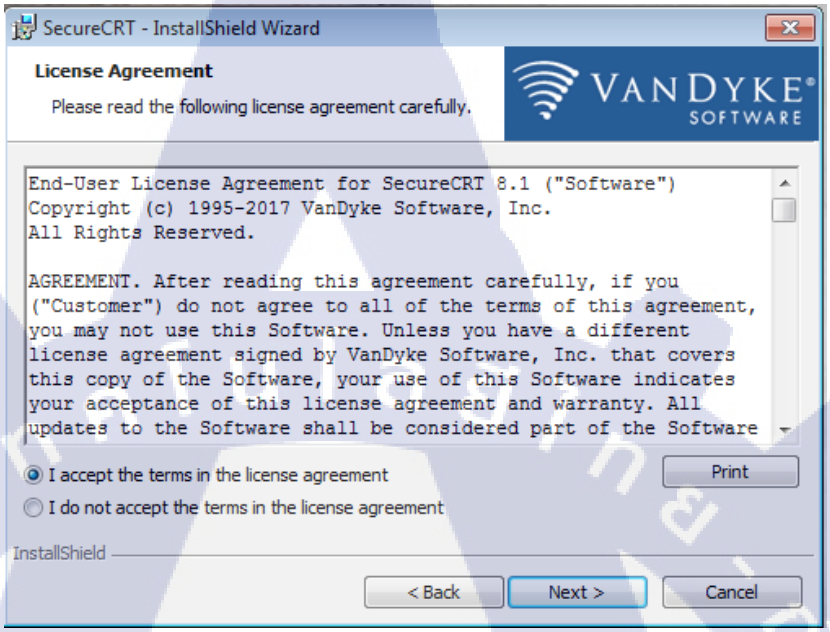
รูปที่ 3.4 รอการเตรียมข้อมูลของโปรแกรม

3.3.2.4 เมื่อหน้าต่างโปรแกรมแสดงขึ้นมาให้คลิก Next เพื่อเข้าสู่ขั้นตอนต่อไปของการติดตั้งโปรแกรม



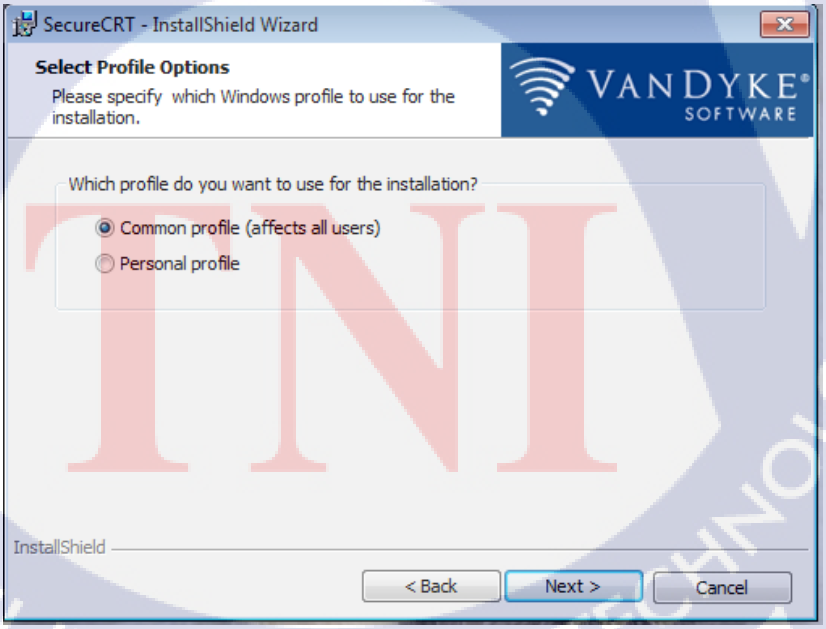
รูปที่ 3.5 หน้าต่างการติดตั้งของโปรแกรม SecureCRT

3.3.2.5 เลือก I accept the terms in the license agreement และคลิก Next



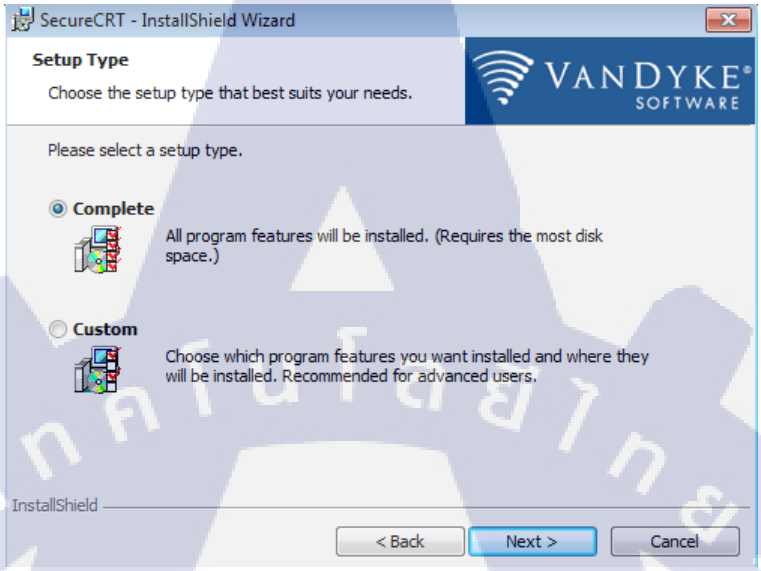
รูปที่ 3.6 เลือก accept เพื่อไปสู่ขั้นตอนต่อไปของการติดตั้งโปรแกรม SecureCRT

3.3.2.6 เลือก Common Profile (affects all users) และคลิก Next เพื่อไปสู่ขั้นตอนต่อไป



