อบรมเชิงปฏิบัติการ
หลักสูตรการบริหารจัดการ ระบบเครือข่ายคอมพิวเตอร์ ภายในสำนักงานตรวจบัญชีสหกรณ์

โครงการเช่าวงจรสืบค้นข้อมูล และวงจรสำหรับระบบ VPN
พร้อมระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์
ประจำปีงบประมาณ พ.ศ. 2563

กรมตรวจบัญชีสหกรณ์
Cooperative Auditing Department

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กลุ่มระบบเครือข่ายคอมพิวเตอร์
โทร. 02 281 2714
e-mail: netgrp@cad.go.th

dragons move
บริษัท ดราก้อนส์ มู้ฟ จำกัด (สำนักงานใหญ่)
94/389 ถนนคู้บอน แขวงบางชัน เขตคลองสามวา กรุงเทพมหานคร 10510
เลขประจำตัวผู้เสียภาษี 0105554021505

กำหนดการอบรมเชิงปฏิบัติการ
หลักสูตร การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ภายในสำนักงานตรวจบัญชีสหกรณ์
รุ่นที่ 1 (ครั้งที่ 1) ระหว่างวันที่ 12 - 13 กุมภาพันธ์ 2563
(ครั้งที่ 2) ระหว่างวันที่ 19 - 20 พฤษภาคม 2563
รุ่นที่ 2 (ครั้งที่ 1) ระหว่างวันที่ 5 - 6 มีนาคม 2563
(ครั้งที่ 2) ระหว่างวันที่ 16 - 17 มิถุนายน 2563
รุ่นที่ 3 (ครั้งที่ 1) ระหว่างวันที่ 19 - 20 มีนาคม 2563
(ครั้งที่ 2) ระหว่างวันที่ 26-27 พฤษภาคม 2563
รุ่นที่ 4 (ครั้งที่ 1) ระหว่างวันที่ 7 - 8 เมษายน 2563
(ครั้งที่ 2) ระหว่างวันที่ 24 - 25 มิถุนายน 2563

เวลา	หัวข้ออบรม
	วันที่ 1
11.00 น.	ลงทะเบียน
11.00-12.00 น.	**พิธีเปิดการอบรม**
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	• การใช้เทคโนโลยีดิจิทัลเพื่อการประยุกต์และพัฒนาองค์กรสู่การเป็นรัฐบาลดิจิทัล
14.30-14.45 น.	พักรับประทานอาหารว่าง
14.45-15.00 น.	• การใช้เทคโนโลยีดิจิทัลเพื่อการประยุกต์และพัฒนาองค์กรสู่การเป็นรัฐบาลดิจิทัล
15.00-16.00 น.	• ความรู้พื้นฐานด้านระบบเครือข่ายคอมพิวเตอร์และระบบเครือข่าย VPN
16.00-17.00 น.	• ระบบเครือข่ายคอมพิวเตอร์ของสำนักงานตรวจบัญชีสหกรณ์ในภาพรวม
	วันที่ 2
09.00-10.30 น.	• ความรู้พื้นฐานที่จำเป็นในการดูแลระบบเครือข่าย และการติดตั้งอุปกรณ์เครือข่าย
10.30-10.45 น.	พักรับประทานอาหารว่าง
10.45-11.00 น.	• การตรวจเช็คและการแก้ไขปัญหาเครือข่ายเบื้องต้น
11.00-12.00 น.	• ความรู้พื้นฐานเกี่ยวกับเทคโนโลยี Cloud Computing และ รูปแบบภัยคุกคามต่าง ๆ
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-15.00 น.	• แลกเปลี่ยนความคิดเห็น/ประเมินผลการอบรม

หมายเหตุ 1. พักรับประทานอาหารว่างและเครื่องดื่มภาคเช้า 10.30 – 10.45 น.
ภาคบ่าย 14.30 – 14.45 น.
2. ตารางการอบรมอาจปรับเปลี่ยนได้ตามความเหมาะสม

อบรมเชิงปฏิบัติการ

หลักสูตรการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ภายในสำนักงานตรวจบัญชีสหกรณ์

วันที่ 12 – 13 กุมภาพันธ์ 2563

ณ ห้องอบรมเชิงปฏิบัติการ กรมตรวจบัญชีสหกรณ์

1

หัวข้ออบรม

2

1. การใช้เทคโนโลยีดิจิทัล เพื่อการประยุกต์และพัฒนาองค์กรสู่การเป็นรัฐบาลดิจิทัล
2. ความรู้พื้นฐานด้านระบบเครือข่ายคอมพิวเตอร์และระบบเครือข่าย VPN
3. ระบบเครือข่ายคอมพิวเตอร์ของสำนักงานตรวจบัญชีสหกรณ์ในภาพรวม
4. การดูระบบเครือข่าย และการติดตั้งอุปกรณ์เครือข่าย
5. การตรวจเช็คและการแก้ไขปัญหาระบบเครือข่ายเบื้องต้น
6. ความรู้พื้นฐานเกี่ยวกับเทคโนโลยี Cloud Computing และรูปแบบภัยคุกคามต่าง ๆ

01

การใช้เทคโนโลยีดิจิทัล เพื่อการประยุกต์และพัฒนาองค์กรสู่การเป็นรัฐบาลดิจิทัล

เพื่อให้ผู้เข้าอบรมมีความรู้ ความเข้าใจเกี่ยวกับการใช้เทคโนโลยีดิจิทัล

4

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

5

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในราชกิจจานุเบกษา วันที่ 27 พฤษภาคม 2562 ซึ่งมีผลบังคับใช้ในวันที่ 28 พฤษภาคม 2563

ทำไมถึงต้องมี พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

1. ประเทศไทยต้องมี พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากสหภาพยุโรป (European Union: EU) ได้ออก GDPR (General Data Protection Regulation) เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคล บังคับใช้เมื่อ 25 พฤษภาคม พ.ศ. 2561 ซึ่งนอกจากมีผลบังคับใช้แก่การส่งข้อมูลภายในประเทศสมาชิกสหภาพยุโรป

2. ผู้ประกอบการ ในไทยที่ต้องติดต่อ รับส่งข้อมูลส่วนบุคคลของประชาชนในประเทศที่เป็นสมาชิกสหภาพยุโรป (Cross-Border Data Transfer Issues) ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

6

3. เนื่องจากปัจจุบันมีการละเมิดข้อมูลส่วนบุคคลมากขึ้น จนสร้างความเดือดร้อนรำคาญหรือเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การละเมิดข้อมูลส่วนบุคคลทำได้ง่าย สะดวก และรวดเร็ว

ที่สำคัญ มาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศ มีผลกระทบต่อการค้าระหว่างประเทศ และการทำธุรกิจระหว่างประเทศ หากประเทศไทยไม่มีกฎหมายเกี่ยวกับ
การคุ้มครองข้อมูลส่วนบุคคล ย่อมทำให้เสียโอกาสและความเชื่อมั่น จากกลุ่มประเทศในสหภาพยุโรป และอาจรวมไปถึงประชาคมโลกที่กำลังตื่นตัว เรื่อง Data Protection เพราะเหตุการณ์ใหญ่ ๆ ที่เกิดขึ้นแล้ว เช่น การรั่วไหลของข้อมูลส่วนบุคคลของผู้ใช้เฟ

จึงต้องกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เพื่อกำหนดหลักเกณฑ์และมาตรการกำกับดูแลในการเก็บรวบรวม การใช้และเปิดเผยข้อมูลส่วนบุคคลให้เป็นมาตรฐานสากล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

7

กฎหมายฉบับนี้เกี่ยวข้องกับเราทุกคนในฐานะที่เป็นเจ้าของข้อมูล รวมถึงผู้ประกอบการ หน่วยงานต่าง ๆ ที่มีหน้าที่โดยตรงกับการเก็บข้อมูลส่วนบุคคล เพื่อนำไปใช้งาน โดยสรุปประเด็นสำคัญ 8 ประเด็น ดังนี้

1. กฎหมายคุ้มครองข้อมูลส่วนบุคคลของบุคคลธรรมดาเท่านั้น
2. เจ้าของข้อมูลส่วนบุคคลต้องยินยอมก่อน
3. แจ้งรายละเอียดชัดเจนครบถ้วน
4. ผู้มีสิทธิ์เด็ดขาดคือเจ้าของข้อมูล
5. ผู้เก็บต้องรักษาข้อมูลให้ปลอดภัยเป็นความลับ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

8

6. ครอบคลุมผู้เก็บ-ใช้-เปิดเผยข้อมูลทั้งในและนอกประเทศ
7. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ใช้ Outsource ได้
8. ฝ่าฝืนมีโทษถูกจับติดคุก ปรับเงินสูงสุด 5 ล้านบาท

หากฝ่าฝืนมีโทษทั้งทางอาญา ทางแพ่ง และทางปกครอง
สำหรับโทษทางอาญา หากมีการฝ่าฝืนมีโทษจำคุกไม่เกิน 6 เดือนถึง 1 ปี หรือปรับไม่เกิน 500,000 ถึง 1,000,000 บาท หรือทั้งจำทั้งปรับ
ส่วนระวางโทษปรับทางทางปกครองไม่เกิน 500,000 ถึง 5,000,000 บาท

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

9

บุคคลทั่วไป ต้องทำอะไรบ้าง?