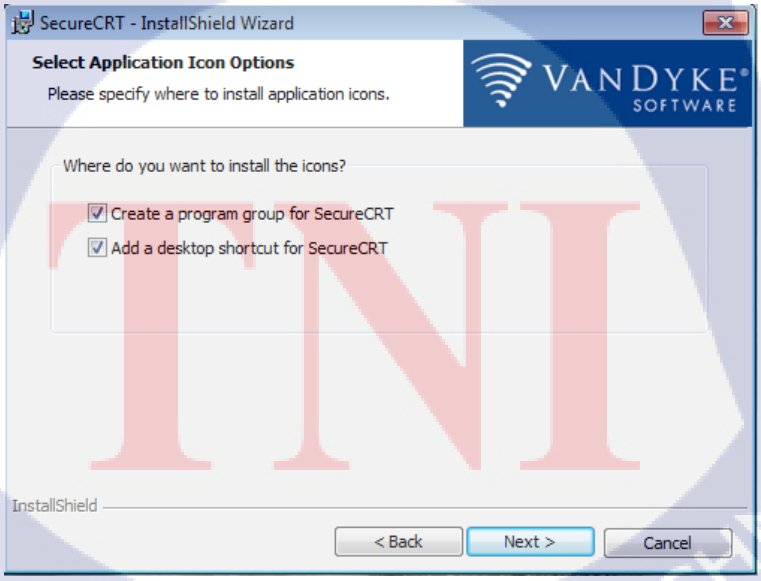
รูปที่ 3.7 เลือก Common Profile

3.3.2.7 เลือก Complete และ คลิก Next เพื่อไปสู่ขั้นตอนต่อไป



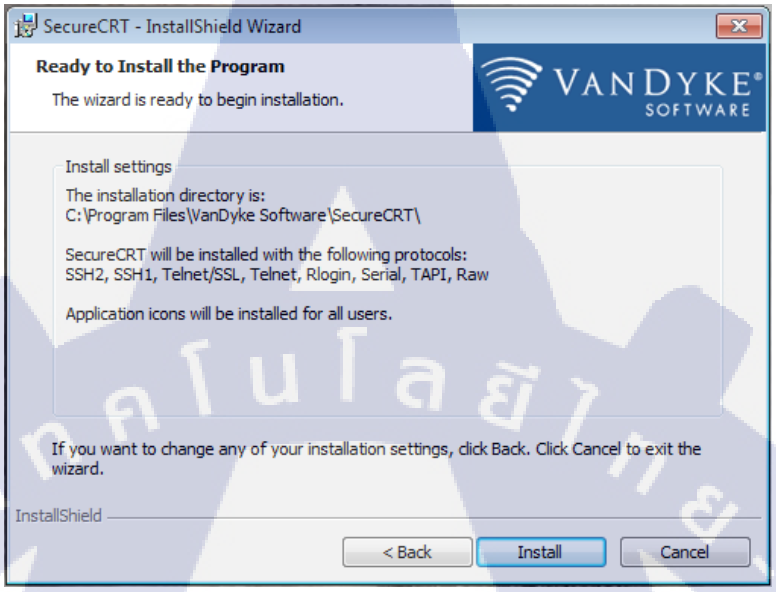
รูปที่ 3.8 เลือก Complete เพื่อติดตั้ง Features ทั้งหมด

3.3.2.8 เลือกทั้ง Create a program group for SecureCRT และ Add a desktop shortcut for SecureCRT เพื่อสะดวกในการใช้งาน และ คลิก Next



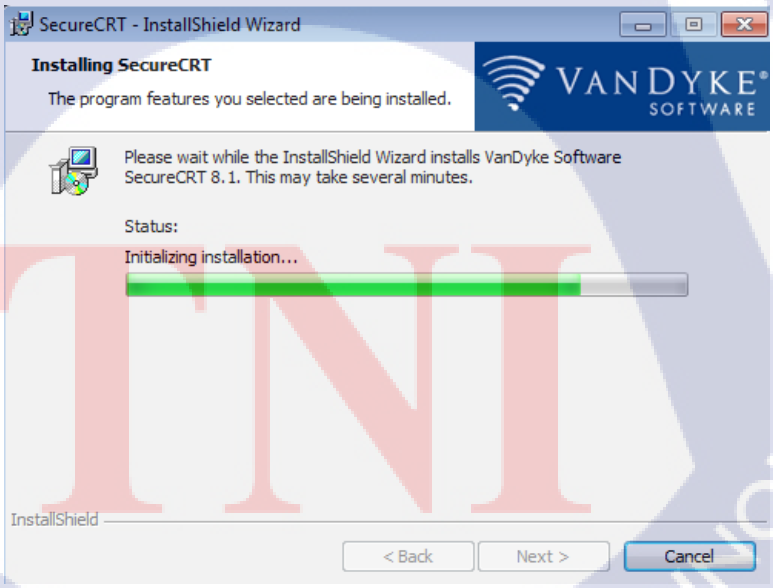
รูปที่ 3.9 เลือก Create a program

3.3.2.9 คลิก Install เพื่อติดตั้งโปรแกรม SecureCRT



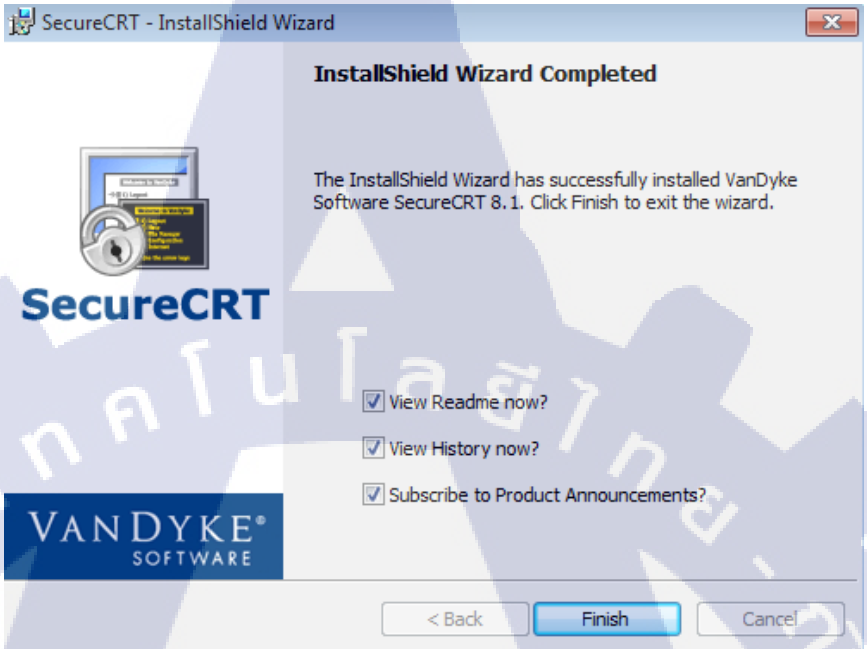
รูปที่ 3.10 คลิก Install เพื่อติดตั้งโปรแกรม SecureCRT

3.3.2.10 รอการติดตั้งของโปรแกรม SecureCRT



รูปที่ 3.11 รอการติดตั้งของโปรแกรม SecureCRT

3.3.2.11 คลิก Finish เพื่อการติดตั้งที่สำเร็จสมบูรณ์



รูปที่ 3.12 การลงโปรแกรม SecureCRT เสร็จสมบูรณ์

3.3.3 ตั้งค่าอุปกรณ์ Router

3.3.3.1 เริ่มจากการสร้าง interface Cellular ขึ้นมาเป็นอันดับแรก โดยในเครื่องของเราจะต้องมี Cellular ที่เป็น Module รุ่นที่รับ Cellular ได้

```
!
interface Cellular0
 ip address negotiated
 ip virtual-reassembly in
 encapsulation slip
 dialer in-band
 dialer pool-member 1
 async mode interactive
!
```

รูปที่ 3.13 สร้าง interface Cellular

3.3.3.2 สร้าง interface Dialer0 ขึ้นมาภายใต้ Cellular0 โดย Cellular0 สามารถสร้าง Dialer ได้หลายอัน แต่กรณีนี้ จะสร้างเพียงแค่ 1 อัน

```
!
interface Dialer0
 ip address negotiated
 ip virtual-reassembly in
 encapsulation slip
 dialer pool 1
 dialer idle-timeout 0
 dialer string lte
 dialer persistent
 dialer-group 1
!
```

รูปที่ 3.14 สร้าง interface Dialer

3.3.3.3 สร้าง Tunnel0 ขึ้นมา และกำหนด IP Address

```
interface Tunnel0
 ip address 10.10.251.36 255.255.255.0
 no ip redirects
```

รูปที่ 3.15 สร้าง Tunnel0

3.3.3.4 เมื่อสร้าง Tunnel0 ขึ้นมา ทำการ Config ให้ IP (10.10.251.36) ฝั่งcarrier สามารถติดต่อกับ IP (10.10.251.1) ฝั่ง Backbone ได้

```
interface Tunnel0
 ip address 10.10.251.36 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 ip nhrp map multicast 172.29.15.6
 ip nhrp map 10.10.251.1 172.29.15.6
 ip nhrp network-id 6
 ip nhrp nhs 10.10.251.1
```

รูปที่ 3.16 Config IP ฝั่ง และ ฝั่ง Backbone

3.3.3.5 เมื่อทำให้ IP ทั้งสองฝั่งติดต่อกันได้แล้ว จึงได้ทำการเพิ่มความ Security โดยการใช้ KEY และ IPSec ในการตรวจสอบการเชื่อมต่อของระบบเครือข่าย ว่าสามารถทำการติดต่อสื่อสารระหว่างอุปกรณ์ที่จะใช้ในการ IPSec VPN ได้อย่างปกติ และทำการออกแบบรูปแบบและรายละเอียดที่จะใช้ในการรักษาความปลอดภัยของข้อมูล รวมถึงการเปิดการทำงานของ ISAKMP บน Interface ที่ใช้ติดต่อสื่อสารกับอุปกรณ์ IPSec ฝั่งตรงข้าม

โดยการตั้งค่า ISAKMP Policy Set เพื่อใช้ในการสร้าง ISAKMP SA โดยจะต้องทำการกำหนดค่าให้ตรงกันระว่างอุปกรณ์ที่ใช้ในการทำ IPSec VPN ซึ่งจะต้องมีค่าที่ต้องทำการกำหนด ได้แก่

Authentication กำหนดวิธีการที่จะใช้ในการพิสูจน์ตัวตน โดยครั้งนี้เราเลือกใช้ Pre-shared Key

Encryption เลือก algorithm ที่จะใช้ในการเข้ารหัสข้อมูล โดยครั้งนี้เราเลือกใช้ AES

Hash เลือก algorithm ที่จะใช้ในการตรวจสอบความถูกต้องของข้อมูล โดยจะมีตัวเลือกเรียงตามระดับความปลอดภัย โดยครั้งนี้เราเลือกใช้ SHA

DH Group เลือกขนาดของจำนวนเฉพาะที่จะนำมาใช้ในการแลกเปลี่ยน Key ระหว่างอุปกรณ์ โดยจะมีตัวเลือก เรียงตามระดับการรักษาความปลอดภัย โดยครั้งนี้เราเลือกใช้ group 5 (1536 bit)

```
!
crypto keyring POC_XXX_KEYRING
  pre-shared-key address 0.0.0.0 0.0.0.0 key POC_XXX_KEY
!
crypto isakmp policy 1
 encr aes
 hash sha256
 authentication pre-share
 group 5
```

รูปที่ 3.17 การตั้งค่า IPSec โดยเปิดการทำงานของ ISAKMP Policy Set

3.3.3.6 จากนั้นทำการตั้งค่า KEY ให้กับ isakmp โดยที่ IP ของ Router ฝั่งตรงข้าม เป็นอะไร KEY ก็ต้องเหมือนกันด้วย

```
crypto isakmp profile POC_XXX_ISAKMP
   keyring POC_XXX_KEYRING
   match identity address 0.0.0.0
```

รูปที่ 3.18 ตั้งค่า KEY ให้กับ isakmp

3.3.3.7 เมื่อทำการ Config ค่า isakmp ก็ทำการจัดหมวดหมู่เงื่อนไขของ IPSec โดยให้เงื่อนไขของ isakmp ภายใต้ชื่อ “transform-set” และอยู่ในโหมด Transport ดังตามรูป

```
!
crypto ipsec transform-set POC_XXX_SET esp-aes esp-sha256-hmac
 mode transport
!
```

รูปที่ 3.19 จัดหมวดเงื่อนไขของ isakmp ภายใต้ชื่อ “transform-set”

3.3.3.8 ทำ IPSec Profile โดยตั้งชื่อว่า “POC_XXX_IPSEC” เพื่อง่ายต่อการนำไปใช้ในการเข้ารหัสแก่ Tunnel อื่น โดนต้องผ่านเงื่อนไข 2 Set ที่อยู่ภายใน Profile “POC_XXX_IPSEC”

```
!
crypto ipsec profile POC_XXX_IPSEC
 set transform-set POC_XXX_SET
 set isakmp-profile POC_XXX_ISAKMP
!
```

รูปที่ 3.20 ทำ IPSec Profile

3.3.3.9 จากนั้น กลับเข้าที่ interface Tunnel0 เพื่อเพิ่มเงื่อนไข IPSec (บรรทัดสุดท้าย) โดยภายใต้ชื่อ Profile “POC_XXX_IPSEC” ได้มีเงื่อนไขใน transform-set และ isakmp-profile จากที่ตั้งเอาไว้ในเมื่อ ข้อ 3.3.3.5 – 3.3.3.8 โดยเมื่อใส่เงื่อนไขไป การที่Router ฝั่งเรา กับฝ่ายตรงข้าม จะติดต่อสื่อสารกันได้นั้นจำเป็นต้องมี KEY และ IPSec ที่เหมือนกัน เพื่อเป็นการเพิ่มความปลอดภัยในการติดต่อสื่อสาร ซึ่งถ้าหากเงื่อนไขตรงกัน Tunnel ก็จะ Up ขึ้นมาเอง

```
interface Tunnel0
 ip address 10.10.251.36 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 ip nhrp map multicast 172.29.15.6
 ip nhrp map 10.10.251.1 172.29.15.6
 ip nhrp network-id 6
 ip nhrp nhs 10.10.251.1
 ip nhrp shortcut
 ip virtual-reassembly in
 ip tcp adjust-mss 1360
 tunnel source Dialer0
 tunnel mode gre multipoint
 tunnel key 106
 tunnel protection ipsec profile POC_XXX_IPSEC
```