1. ก่อนจะให้ข้อมูลสำคัญ ควรมีการเก็บบันทึกเป็นหลักฐาน หรือมีการขอสำเนาของเอกสารที่มีข้อมูลส่วนบุคคล
2. เมื่อใดพบว่าข้อมูลส่วนบุคคลได้ถูกนำไปใช้ผิดวัตถุประสงค์ จะได้ใช้เป็นหลักฐานในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ
3. มีสติรอบคอบในการให้ข้อมูลส่วนบุคคลแก่เว็บไซต์/แอปพลิเคชัน ที่มีการขอความยินยอมจากเจ้าของข้อมูล ยกตัวอย่าง เช่น การทำงานของเว็บไซต์/แอปพลิเคชัน เช่นปัจจุบันนี้หลายแอปพลิเคชันจะเชื่อมต่อระบบสมาชิกกับเฟซบุ๊ก มีการขอชื่ออีเมลและรายชื่อเพื่อนในเฟซบุ๊กของเรา หากเราเห็นว่าไม่จำเป็นที่ต้องให้ข้อมูลรายชื่อเพื่อน ก็สามารถคลิกเพื่อไม่ยินยอม และยินยอมให้เฉพาะอีเมลเพื่อการเข้าระบบของแอปพลิเคชันนั้น ๆ ได้
4. เจ้าของข้อมูลต้องทำหน้าที่ “คุ้มครองข้อมูลของตนเอง” ด้วย ไม่ด่วนยินยอมหรือให้ข้อมูลโดยที่ยังไม่ได้ศึกษารายละเอียดของขอบเขตการใช้ข้อมูลส่วนบุคคล

10

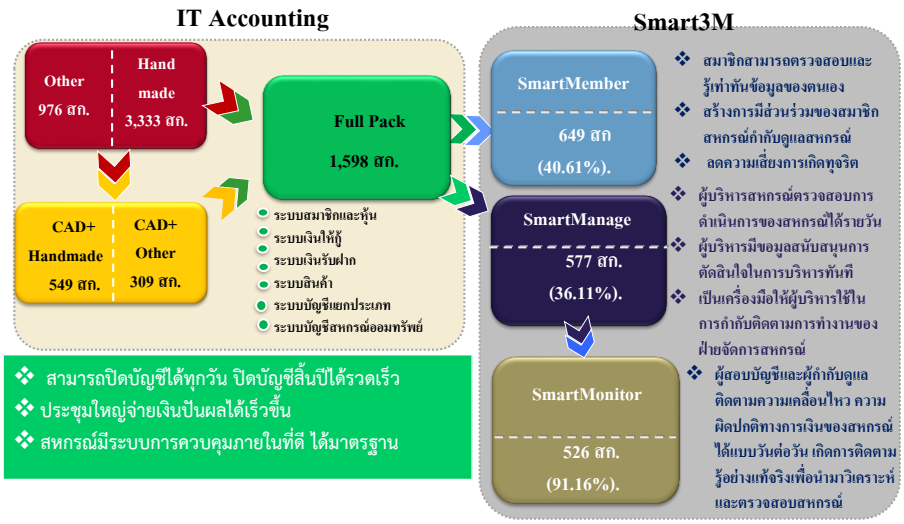
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

ประโยชน์ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

1. คุ้มครองข้อมูลส่วนบุคคลไม่ให้ถูกนำไปใช้ประโยชน์ด้านอื่น
2. ป้องกันและแก้ไขปัญหาการละเมิดสิทธิข้อมูลส่วนบุคคล
3. สร้างกลไกหรือมาตรฐานการกำกับดูแลในการคุ้มครองข้อมูลส่วนบุคคล
4. สามารถฟ้องเรียกค่าสินไหมทดแทนกรณีถูกละเมิดข้อมูลส่วนบุคคล

กลุ่มพัฒนาระบบบัญชีคอมพิวเตอร์

IT Accounting & Smart3M



แผนการนำโปรแกรมออกใช้งาน

13

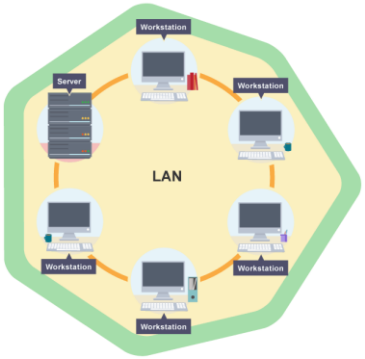
02

ความรู้พื้นฐานด้านระบบเครือข่ายคอมพิวเตอร์และระบบเครือข่าย VPN

เพื่อให้ผู้เข้าอบรมได้รับความรู้ ความเข้าใจเกี่ยวกับระบบเครือข่ายเบื้องต้นและระบบเครือข่าย VPN ที่ใช้งานในปัจจุบัน

โครงสร้างพื้นฐานระบบเครือข่ายคอมพิวเตอร์

15



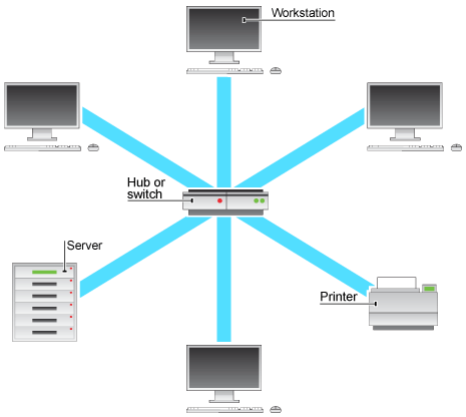
ระบบเครือข่ายแบบมีสาย
LAN (Local Area Network)

ระบบเครือข่ายแบบไร้สาย
(Wireless Lan)

16

ระบบเครือข่ายแบบมีสาย LAN (Local Area Network)

ระบบเครือข่าย แบบเชื่อมต่อคอมพิวเตอร์เข้าด้วยกันในระยะจำกัด เช่น ในอาคารเดียวกัน หรือบริเวณเดียวกันที่สามารถลากสายถึงกันได้โดยตรง ส่วนมากจะใช้สายเคเบิ้ล หรือ ที่เรียกกันว่า สายแลน เป็นตัวกลางในการเชื่อมต่อ



17

ระบบเครือข่ายแบบมีสาย LAN (Local Area Network)

ข้อดี

- สามารถใช้ทรัพยากรที่มีในวง LAN ร่วมกันได้
- ประหยัดค่าใช้จ่าย
- ขนย้ายข้อมูลระหว่างเครื่องต่อเครื่องในระบบได้อย่างรวดเร็ว
- สะดวกกับผู้ใช้งาน สามารถติดต่อสื่อสารข้อมูล ข้อความ และซอฟต์แวร์กับระบบอื่นภายนอกเครือข่ายได้ง่าย
- ง่ายต่อการวบคุม

ข้อจำกัด

- ข้อจำกัดของระยะทาง
- ยากต่อการควบคุมให้มีมาตรฐานการทำงานแบบเดียวกัน
- ยุ่งยากต่อการดูแลรักษา
- ซอฟต์แวร์ที่ใช้กับระบบ LAN ในปัจจุบันยังพัฒนาได้ไม่ดีเทียบเท่ากับซอฟต์แวร์ในระบบของเครื่องมินิคอมพิวเตอร์หรือเมนเฟรมซึ่งมีมาก่อน และราคาของซอฟต์แวร์เฉพาะสำหรับระบบ LAN ยังมีราคาสูงอยู่

18

ระบบเครือข่ายแบบไร้สาย (Wireless LAN)

ระบบเครือข่ายไร้สาย (Wireless Local Area Network) คือ ระบบการสื่อสารข้อมูลที่มีรูปแบบในการสื่อสารแบบไม่ใช้สาย โดยใช้การส่งคลื่นความถี่วิทยุในย่านวิทยุ RF และ คลื่นอินฟราเรด ในการรับและส่งข้อมูลระหว่างคอมพิวเตอร์แต่ละเครื่อง ผ่านอากาศ, ทะลุกำแพง, เพดานหรือสิ่งก่อสร้างอื่น ๆ โดยปราศจากความต้องการของการเดินสาย

19

ระยะทางการเชื่อมต่อของระบบ Wireless LAN

ภายในอาคาร

- ระยะ 50 เมตร ได้ความเร็วประมาณ 11 Mbps.
- ระยะ 80 เมตร ได้ความเร็วประมาณ 5.5 Mbps.
- ระยะ 120 เมตร ได้ความเร็วประมาณ 2 Mbps.
- ระยะ 150 เมตร ได้ความเร็วประมาณ 1 Mbps.

ภายนอกอาคาร

- ระยะ 250 เมตร ได้ความเร็วประมาณ 11 Mbps.
- ระยะ 350 เมตร ได้ความเร็วประมาณ 5.5 Mbps.
- ระยะ 400 เมตร ได้ความเร็วประมาณ 2 Mbps.
- ระยะ 500 เมตร ได้ความเร็วประมาณ 1 Mbps.

20

ระบบเครือข่ายแบบไร้สาย (Wireless LAN)

ข้อดี

- มีความคล่องตัวสูง
- สามารถติดตั้งได้ง่ายและรวดเร็ว
- สามารถขยายระบบเครือข่ายได้ง่าย
- ลดค่าใช้จ่ายโดยรวม ที่ผู้ลงทุนต้องลงทุน
- เครือข่ายไร้สายทำให้องค์กรสามารถปรับขนาดและความเหมาะสมได้ง่าย สามารถขยายเครือข่ายได้ไม่จำกัด

ข้อจำกัด

- มีอัตราการลดทอนสัญญาณสูง
- มีสัญญาณรบกวนสูง
- ต้องแชร์กันใช้ช่องสัญญาณคลื่นความถี่เดียวกัน
- ยังมี หลายมาตรฐาน ตามผู้ผลิต แต่ละราย ทำให้มีปัญหาในการใช้งานร่วมกัน
- ราคาแพงกว่าระบบเครือข่ายแบบมีสาย
- มีความเร็วไม่สูงมากนัก

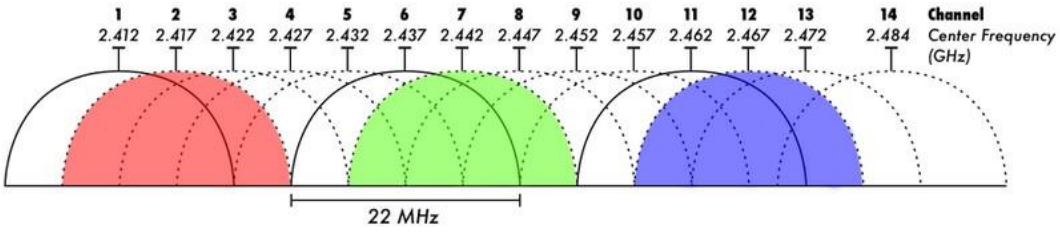
21

มาตรฐานความเร็วของ Wireless LAN IEEE 802.11

IEEE Standard	Frequency	Speed
802.11a	5GHz	54Mbps
802.11b	2.4GHz	11Mbps
802.11g	2.4GHz	54Mbps
802.11n	2.4 and 5GHz	Up to 450 Mbps*
802.11ac	5GHz	Up to 1300 Mbps*

22

มาตรฐานสัญญาณ Wireless 2.4 GHz Channel



มาตรฐานสัญญาณ Wireless 5 GHz Channel

23

IEEE Standard	Channel Width
802.11a	20MHz
802.11n	20MHz
	40MHz
802.11ac	20MHz
	40MHz
	80MHz
	160MHz

ความรู้พื้นฐานด้านอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์

24

รู้จักอุปกรณ์เครือข่าย Switch/Hub, Router/ONU, Wireless Access Point ชนิดต่าง ๆ

Switch/Hub หน้าที่หลักคือ เชื่อมต่อให้เครื่องคอมพิวเตอร์ที่ตั้งอยู่คนละที่ สามารถติดต่อสื่อสารกันได้ ก็คือเป็นอุปกรณ์สำหรับเชื่อมต่ออุปกรณ์ในระบบเครือข่ายเข้าด้วยกัน

- Hub จะทำหน้าที่ทวนซ้ำสัญญาณ เช่น ในระบบเครือข่ายมี PC 10 เครื่อง เมื่อ PC1 ต้องการส่งข้อมูลไปยัง PC5 ในขณะนั้น PC อื่นๆ จะไม่สามารถส่งข้อมูลได้ และ ปัจจุบันแทบจะไม่มีการใช้งานแล้ว
- Switch จะทำงานเหมือนกับ Hub แต่ขณะที่ PC1ส่งข้อมูล ไปยัง PC5 PC อื่นๆ จะยังสามารถส่งข้อมูลได้พร้อมๆ กัน

25

- Layer 3 Switch คืออะไร

  คือ อุปกรณ์ในการทำ Routing (รับส่งข้อมูลระหว่างเน็ตเวิร์ค) เหมาะสมในการนำไปใช้ในระบบเน็ตเวิร์กที่มีการใช้งาน VLAN (VLAN เป็นการแบ่งพอร์ตต่าง ๆ ที่มีอยู่ในสวิทช์ ให้เป็นเสมือนแยกกันอยู่คนละเน็ตเวิร์ค) และต้องการให้อุปกรณ์ Computer ที่อยู่ในแต่ละ VLAN สามารถติดต่อกันได้

- สวิตช์ (Switch) เป็นอุปกรณ์ที่พัฒนาการต่อจากฮับอีกทีหนึ่งมีความสามารถมากกว่า Hub โดยการทำงานของสวิตช์จะส่งข้อมูลออกไปเฉพาะพอร์ตที่ใช้ในการติดต่อกับเครื่องคอมพิวเตอร์ PC ปลายทางเท่านั้น ไม่ส่งกระจายข้อมูลไปยังทุกพอร์ตเหมือนอย่างฮับ ทำให้ในสวิตช์ไม่มีปัญหาการชนของข้อมูล สวิตช์จะทำงานอยู่ในชั้น Data Link Layer คือจะรับผิดชอบในการเชื่อมโยงของข้อมูล ตรวจสอบความถูกต้องของการติดต่อจากโหนดหนึ่งไปอีกโหนดหนึ่งและความสมบูรณ์ของการรับส่งข้อมูล สำหรับในชั้นเชื่อมโยงข้อมูลนั่นจะทำการแบ่งข้อมูลระดับบิตที่ได้รับจากชั้น Physical Layer เป็นข้อมูลชนิดที่เรียกว่า เฟรม ก่อนจะส่งไปยังชั้นถัดไป ก็คือ Network Layer

- Switch กับ Hub แตกต่างกันอย่างไร

  Switch กับ Hub นั้นจะทำหน้าที่คล้าย กันเพียงแต่ Hub นั้นเวลาส่งข้อมูลนั้นจะเป็นแบบ broadcast กระจายไปทุกเครื่องแต่ถ้าเป็น switch นั้น จะดูว่าข้อมูลนี่เป็น ของเครื่องไหนแล้วค่อยส่งไปยังเครื่องนั้น นอกจากนี้ความเร็วในการส่งข้อมูลก็ต่างกันคือ speed Hub คือspeed / N เครื่องเช่น LAN 100 Mbps. 10 เครื่อง ทุกเครื่องได้แค่ 10 Mbps. ส่วน speed Switch นั้น LAN 100 Mbps. ทุกเครื่องได้ 100 Mbps.