รูปที่ 3.21 เพิ่มเงื่อนไข IPSec ให้กับ Tunnel0

3.3.3.10 หลังที่ Tunnel ทำการ Up ขึ้นมาแล้ว ในมุมของ Routing ในด้าน Wide Link จะใช้ Dynamic Route โดยครั้งนี้ Routing Protocol เราเลือกใช้ OSFP ในงานนี้ ซึ่งโดยปกติแล้วค่า AD (Administrative Distance) ของ OSPF จะมีค่า เท่ากับ 110 แต่ครั้งนี้ เราตั้งค่าให้ ค่า AD เท่ากับ 250 ซึ่งสามารถอธิบายได้ว่า ในกรณีที่ Link เส้นทางหลักตายหรือเกิดขัดข้องไม่สามารถใช้งานได้จึงจะมาใช้งานที่เส้นทางสำรอง Back-up นี้อัตโนมัติ

```
ip route 0.0.0.0 0.0.0.0 10.10.251.1 250 name 3G-Backup-Link

ip route 172.29.15.6 255.255.255.255 Dialer0 name hub_tunnel_source
```

ค่า AD

รูปที่ 3.22 ตั้งค่า AD ให้กับ OSPF

3.3.3.11 เมื่อทำการ show run ออกมาในรูปแบบดังรูป

```
!
crypto keyring POC_XXX_KEYRING
  pre-shared-key address 0.0.0.0 0.0.0.0 key POC_XXX_KEY
!
crypto isakmp policy 1
 encr aes
 hash sha256
 authentication pre-share
 group 5
crypto isakmp profile POC_XXX_ISAKMP
   keyring POC_XXX_KEYRING
   match identity address 0.0.0.0
!
!
crypto ipsec transform-set POC_XXX_SET esp-aes esp-sha256-hmac
 mode transport
!
crypto ipsec profile POC_XXX_IPSEC
 set transform-set POC_XXX_SET
 set isakmp-profile POC_XXX_ISAKMP
!
```

รูปที่ 3.23 Show run รูปที่ 1

```
interface Tunnel0
 ip address 10.10.251.36 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 ip nhrp map multicast 172.29.15.6
 ip nhrp map 10.10.251.1 172.29.15.6
 ip nhrp network-id 6
 ip nhrp nhs 10.10.251.1
 ip nhrp shortcut
 ip virtual-reassembly in
 ip tcp adjust-mss 1360
 tunnel source Dialer0
 tunnel mode gre multipoint
 tunnel key 106
 tunnel protection ipsec profile POC_XXX_IPSEC
!
interface Cellular0
 ip address negotiated
 ip virtual-reassembly in
 encapsulation slip
 dialer in-band
 dialer pool-member 1
 async mode interactive
!
interface Dialer0
 ip address negotiated
 ip virtual-reassembly in
 encapsulation slip
 dialer pool 1
 dialer idle-timeout 0
 dialer string lte
 dialer persistent
 dialer-group 1
!
```

รูปที่ 3.24 Show run รูปที่ 2

```
ip route 0.0.0.0 0.0.0.0 10.10.251.1 250 name 3G-Backup-Link

ip route 172.29.15.6 255.255.255.255 Dialer0 name
hub_tunnel_source

!
interface Tunnel0
 ip address 10.10.251.36 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 ip nhrp map multicast 172.29.15.6
 ip nhrp map 10.10.251.1 172.29.15.6
 ip nhrp network-id 6
 ip nhrp nhs 10.10.251.1
 ip nhrp shortcut
 ip virtual-reassembly in
 ip tcp adjust-mss 1360
 tunnel source Dialer0
 tunnel mode gre multipoint
 tunnel key 106
 tunnel protection ipsec profile POC_XXX_IPSEC
!
```

รูปที่ 3.25 Show run รูปที่ 3

บทที่ 4

สรุปผลการดำเนินงาน การวิเคราะห์และสรุปผลต่างๆ

4.1 ผลการดำเนินงาน

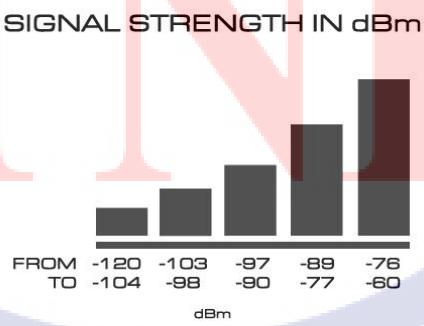
จากผลที่ได้จากการปฏิบัติงานสหกิจศึกษาที่บริษัทบริษัท เอ็นทีที คอมมิวนิเคชั่นส์(ประเทศไทย) จำกัด ในครั้งนี้ได้มีโอกาสเข้าร่วมในการทำระบบ 3G/4G Back-up Link และทำการทดสอบระบบที่ได้นำไปเป็น Services ให้แก่ลูกค้ารายหนึ่งของบริษัท อีกทั้งยังมีโอกาสได้เข้าไปเยี่ยมชม Data Center ของบริษัท เอ็นทีที ทั้งสองสาขา (สาขา บางนา และ สาขาอมตะนคร) ทำให้มีความรู้และประสบการณ์ในการทำงานเพื่อนำไปพัฒนาตนเองในอนาคตได้

4.1.1 ผลของการดำเนินการทดสอบระบบ ได้ผลการทดสอบออกมาเป็น 3 แบบ คือ

4.1.1.1 Test Signal Strength

โดยพิจารณาจากตัวเลขของ Signal Strength ที่แสดงออกมาโดยมีหน่วย dBm ซึ่งส่วนใหญ่จะแสดงเป็นค่า – ถ้าหากมองจากตัวเลขไม่รวมเครื่องหมายลบ “ยิ่งตัวเลขมีค่าน้อยแสดงว่าดีกว่าตัวเลขที่มีค่ามากกว่า” หรือ อีกแบบหนึ่งคือ “ยิ่งตัวเลขเข้าใกล้ 0 มากเท่าไหร่ยิ่งดี”

หากมองรูปที่ 4.1 จะเห็นได้ว่าเมื่อค่า Signal Strength มีค่าน้อยมากเท่าไหร่ สัญญาณก็จะมีความเข้มมากขึ้นเท่านั้น