การเลือกซื้อ และ ติดตั้ง Switch หรือ Hub

26

- ความเร็ว ถ้าหากการ์ดเครือข่ายในระบบมีความเร็ว 10/100/1000 Mbps. ก็ควรใช้ Switch ที่มีความเร็วเท่ากันคือ 10/100/1000 Mbps.
- จำนวนช่องต่อเข้าคอมพิวเตอร์ (Port) และควรจะเลือกช่องที่ต่อพอร์ตเผื่อไว้ในอนาคตด้วย
- Switch ขอบเขตการรับประกัน ควรจะได้รับประกันตลอดการใช้งาน และจากการมองหาประโยชน์อื่นๆ เช่น จากผู้เชี่ยวชาญเฉพาะทาง, การบริการหลังจากขาย และ ผลิตภัณฑ์ ฯลฯ
- อาจจะต้องการเริ่มจาก Switch ที่ใหญ่ ดังเช่น 8 หรือ 16 - 24 port ขึ้นอยู่กับจำนวนเครื่องคอมพิวเตอร์ และอุปกรณ์อื่นๆ จะเชื่อมต่อกับเครือข่ายของคุณ

ONU

27

ONU คืออะไร?

ONU ย่อมาจาก Optical Network Unit เป็นอุปกรณ์ที่ใช้ปลายทาง หรือพูดง่ายๆ ก็คือ เป็นอุปกรณ์ที่วางไว้ที่บ้านเรา เพื่อรับข้อมูลการใช้งานอินเทอร์เน็ตในระบบ FTTx คล้ายๆ โมเด็มหรือเร้าเตอร์ เพียงแต่ ONU จะรองรับ Speed ที่สูงกว่า และสายที่ใช้เชื่อมต่อสัญญาณ จากเดิมที่เป็นสายโทรศัพท์ ก็จะเป็นสาย Patch Cord แทน

Router

28

Router คืออะไร?

Router คือ อุปกรณ์ที่ทำหน้าที่เชื่อมต่อระบบเครือข่ายอย่างหนึ่ง ซึ่งถ้าแปลความหมายคำว่า Route ก็คือ ถนน นั่นเอง ดังนั้น การเชื่อมต่อคอมพิวเตอร์ด้วย Router ทำให้เราสามารถเชื่อมต่อคอมพิวเตอร์ได้มากกว่าหนึ่งเครื่องในเวลาเดียวกัน ซึ่ง Router นั้นจะมีซอฟต์แวร์ที่ใช้ในการควบคุมการทำงาน และตัว Router จะมีช่องที่ใช้เสียบต่อสายสัญญาณเรียกว่า Port LAN ซึ่งโดยทั่วไปมักมี 5 Ports หรือมากกว่า ใน Router 1 ตัว

การทำงานของ Router

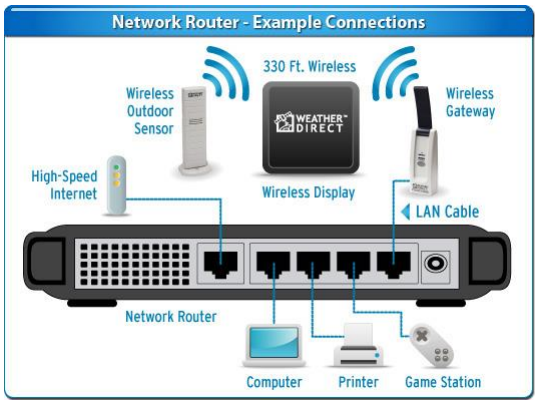
29

ทำหน้าที่เป็น Router

หาเส้นทางส่งผ่านข้อมูลโดยเป็นตัวกลางสำหรับใช้ส่งต่อข้อมูลจากระบบเครือข่ายต้นทางไปยังระบบเครือข่ายปลายทางโดยสามารถที่จะทำการเชื่อมโยงเส้นทางสัญญาณสื่อสารที่แตกต่างกันได้ 2 เมื่อ Router ได้รับข้อมูลจะมีการตรวจดูว่าเป็น Protocol แบบใด หลังจากนั้นก็ทำการตรวจสอบเส้นทางจาก Routing Table ก่อนจะทำการส่งไปยังเครือข่ายปลายทาง

ทำหน้าที่เป็นจุดเชื่อมต่อสัญญาณ

Router นั้นทำหน้าที่เป็นจุดเชื่อมต่อสัญญาณด้วย โดยจะมีช่อง RJ-45 (ETHERNET) นั้นมีไว้สำหรับเชื่อมต่อไปยัง Switch หรือเชื่อมต่อไปยังคอมพิวเตอร์ ถ้าเราเชื่อมต่อไปยัง Switch เราจะต้องใช้สาย LAN ในการเชื่อมต่อ



การทำงานของ Router

30

ทำหน้าที่กำหนด IP Address

เมื่อเราเชื่อมต่อระบบเครือข่ายของเราเข้ากับ ISP แล้ว ISP จะกำหนด IP Address จริงสำหรับการเชื่อมต่อมาให้ และจะทำการกำหนด IP Address ภายใน เพื่อให้เครื่องคอมพิวเตอร์ภายในเครือข่ายของเราสามารถใช้งานระบบอินเตอร์เน็ตได้ทุกเครื่อง

ทำหน้าที่แปลง IP Address

อุปกรณ์ที่ทำหน้าที่แปลง IP Address หรือ NAT ซึ่งมีหลายแบบด้วยกันตัวอย่างเช่น Router, Firewall เป็นต้น สำหรับ Router ในปัจจุบันเกือบทุกรุ่นจะมีฟังก์ชั่น NAT ในตัว ซึ่งจะทำการแปลง IP Address ภายในให้เป็น IP Address จริงเพื่อเชื่อมต่อกับระบบอินเตอร์เน็ต

คุณสมบัติที่น่าสนใจของ Router

31

- ทำหน้าที่คล้าย Switch ทำให้เชื่อมต่อได้หลายเครื่องพร้อมกัน
- บางรุ่นรองรับการทำงาน Wireless
- เป็น ONU ในตัว
- Firewall /IPSec VPN (รองรับการเชื่อมต่อทางไกลแบบมี security)
- Antivirus (รุ่นใหม่ๆ ของ Router จะมีโปรแกรม Antivirus ฝังอยู่ด้วย)

สรุปประเภทของ ONU/Router

- บางรุ่นเป็น Router อย่างเดียว
- บางรุ่นเป็นทั้ง Router และ ONU
- บางรุ่นเป็น Router แต่เป็นประเภท Wireless

อุปกรณ์ Access Point - Wireless

32

Access Point คือโหมดพื้นฐานที่สุดของการใช้งาน Wireless อยู่แล้วนั่นคือ Access Point จะทำหน้าที่ในการเชื่อมต่อเครื่องลูกข่ายเข้าสู่ระบบเครือข่ายแบบมีสาย เพื่อเข้าไปใช้งานอินเตอร์เน็ต หรือเข้าไปยังเครือข่าย LAN ของสำนักงานเป็นต้น โดยการเข้าถึงเครือข่ายอาจจะมีการเข้ารหัส (Encryption) โดยผู้ใช้งานจะต้องใส่ Key ก่อนเชื่อมต่อ บนมาตรฐาน WEP หรือ WPA WPA2

ประเภทของอุปกรณ์ Access Point

33

การเลือกใช้ระหว่าง Wireless Outdoor และ Wireless แบบ Indoor แยกการทำงานกันให้ถูก หากใช้ภายในอาคาร ต้องการอุปกรณ์ที่รองรับเครื่องลูกข่ายเยอะ ควรเลือกใช้ Access Point แบบ Indoor แต่หากใช้งานตามไซต์งาน ก่อสร้าง ปั๊มน้ำมัน หรือพื้นที่โล่งกว้าง เครื่องลูกข่ายไม่มาก แนะนำให้ใช้ Wireless แบบ Outdoor ปัจจุบันมีโรงงานผลิตอุปกรณ์ประเภทนี้บางแห่งเอา สถาปัตยกรรม Wireless แบบ Outdoor มาทำในรูปแบบของ Wireless Indoor ลูกค้าก็จะนึกว่า สัญญาณแรง แล้วจะดี แต่ไม่รู้ถึงข้อเสียและข้อจำกัด ควรเลือกให้ถูก เพราะจะมีปัญหาเรื่องการรับสัญญาณ

Access Point แบบ Outdoor

- ด้วยลักษณะคลื่นที่มีความสูงต่ำมาก ทำให้ส่งสัญญาณได้ไกล (ความถี่ Frequency สูง)
- ลักษณะคลื่นความถี่จะมีความสูงต่ำมาก จึงทำให้รับส่งข้อมูลปริมาณมากแบบต่อเนื่องทำได้ไม่ดีสัญญาณจะขึ้นๆ ลงๆ
- มักเกิดปัญหากับการใช้งาน DHCP เครื่องลูกข่ายเครื่องที่ 6-10 มักจะเริ่มรับ IP ไม่ได้
- ติดตั้งนอกอาคารได้ และทนแดดทนฝนได้ดี

ประเภทของอุปกรณ์ Access Point

34

Access Point แบบ indoor

- ลักษณะคลื่นความถี่มีความสูงต่ำน้อย (ความถี่ปกติตามมาตรฐาน)
- ทำให้รับส่งข้อมูลได้มีเสถียรภาพมากกว่า
- แต่อาจส่งสัญญาณได้ไกลสู้ Wireless แบบ Outdoor ไม่ได้ แต่อย่างไรก็ตามสัญญาณก็ยังแรงกว่า Access Point ที่เป็น Wireless N 300 Mbps. อยู่ดี

การเลือกใช้ Wireless Access Point

35

- ความเร็วในการรับส่งข้อมูล
- รัศมีของผลิตภัณฑ์เครือข่ายไร้สายที่ครอบคลุมถึง
- ความเข้ากันได้กับผลิตภัณฑ์ของผู้ผลิตรายอื่น
- Access Point หรือผลิตภัณฑ์ไร้สายอื่นมีความสามารถในการปรับเปลี่ยนช่องสัญญาณและกำลังส่งได้
- ผลิตภัณฑ์มีความน่าเชื่อถือเป็นที่ยอมรับ
- การติดตั้งที่ง่ายและสะดวกในการใช้งาน
- ฟังก์ชั่นในการเข้ารหัสสัญญาณที่ใช้เพื่อความปลอดภัย
- มีการพัฒนาและมีซอฟต์แวร์ให้ดาวน์โหลดเว็บไซต์ของผู้ผลิต
- ผลิตภัณฑ์มีไฟแสดงสถานะการทำงาน
- ผลิตภัณฑ์ที่มีเครื่องหมายแสดงการผ่านการตรวจสอบมาตรฐานจาก Wi-Fi Alliance

การเลือกใช้ Wireless Access Point ตามมาตรฐาน

36

การเลือกใช้ Access Point ตามมาตรฐาน b/g/n

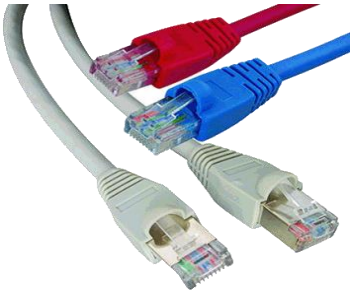
- มีคอมพิวเตอร์ หรือเครื่องเกมคอนโซลไม่กี่เครื่อง
- ดาวน์โหลดไฟล์ขนาดใหญ่บ่อย ๆ
- บ้านหรือพื้นที่ใช้งานไม่กว้างมาก
- มีงบประมาณสำหรับ Wifi Router ไม่สูงมาก เพราะมาตรฐาน AC จะมีราคาค่อนข้างสูง

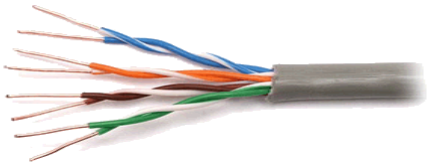
การเลือกใช้ Access Point ตามมาตรฐาน AC

- บ้านหรือพื้นที่ใช้งานมีบริเวณกว้างจนมาตรฐาน N ไม่ครอบคลุมพื้นที่ทั้งหมด
- มี User ที่ใช้งานทั้งคอมพิวเตอร์และเครื่องเกมคอนโซลเชื่อมต่ออยู่หลายเครื่องด้วยกันจนคลื่น 2.4 GHz อาจจะไม่เพียงพอ ต้องมีมาตรฐาน 5 GHz เข้ามาเสริม
- ใช้งานอินเตอร์เน็ตมากกว่าแค่ดาวน์โหลดไฟล์ขนาดใหญ่ ซึ่งอาจรวมไปถึงการเล่นเกมจากเครื่องคอนโซล หรือมี User ถ่ายทอด Live Stream Video ไปพร้อม ๆ กัน ทำให้ต้องการประสิทธิภาพในการทำงานสูงสุดตลอดเวลา

ประเภทของสายสัญญาณ UTP และ Fiber Optic

37



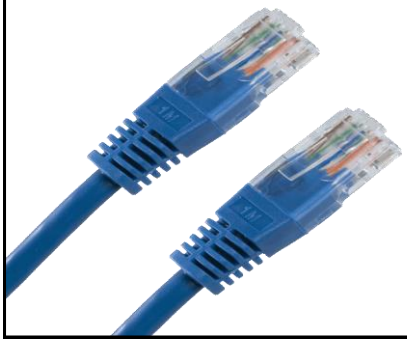


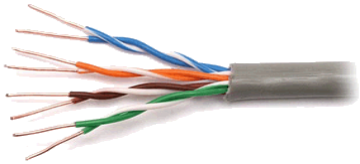
ประเภทของสายสัญญาณ UTP

38

CAT 5E

สายยูทีพี (UTP) ประเภท Catagory5 (CAT-5) ผลิตจากสายทองแดงที่มีการบิดตีเกลียวมากขึ้น มีการป้องกันสัญญาณรบกวนได้ดี และสามารถรองรับการส่งข้อมูลที่ความเร็ว 10/100/1000 Mbps. ที่ความยาว 100 เมตร รองรับการทำงานของอุปกรณ์เครือข่ายในปัจจุบัน เช่น Ethernet, Fast Ethernet, Gigabit Ethernet โดยมี Bandwidth 10/100/1000 Mbps.



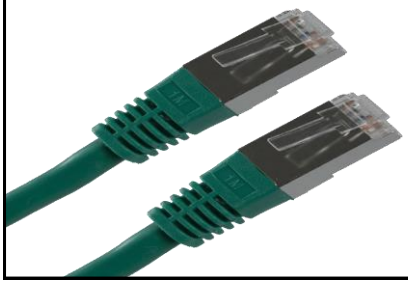


ประเภทของสายสัญญาณ UTP

39

CAT 6

สายประเภทนี้มีสี่คู่สายทองแดงที่มีการบิดรอบเช่นเดียวกับ CAT 5E - CAT 6 ให้ความเร็วสูงสุด 10 Gbps. (ระยะ 55 เมตร) ต่างจาก CAT 5E ที่รองรับความเร็วสูงสุด 1 Gbps.



ประเภทของสายสัญญาณ UTP

40

CAT 6A

สายประเภทนี้สามารถวิ่งด้วยความเร็วในการส่งข้อมูลที่ 10 Gbps. ได้ และ มีขนาดของแกนทองแดงที่ 23 AWG ที่เป็นขนาดมาตรฐานในการส่งสัญญาณ พร้อมด้วยความถี่ในการส่งสัญญาณที่ 500 เม็กกาเฮิตส์ และ ยังมีเปลือกด้านนอกที่ผลิตจากวัสดุ LSZH(Low smoke Zero Haragen) ซึ่งจะไม่ลามไฟ ขณะเกิดเพลิงไหม้ และ ไม่มีควันพิษ

เลือกสาย LAN แบบไหนให้สำนักงานดี ?

41

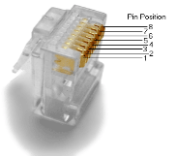
Switch/Hub ที่ใช้ในสำนักงานรองรับความเร็วอยู่ที่เท่าไร?

10/100 Mbps. ⟷ CAT 5E
รองรับ 1000 Mbps.