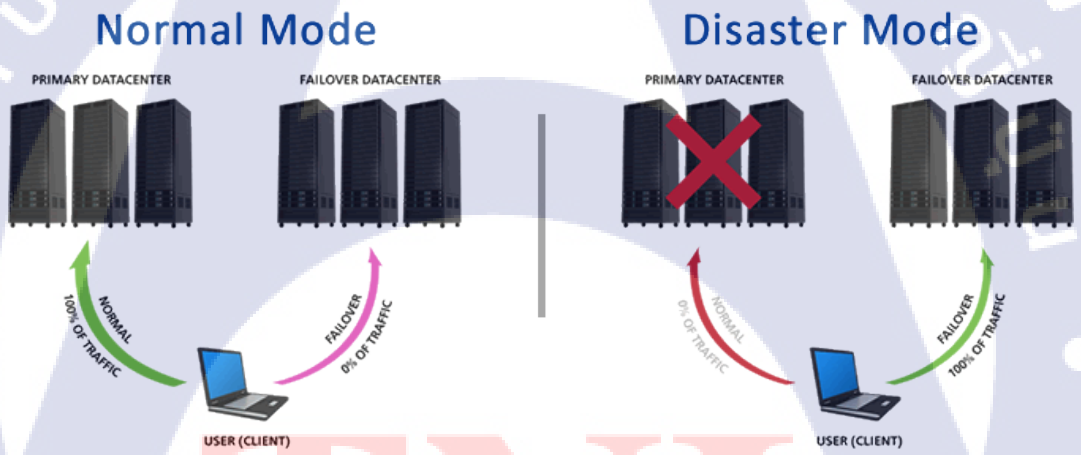
รูปที่ 4.1 กราฟแสดง Signal Strength

4.1.1.2 Test Link Quality

Link Quality คือ ค่าคุณภาพของการเชื่อมต่อ โดยพิจารณาจากการระบุจำนวนPackage ที่ส่งซ้ำแล้วสังเกตุว่าข้อมูลสามารถไหลผ่านได้ดีแค่ไหน

4.1.1.3 Test Failover

ใช้การทดสอบนี้เพื่อต้องการไม่ให้ระบบเกิด Down Time ขึ้น โดยระบบนี้จะใช้ Server อย่างน้อย 2 ตัวในการจัดการ Server ตัวแรก (Active Server) จะเป็นตัวทำงานตามปกติ Server ตัวที่สอง (Backup Server) จะ Stand by ไว้หาก Server ตัวแรกมีปัญหาขัดข้อง Server ตัวที่สองจะทำงานทันทีหลังจากนั้นภายใน 1นาที โดยข้อมูลทั้งหมดจะมีการ Update Real Time กับ Server ทั้งสองเครื่องเพราะฉะนั้นจะไม่มี ข้อมูลใดๆสูญหายหรือไม่ Update หาก Server เครื่องแรกมีปัญหา



รูปที่ 4.2 Failover System

4.2 ผลการวิเคราะห์ข้อมูล

4.2.1 ทดสอบ Signal Strength

โดยการแสดงความเข้มของสัญญาณของ 4G LTE back-up Link โดยใช้คำสั่ง “show cellular 0 radio”

```
Customer0 # show cellular 0 radio
Radio power mode = ON
LTE Rx Channel Number =  1425
LTE Tx Channel Number =  19425
LTE Band =  3
LTE Bandwidth = 15 MHz
Current RSSI = -41 dBm
Current RSRP = -69 dBm
Current RSRQ = -9 dB
Current SNR = 8.2  dB
Radio Access Technology(RAT) Preference = AUTO
Radio Access Technology(RAT) Selected = LTE
Customer0 #
Customer0 #
Customer0 # show cellular 0 radio
Radio power mode = ON
LTE Rx Channel Number =  1425
LTE Tx Channel Number =  19425
LTE Band =  3
LTE Bandwidth = 15 MHz
Current RSSI = -43 dBm
Current RSRP = -68 dBm
Current RSRQ = -7 dB
Current SNR = 12.6  dB
Radio Access Technology(RAT) Preference = AUTO
Radi                ology(RAT) Selected = LTE
Customer0 #show clock
*17:24:06.426 ICT Wed May 3 2017
```

รูปที่ 4.3 ทดสอบ Signal Strength

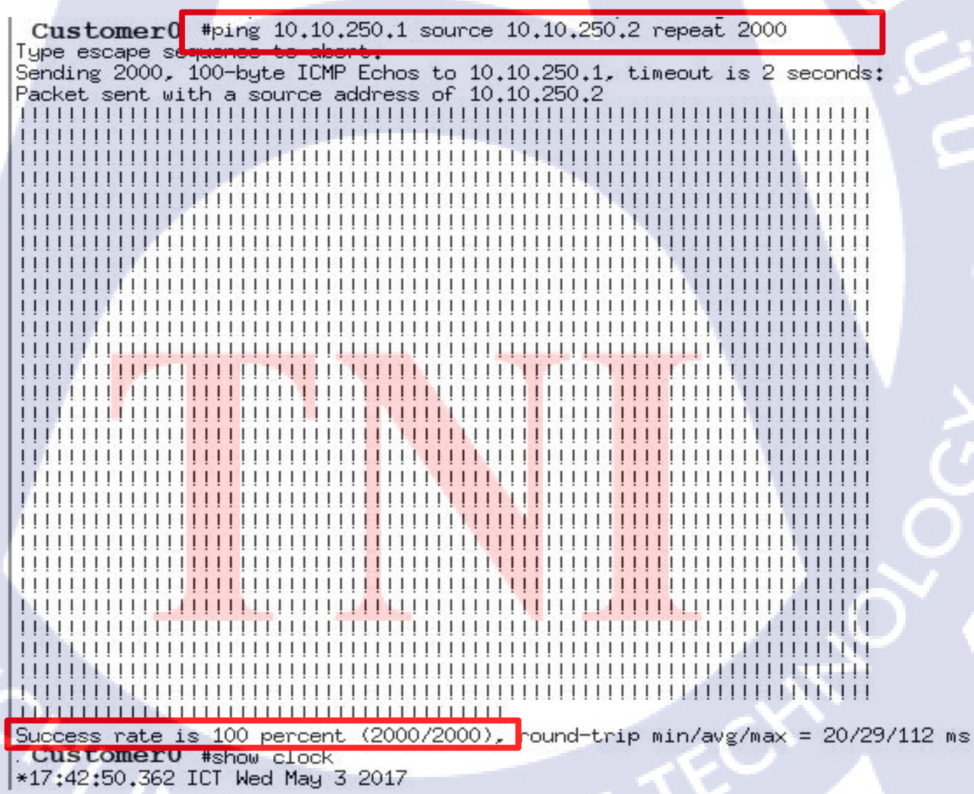
(ภายในภาพใช้คำว่า Customer0 แทนชื่อ site งานจริง เนื่องจากไม่สามารถเปิดเผยได้ภายใต้ Policy ของบริษัทเอ็นทีที คอมมิวนิเคชั่น (ไทยแลนด์) จำกัด)

จากรูปที่ 4.3 จะเห็นได้ว่า Current RSSI = -41 dBm (RSSI ควรดีกว่า -90 dBm สำหรับการเชื่อมต่อที่มั่นคงและเชื่อถือได้)ซึ่ งหมายความว่า ความเข้มของสัญญาณอยู่ระดับที่ดีมาก สามารถเขียนสรุปออกมาเป็นตารางได้ดังตารางที่ 4.1