10 Gbps. ⟷ CAT 6A
รองรับ 10 Gbps. (100 M.)

1000 Mbps. / 1 Gbps
↕
CAT 6
รองรับ 10 Gbps. (55 M.)

การเข้าหัว RJ-45 สาย LAN Cat 5E ตามมาตรฐาน



42

อุปกรณ์ต่างกัน ต่อกันใช้สาย LAN แบบตรง
(Straight-Through Cable)

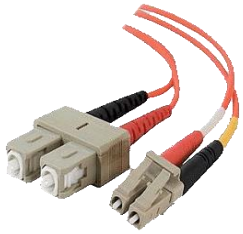
หัวสายด้านที่ 1	ลำดับสายที่	หัวสายด้านที่ 2
ขาว ส้ม	1	ขาว ส้ม
ส้ม	2	ส้ม
ขาว เขียว	3	ขาว เขียว
ฟ้า	4	ฟ้า
ขาว ฟ้า	5	ขาว ฟ้า
เขียว	6	เขียว
ขาว น้ำตาล	7	ขาว น้ำตาล
น้ำตาล	8	น้ำตาล

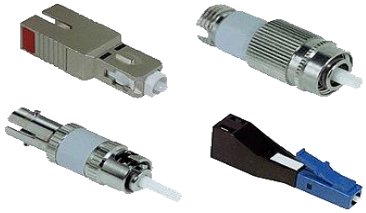
อุปกรณ์เหมือนกัน ต่อกันใช้สาย LAN แบบครอส
(Crossover Cable)

หัวสายด้านที่ 1	ลำดับสายที่	หัวสายด้านที่ 2
ขาว ส้ม	1	ขาว เขียว
ส้ม	2	เขียว
ขาว เขียว	3	ขาว ส้ม
ฟ้า	4	ฟ้า
ขาว ฟ้า	5	ขาว ฟ้า
เขียว	6	ส้ม
ขาว น้ำตาล	7	ขาว น้ำตาล
น้ำตาล	8	น้ำตาล

ประเภทสายเส้นใยแก้วนำแสง (Fiber Optic)

43

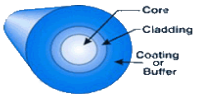


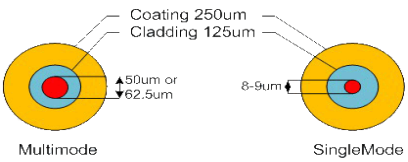


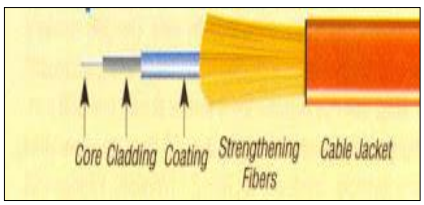
โครงสร้างของเส้นใยแก้วนำแสง (Fiber Optic)

44

- **เส้นแก้ว (Core)** เป็นตัวที่นำสัญญาณแสง จะมีเส้นผ่าศูนย์กลาง 62.5/125 um, 50/125 um, 9/125 u
- **ฉนวนเคลือบ (Cladding)** เป็นสารที่ใช้ในการเคลือบแก้ว (Core) เพื่อให้นำสัญญาณได้ กล่าว คือ แสงที่ถูกส่งไปในแกนแก้วจะถูกขังหรือ เคลื่อนที่ไปตามสายไฟเบอร์ด้วยขบวนการสะท้อนกลับของแสง นิยมเคลือบจนมีเส้นผ่าศูนย์กลาง 125 um
- **ฉนวนป้องกัน (Coating)** เป็นเสมือนผนังของเส้นแก้วเป็นชั้นที่ต่อจาก Cladding เพื่อให้ปลอดภัยขึ้น และใช้ป้องกันแสงจากภายนอกไม่ให้เข้ามาภายในเส้นไฟเบอร์ มีเส้นผ่าศูนย์กลาง 250 um
- **ปลอกสาย (Buffer)** เป็นเสมือนปลอกของสายหรือเสื้อชั้นในที่หุ้มป้องกันสาย และยังช่วยให้การโค้งงอของสายไฟเบอร์มีความยืดหยุ่นมากขึ้นมีเส้นผ่าศูนย์กลางประมาณ 900 um(Buffer Tube)
- **ปลอกหุ้ม (Jacket)** เป็นเสมือนเสื้อชั้นนอกสุดของสายไฟเบอร์ที่ให้เกิดความเรียบร้อย และทำหน้าที่ป้องกันสายไฟเบอร์เป็นชั้นนอกสุดชนิดของ Jacket จะมีหลายชนิด ขึ้นอยู่กับการใช้งานว่าเป็นสายที่เดินภายในอาคาร (Indoor) หรือเดินภายนอกอาคาร (Outdoor)





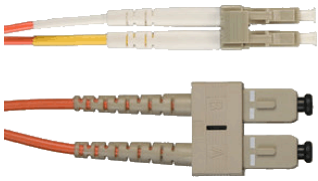


Fiber Optic แบ่งตามการเดินทางของแสงได้ 2 ชนิด คือ

45

Single Mode Fiber

มีแนวของลำแสงอยู่ในแนวเดียว เรียกว่า Single Mode Fiber Optic (SMF) ขนาดเส้นผ่านศูนย์กลางของแกน ขนาด 9 ไมครอน สามารถใช้งานได้ดีที่ระยะทาง 5 - 70 KM



Multi Mode Fiber

มีแนวของลำแสงอยู่เป็นจำนวนมาก เราเรียกว่า Multi-Mode Fiber Optic (MMF) ขนาดเส้นผ่านศูนย์กลางของแกน ขนาด 50 ไมครอน และ 62.5 ไมครอน สามารถใช้งานได้ดีที่ระยะทาง 550 Meter เหมาะกับงานภายในอาคาร เพราะมีระยะใกล้

ระบบเครือข่ายส่วนตัวเสมือน Virtual Private Network (VPN)

46

เครือข่ายเสมือนส่วนตัว ที่ทำงานโดยใช้ โครงสร้างของเครือข่ายสาธารณะ หรืออาจจะวิ่งบนเครือข่ายไอพีก็ได้ แต่ยังสามารถคงความเป็นเครือข่ายเฉพาะขององค์กรได้ด้วยการเข้ารหัส package ก่อนส่ง เพื่อให้ข้อมูลมีความปลอดภัยมากขึ้น VPN เป็นเทคโนโลยีการเชื่อมต่อเครือข่ายนอกอาคาร (WAN-Wide Area Network)ที่กำลังเป็นที่สนใจและเริ่มนำไปใช้ในหน่วยงานที่มีหลายสาขา หรือ มีสำนักงานกระจายอยู่ในหลายภูมิภาค ในระบบ VPN การเชื่อมต่อระหว่างสำนักงานโดยใช้เครือข่าย Internet แทนการต่อเชื่อมด้วย Leased line หรือ Frame Relay

ทำไมต้องใช้ระบบเครือข่ายเสมือนส่วนตัว VPN

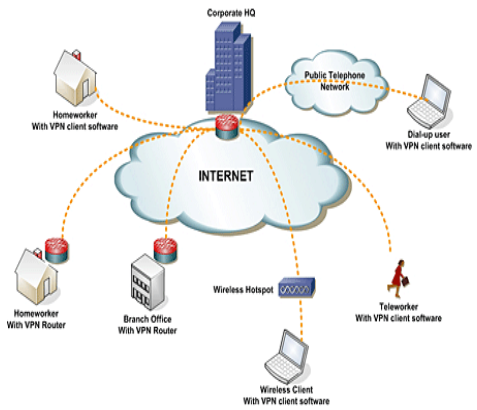
47

เทคโนโลยี VPN ได้เข้ามาเป็นอีกทางเลือกหนึ่ง เนื่องจากได้ใช้สื่อกลางคือ Internet ที่มีการติดตั้งอยู่อย่างแพร่หลายเข้ามาสร้าง ระบบเน็ตเวิร์คจำลอง โดยมีการสร้างอุโมงค์ข้อมูล (Tunnel) เชื่อมต่อกัน ระหว่างต้นทางกับปลายทาง ทำให้เสมือนว่าเป็นระบบเน็ตเวิร์คเดียวกัน สามารถส่งข้อมูลต่างๆที่ระบบเน็ตเวิร์คทำได้ โดยข้อมูลที่ส่งนั้นจะถูกส่งผ่านไปในอุโมงค์ข้อมูล ทำให้มีความปลอดภัยสูง ใกล้เคียงกับ leased line แต่ค่าใช้จ่ายในการทำ VPN นั้น ต่ำกว่าการเช่าสายสัญญาณมาก

ความสามารถของระบบเครือข่ายเสมือนส่วนตัว VPN

48

- การสร้างวงจรเสมือนจริงผ่านเครือข่าย Internet ใช้หลักการให้เครือข่ายย่อยเชื่อมกับ Internet ที่สำนักงานใหญ่ ซึ่งจะเสียค่าเช่าวงจรเฉพาะสาขา และค่าบริการ Internet เท่านั้น ทำให้เราสามารถใช้งาน Internet ได้เหมือนเครือข่ายภายในสำนักงานของเราเลย
- มีความปลอดภัยในการใช้งานค่อนข้างสูง

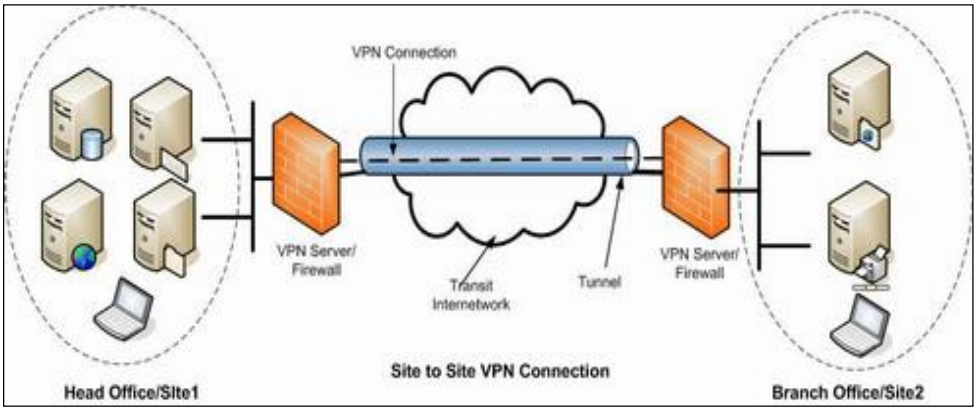


รูปแบบการให้บริการของ VPN

49

❖**Intranet VPN (ปัจจุบันสำนักงานตรวจบัญชีสหกรณ์ใช้รูปแบบนี้)**

เป็นรูปแบบของ VPN ที่ใช้เฉพาะภายในองค์กรเท่านั้น เช่น การเชื่อมต่อเครือข่ายระหว่างสำนักงานใหญ่กับสำนักงานย่อยในกรุงเทพและต่างจังหวัด โดยเป็นการเชื่อมต่ออินเทอร์เน็ตผ่านผู้ให้บริการท้องถิ่นแล้วจึงเชื่อมต่อเข้ากับเครือข่ายส่วนตัวเสมือนขององค์กร จากเดิมที่ทำการเชื่อมต่อโดยใช้ Leased Line หรือ Frame relay

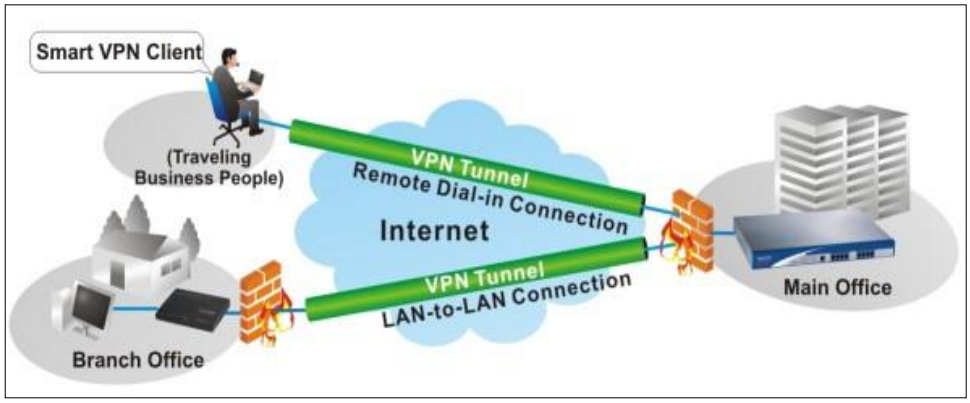


รูปแบบการให้บริการของ VPN

50

❖**Remote Access VPN**

เป็นรูปแบบการเข้าถึงเครือข่ายระยะไกลจากอุปกรณ์เคลื่อนที่ต่าง ๆ ซึ่งสามารถเข้าถึงเครือข่ายได้ใน 2 ลักษณะ ลักษณะแรก เป็นการเข้าถึงจากไคลเอ็นต์ทั่วไป ไคลเอ็นต์จะอาศัยผู้ให้บริการอินเทอร์เน็ตเป็นตัวกลางในการติดต่อและเข้ารหัสการส่งสัญญาณจากไคลเอ็นต์ไปยังเครื่องไอเอสพีและลักษณะที่สองเป็นการเข้าถึงจากเครื่องแอ็กเซสเซิร์ฟเวอร์ (Network Access Server-Nas)



51

ข้อดีของระบบ VPN

- สามารถขยายการเชื่อมต่อเครือข่ายได้แม้ว่าเครือข่ายนั้นจะอยู่สถานที่ต่างกัน
- มีความยืดหยุ่นสูงเพราะสามารถใช้ VPN ที่ใดก็ได้ และยังสามารถขยาย Bandwidth ในการใช้งานได้ง่ายดาย โดยเฉพาะในการทำ Remote Access ให้ผู้ใช้ติดต่อเข้ามาใช้งานเครือข่ายได้จากสถานที่อื่น
- สามารถเชื่อมโยงเครือข่ายและแลกเปลี่ยนข้อมูลออกภายนอกองค์กรได้อย่างปลอดภัย โดยใช้มาตรการระบบเปิดและมีการเข้ารหัสข้อมูลก่อนการส่งข้อมูลทุกครั้ง
- สามารถลดค่าใช้จ่ายในการเชื่อมต่อ ง่ายต่อการดูแลรักษาการใช้งานและการเชื่อมต่อ

ข้อเสียของระบบ VPN

- ไม่สามารถที่จะควบคุมความเร็ว การเข้าถึงและคุณภาพของ VPN ได้ เนื่องจากVPN ทำงานอยู่บนเครือข่ายอินเทอร์เน็ตซึ่งเป็นเรื่องที่อยู่เหนือการควบคุมของผู้ดูแล
- VPN ยังถือว่าเป็นเทคโนโลยีที่ค่อนข้างใหม่สำหรับประเทศไทยและมีความหลากหลายต่างกันตามผู้ผลิตแต่ละราย ฉะนั้นจึงยังไม่มีมาตรฐานที่สามารถใช้ร่วมกันได้แพร่หลาย
- VPN บางประเภทต้องอาศัยความสามารถของอุปกรณ์เสริมเพื่อช่วยในการเข้ารหัส และต้องมีการอัพเกรดประสิทธิภาพ

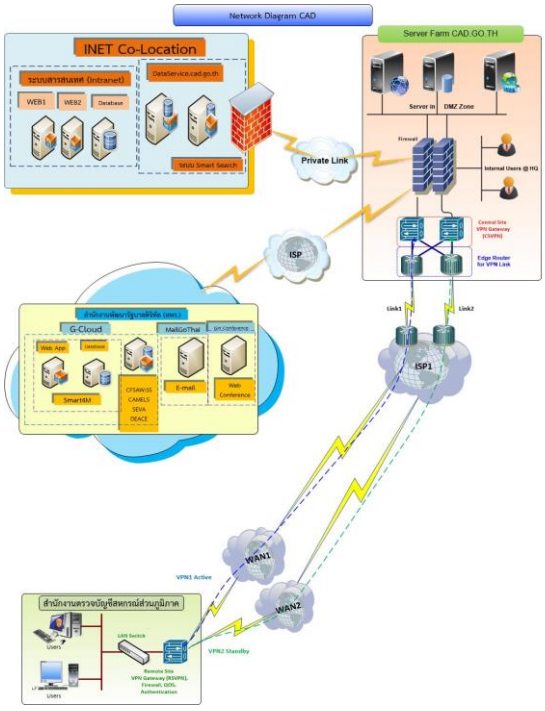
03

ระบบเครือข่ายคอมพิวเตอร์ของสำนักงานตรวจบัญชีสหกรณ์ในภาพรวม

เพื่อให้ผู้เข้าอบรมทราบถึงโครงสร้างระบบเครือข่ายของหน่วยงาน

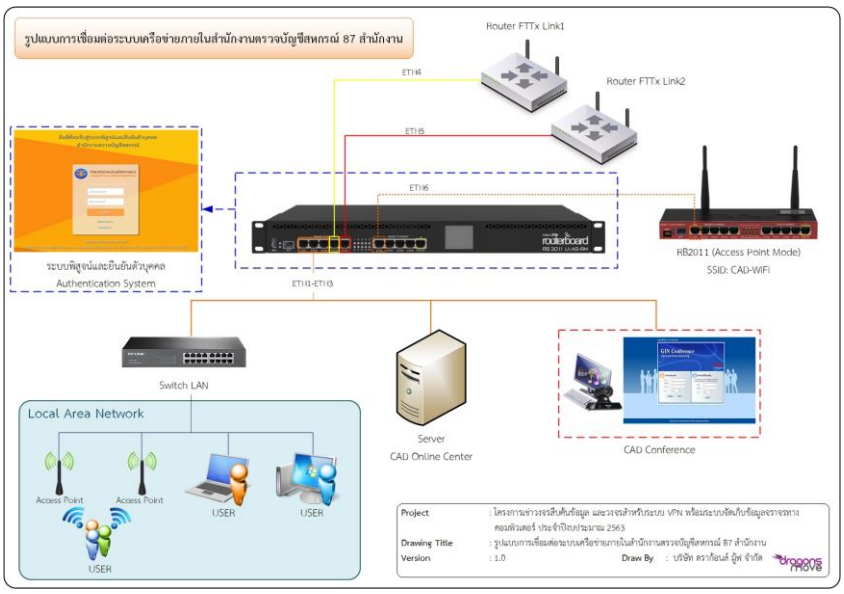
ระบบเครือข่ายคอมพิวเตอร์ของสำนักงานตรวจบัญชีสหกรณ์ในภาพรวม