RSSI (Received Signal Strength Indicator)	Lower -100 dBm **Low**	During -99 to -90 dBm **Low or medium**	During -89 to -70 dBm **Medium**	-69 dBm or higher **High**	**Result**
				-41	**OK**

ตารางที่ 4.1 ผลการ Test Signal Strength

4.2.2 ทดสอบคุณภาพของ Link 4G Back-up โดยใช้คำสั่ง ping



รูปที่ 4.4 ทดสอบ Link Quality

โดยการ ping และใส่ค่า repeat = 2000 เพื่อทดสอบข้อมูลของ Package ที่ส่งซ้ำๆ ไป การไหลของข้อมูลจะยังสามารถไหลเวียนได้อย่างปกติไหม ปรากฏว่า ข้อมูลสามารถไหลเวียนได้อย่างราบรื่นและมีประสิทธิภาพ จึงสามารถสรุปได้ดังตาราง ที่ 4.2

Site	Central 3G router at NTT DC Bangna	Ping Setup	Statistic			Result
		Packet count	**Min**	**Max**	**Average**	**Result**
	10.10.250.1	2000	20	112	29	**OK**

ตารางที่ 4.2 ผลการทดสอบ Link Quality

4.2.3 ทดสอบ Failover

4.2.3.1 ทดสอบ Failover โดยคำสั่ง Traceroute (จากสาขาไปยัง HQ)

ในสถานการณ์ปกติการไหลเวียนของสาขาไปยัง HQ จะดำเนินการวิ่งผ่านทางสายไฟก่อน

```
Customer0    #traceroute 172.17.4.41
Type escape sequence to abort.
Tracing the route to 172.17.4.41
VRF info: (vrf in name/id, vrf out name/id)
  1 10.11.50.145 4 msec 4 msec 4 msec
  2 10.10.254.34 4 msec 4 msec 16 msec
  3 10.10.254.36 4 msec 4 msec 4 msec
  4  *  *  *
  5 172.17.4.41 4 msec 4 msec 8 msec
Customer0    #
```

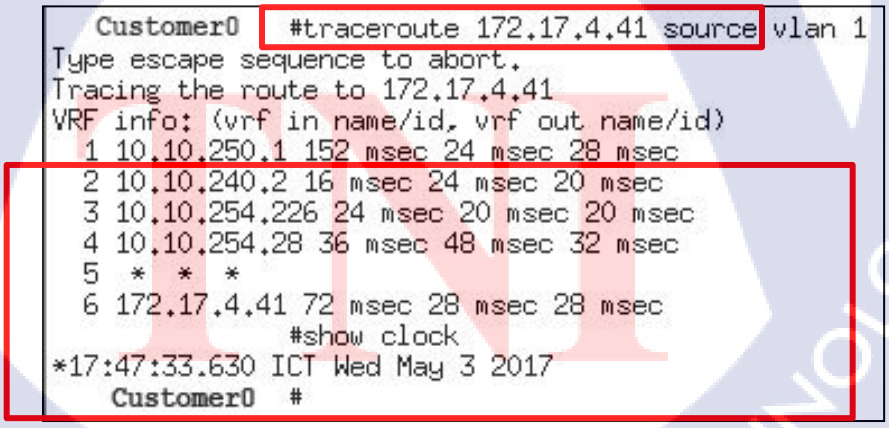
รูปที่ 4.5 ทดสอบ Failover โดยคำสั่ง Traceroute

Source		Destination		Hop	Route	Result
Site	IP Address	Site	IP Address			
Branch site	10.11.84.1	HQ	172.17.4.41	1HOP	10.11.50.145	**OK**
				2HOP	10.10.254.34	**OK**
				3HOP	10.10.254.36	**OK**
				4HOP	* * *	**OK**
				5HOP	172.17.4.41	**OK**
				6HOP		OK/NG
				7HOP		OK/NG
				8HOP		OK/NG

ตารางที่ 4.6 ผลการทดสอบ Failover โดยดูการวิ่งของ Hop ผ่านสายไฟ

4.2.3.2 ทดสอบการเชื่อมต่อแบบDown wire link

จากนั้นพบว่าการ traffic ของไซต์สาขาไปยังHQสามารถเปิดใช้งานโดยอัตโนมัติผ่านทาง3G Back-up Link แทนได้ตามปกติ



รูปที่ 4.6 ทดสอบการเชื่อมโยงแบบDown wire link

Source		Destination		Hop	Route	Result
Site	IP Address	Site	IP Address			
Branch site	10.11.84.1	HQ	172.17.4.41	1HOP	10.10.250.1	**OK**
				2HOP	10.10.240.2	**OK**
				3HOP	10.10.254.226	**OK**
				4HOP	10.10.254.28	**OK**
				5HOP	* * *	**OK**
				6HOP	172.17.4.41	**OK**
				7HOP		OK/NG
				8HOP		OK/NG

ตารางที่ 4.7 ผลการทดสอบ Failover โดยดูการวิ่งของ Hop ผ่าน 3G Back-up Link

4.3 วิเคราะห์และวิจารณ์ข้อมูลโดยเปรียบเทียบผลที่ได้รับกับวัตถุประสงค์และจุดมุ่งหมายในการปฏิบัติงานหรือการจัดทำโครงการ

หลังจากได้ทำบริการนี้ขึ้นก็ได้มีการจัดทำแบบสำรวจความพึงพอใจแก่ผู้ใช้บริการและผู้เกี่ยวข้องเพื่อทำแบบสรุปว่าการให้บริการในครั้งนี้สามารถตอบโจทย์กับสิ่งที่ลูกค้าต้องหรือไม่

โดยทำการสำรวจพนักงานบริษัทลูกค้าและพนักงานบริษัท NTT ผู้ที่มีส่วนเกี่ยวข้องกับโครงงานในครั้งนี้ จำนวน 55 คน โดยแบ่งออกเป็น พนักงานบริษัทลูกค้า 30 คน และ พนักงานบริษัท NTT 25 คน รวมทั้งสิ้น 55 คน โดยมีหัวข้อการประเมินดังนี้

1. เมื่อเส้นทางอินเทอร์เน็ตหลักถูกตัดขาด อุปการณ์สามารถสลับมาให้บริการเส้นทางสำรองอัตโนมัติ
2. เมื่อเส้นทางหลักกลับมาใช้งานได้อุปกรณ์สลับกลับไปใช้เส้นทางหลัก
3. การเชื่อมต่ออินเทอร์เน็ตเป็นไปได้อย่างลื่นไหล
4. ความเร็วอินเทอร์เน็ตจาก 3G Router ไม่ช้าเกินไป สามารถทำงานได้อย่างไม่ขัดข้อง
5. มีการติดตามผลงานเป็นระบะ และแก้ไขปัญหาอย่างรวดเร็ว

โดยแบ่งการประเมินออกเป็น 3 ระดับ

1. พอใจมาก
2. พอใจ
3. ไม่พอใจ

สรุปผลการสำรวจที่ได้ หลังจากคิดเป็นเปอร์เซ็น คือ

1. เมื่อเส้นทางหลักถูกตัดขาด อุปการณ์สามารถสลับมาให้บริการเส้นทางสำรองอัตโนมัติ พอใจมาก 81.81 % , พอใจ 18.19 %, ไม่พอใจ 0 %

2. เมื่อเส้นทางหลักกลับมาใช้งานได้อุปกรณ์สลับกลับไปใช้เส้นทางหลัก
   พอใจมาก 81.81 % , พอใจ 18.19 %, ไม่พอใจ 0 %
3. การเชื่อมต่ออินเทอร์เน็ตเป็นไปได้อย่างลื่นไหล
   พอใจมาก 58.18 % , พอใจ 27.27 %, ไม่พอใจ 14.54 %,
4. ความเร็วอินเทอร์เน็ตจาก 3G Router ไม่ช้าเกินไป สามารถทำงานได้อย่างไม่ขัดข้อง
   พอใจมาก 50.90 % , พอใจ 21.18 %, ไม่พอใจ 9.09 %,
5. มีการติดตามผลงานเป็นระบะ และแก้ไขปัญหาอย่างรวดเร็ว
   พอใจมาก 90.90 % , พอใจ 7.27 %, ไม่พอใจ 1.81 %,

จากหัวข้อการประเมินข้อที่ 3

มีความไม่พอใจ 14.54 % หรือ 8 คน ได้ให้ความคิดเห็นสาเหตุที่ไม่พอใจว่า ในขณะใช้อินเทอร์เน็ต จะมีอาการที่โหลดหน้าเว็บไม่ขึ้น ต้องกด refresh จึงจะสามารถเข้าเว็บไซต์ได้ ซึ่งสาเหตุอาจเกิดจากสภาพอาการและการให้บริการอินเทอร์เน็ตของการผู้ให้บริการเครือข่าย

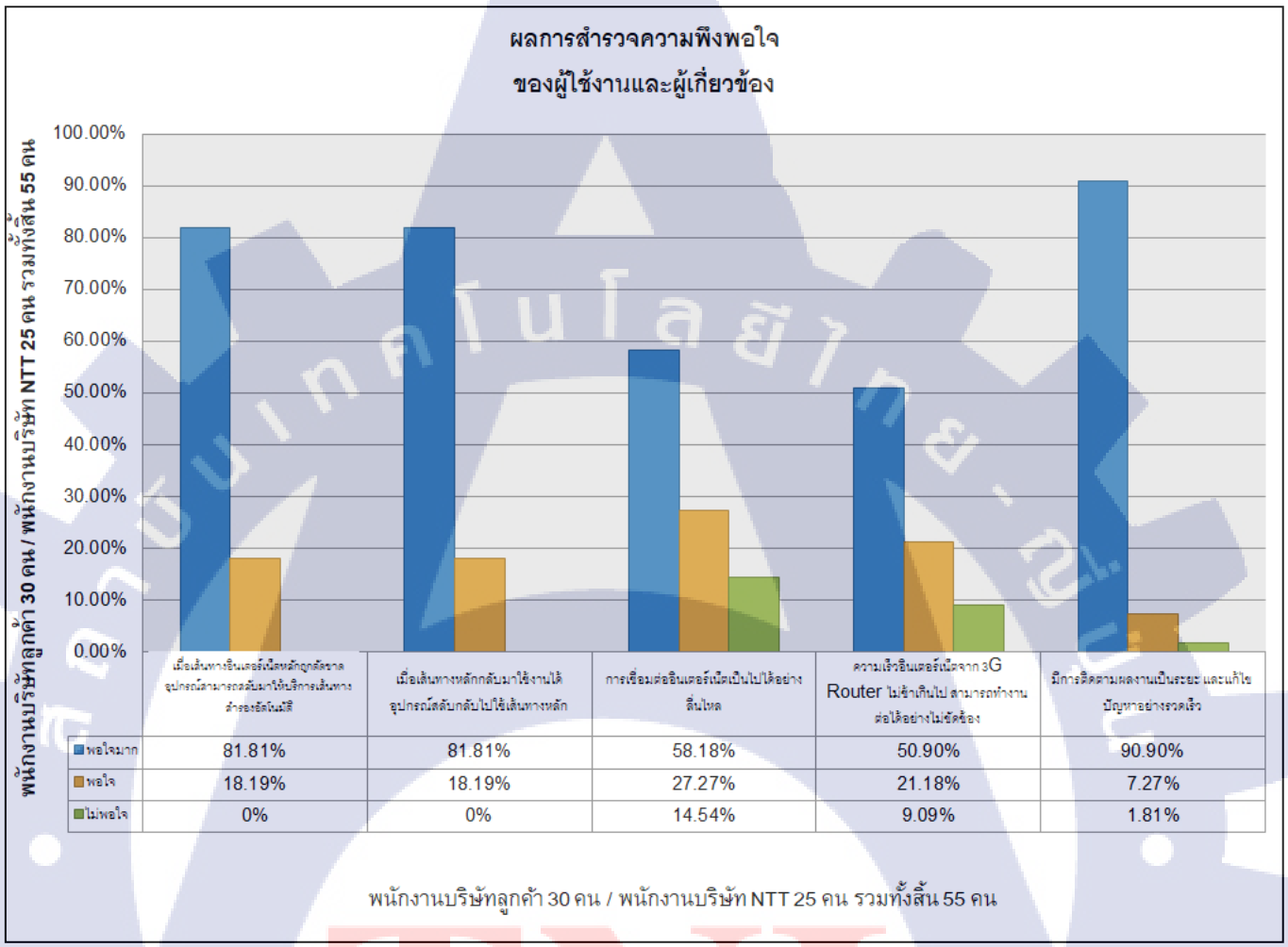
จากหัวข้อประเมินข้อที่ 4

มีความไม่พอใจ 9.09 % หรือ 5 คน ได้ให้ความคิดเห็นสาเหตุที่ไม่พอใจว่า ขณะที่ใช้อินเทอร์เน็ต อินเทอร์เน็ตค่อนข้างช้า ซึ่งสาเหตุอาจเป็นเพราะจุดที่คอมพิวเตอร์ของผู้ใช้บริการอยู่ในบริเวณอับสัญญาณ หรืออาจจะมีเสาบังทำให้อินเทอร์เน็ตเกิดการสะท้อนทำให้ส่งสัญญาณไปถึงได้ช้า

จากหัวข้อประเมินข้อที่ 5

มีความไม่พอใจ 1.81 % หรือ 1 คน ได้ให้ความคิดเห็นสาเหตุที่ไม่พอใจว่า ไม่สามารถติดต่อทาง NTT ได้ในตอนที่ต้องการการแก้ไขปัญหา ซึ่งสาเหตุอาจเกิดจากการที่ขณะนั้นทาง NTT กำลังให้บริการลูกค้าท่านอื่นอยู่ทำให้ไม่สามารถให้บริการลูกค้าท่านนั้นในเวลานั้นได้

ซึ่งหลังจากได้รวบรวมแบบสำรรวจมากซึ่งนำมาทำข้อมูลเพื่อเป็นข้อมูลที่จะใช้ในการปรับปรุงการให้บริการให้ดีมากยิ่งขึ้น ซึ่งแบบสำรวจได้ทำการจัดทำขึ้นดังรูปภาพที่ 4.7



รูปที่ 4.7 ผลการสำรวจความพึงพอใจของผู้ใช้งานและผู้เกี่ยวข้อง

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการดำเนินงาน

จากการที่ได้ปฏิบัติงานสหกิจศึกษาที่บริษัท บริษัท เอ็นทีที คอมมิวนิเคชั่นส์ (ประเทศไทย) จำกัด ผู้ปฏิบัติงานได้รับมอบหมายให้จัดโครงงานการทดสอบระบบการเชื่อมโยงเส้นทางอินเทอร์เน็ตสำรอง 3G/4G โดยเป็นโครงงานที่นำให้ลูกค้าใช้จริง โดยเป็นส่วนหนึ่งของการให้บริการของบริษัท เอ็นทีที คอมมิวนิเคชั่นส์ (ประเทศไทย) จำกัด ซึ่งผลการดำเนินงานนั้นประสบความสำเร็จไปได้ด้วยดี อีกทั้งยังได้รับรู้และประสบการณ์ใหม่ๆ ในเรื่องของ Network อาทิ เช่น การติดตั้งอุปกรณ์ที่ไซต์งานของลูกค้า การconfig เราเตอร์ก่อนนำไปติดตั้งที่ไซต์งานของลูกค้า การทดสอบระบบว่าหากเมื่อใช้งานจริงแล้วจะสามารถทำงานได้จริงเหมือนอย่างที่เขียนไดอาแกรมไว้หรือไม่ นอกจากประสบการณ์ในการทำงานแล้วยังได้รับประสบการณ์ในการทำงานร่วมกับผู้อื่น และการแก้ไขปัญหาเฉพาะหน้าได้

ตลอดการฝึกสหกิจศึกษานั้นทำให้รู้สึกถึงชีวิตการทำงานจริง และสิ่งที่ต้องมีในการทำงาน เช่น การตรงต่อเวลา ความรับผิดชอบต่องานของตนเอง และ อื่นๆ ทำให้มีประสบการณ์ที่มากขึ้นกว่าตอนเรียนรู้เพียงภายในห้องเรียน ทำให้เราได้พบเจอกับปัญหาจริงที่เกิดขึ้นและการหาแนวทางการแก้ไขปัญหา แก้ไขให้ทันเวลาและถูกต้องตรงตามปัญหาที่เกิดขึ้น

5.2 แนวทางการแก้ไขปัญหา

5.2.1 ปัญหาที่พบระหว่างปฏิบัติงาน

1) 3G Router ไม่มีสามารถเร่งความเร่งอินเทอร์เน็ตให้เร็วเหมือนกับสายไฟเบอร์ออพติค ทำให้การทำงานต้องใช้เวลามากขึ้นเล็กน้อย

5.3 แนวทางการแก้ไขปัญหา

1) ลองเปลี่ยนยี่ห้อของ Router

2) หาอุปกรณ์ที่ช่วยในการเร่งความเร็วอินเทอร์เน็ตเข้ามาช่วย

5.3 ข้อเสนอแนะจากการดำเนินงาน

5.3.1 ควรลองใช้ Router ยี่ห้ออื่นนอกจาก Cisco

5.3.2 การสั่งซื้ออุปกรณ์ ควรสั่งล่วงหน้า 2 เดือน หรือ ทำสัญญาเรื่องระยะเวลาการขนส่งเพื่อไม่ให้ล่าช้าเกินกำหนด

เอกสารอ้างอิง

1. VanDyke Software Inc.. (2014). SecureCRT [Online],Available : https://software.thaiware.com/6947-SecureCRT.html [2017, June 1].
2. rightsoftcorp. (2011). SmartCard [Online],Available : http://www.rightsoftcorp.com/?name=news&file=readnews&id=19[2017, June 5].
3. VanDyke Software Inc.. (2014). SecureCRT [Online],Available : http://netprime-system.com/introduce-to-dmvpn-part2-nhrp/ [2017, June 5].
4. netprime. (2017). NHRP [Online],Available : http://running-config.blogspot.com/2011/04/site-to-site-ipsec-vpn-pre-shared-key.html[2017, June 13].
5. kunggiggs. (2014). IPSec [Online],Available : https://www.gotoknow.org/posts/239902 [2017, June 13].
6. netprime. (2017). MGRE[Online],Available : http://netprime-system.com/introduce-to-dmvpn-part1-mgre/ [2017, June 14]
7. ฐาปกรณ์ หาญรักษ์.(2013).การหาค่า MTU ที่เหมาะสมและการตั้งค่า MTU บน Router [Online],Available : http://kb.linksys2u.com/?p=329 [2017, June 14]
8. wikipedia. (2016). FailOver [Online],Available : https://en.wikipedia.org/wiki/Failover [2017, June 22].
9. โต๊ะประจำ. (2009). IPSec [Online],Available : http://www.bloggang.com/viewblog.php?id=itm0064&date=17-03-2009&group=3&gblog=4 [2017, June 22].

ภาคผนวก

ภาคผนวก ก.

รายงานประจำสัปดาห์

ประวัติผู้วิจัย

ชื่อ – สกุล	ฐิตาพร จุลเกษม
วัน เดือน ปีเกิด	14 กุมภาพันธ์ 2539
ประวัติการศึกษา	
ระดับประถมศึกษา	ประถมศึกษาตอนปลาย พ.ศ. 2551
	โรงเรียนเศรษฐบุตรอุปถัมภ์
ระดับมัธยมศึกษา	มัธยมศึกษาตอนปลาย พ.ศ. 2554
	โรงเรียนสตรีวิทยา๒
ระดับอุดมศึกษา	คณะเทคโนโลยีสารสนเทศ สาขาเทคโนโลยีสารสนเทศ พ.ศ.2557
	สถาบันเทคโนโลยีไทย-ญี่ปุ่น
ทุนการศึกษา	-ไม่มี-
ประวัติการฝึกอบรม	พ.ศ. 2558
	Professional Network Installation and Management Workshop
	MISS DAY by IT Connect
	Cybersecurity Summit
	Submarine Seminar
	พ.ศ. 2559
	ABK-TNI Japanese Language Special Course
ผลงานที่ได้รับการตีพิมพ์	-ไม่มี-