53



ระบบเครือข่ายที่ใช้งานภายในสำนักงานตรวจบัญชีสหกรณ์

54



ระบบเครือข่ายที่ใช้งานภายในสำนักงานตรวจบัญชีสหกรณ์

55

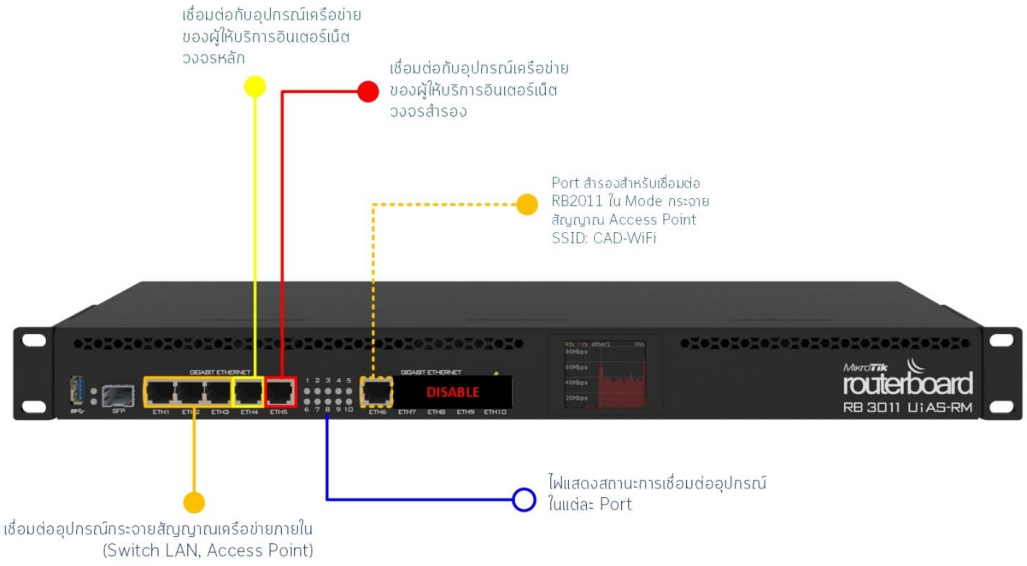
อุปกรณ์ Router ของผู้ให้บริการอินเตอร์เน็ต เช่น CAT, TOT, 3BB, TRUE เป็นต้น จำนวน 2 วงจร

อุปกรณ์ VPN Router ทำหน้าที่เชื่อมต่อกับอุปกรณ์ Router ของผู้ให้บริการอินเตอร์เน็ตทั้ง 2 วงจร เพื่อให้บริการอินเตอร์เน็ตผ่านระบบ Authentication พร้อมระบบจัดเก็บ LOG รวมไปถึงทำหน้าที่เชื่อมต่อ VPN ไปยังกรมตรวจบัญชีสหกรณ์ และยังทำงานในลักษณะ Active/Standby เมื่อวงจรอินเตอร์เน็ตวงจรใดวงจรหนึ่งขัดข้อง ให้ใช้งานอินเตอร์เน็ตผ่านวงจรอินเตอร์เน็ตอีกหนึ่งวงจรได้

อุปกรณ์กระจายสัญญาณภายในสำนักงาน เช่น Switch หรือ Access Point เป็นต้น

การเชื่อมต่ออุปกรณ์เครือข่ายภายในสำนักงานตรวจบัญชีสหกรณ์

56

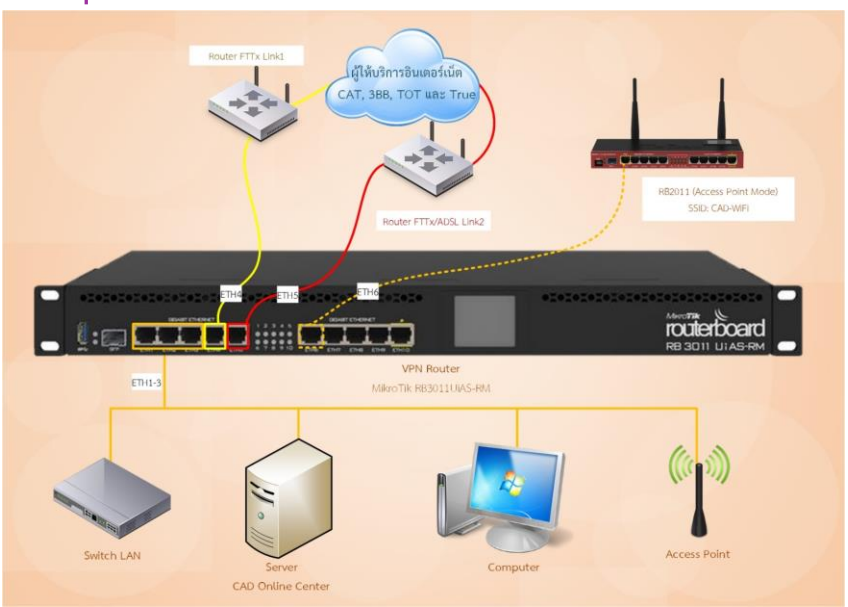


การเชื่อมต่ออุปกรณ์เครือข่ายภายในสำนักงานตรวจบัญชีสหกรณ์ 57

ช่องทางการเชื่อมต่อระบบเครือข่ายภายในอุปกรณ์ RB3011UiAS-RM

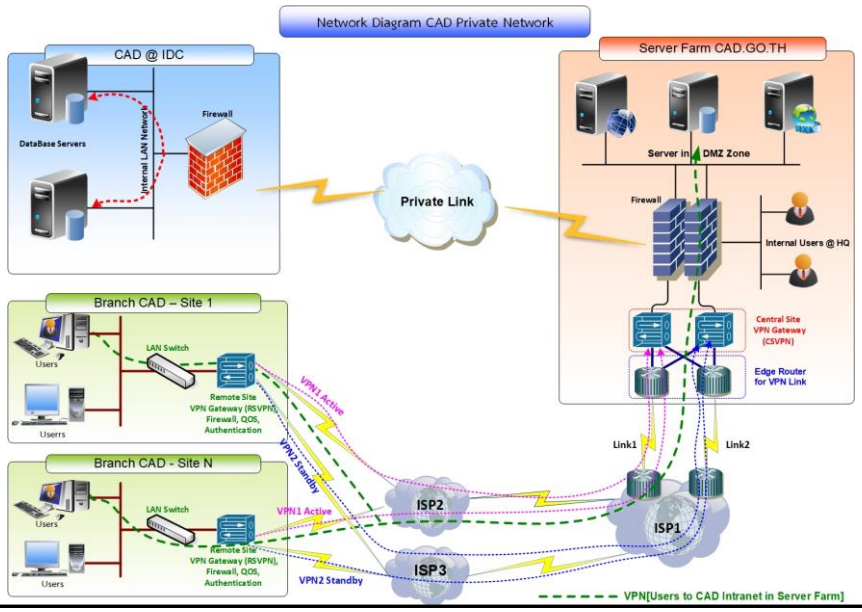
ETH 1 (PoE)	: ระบบ CAD Conference หรืออุปกรณ์กระจายสัญญาณเครือข่ายภายใน (Switch LAN, Access Point)
ETH 2	: ระบบ CAD Conference หรืออุปกรณ์กระจายสัญญาณเครือข่ายภายใน (Switch LAN, Access Point)
ETH 3	: ระบบ CAD Conference หรืออุปกรณ์กระจายสัญญาณเครือข่ายภายใน (Switch LAN, Access Point)
ETH 4	: FTTx อินเตอร์เน็ตวงจรหลัก
ETH 5	: FTTx อินเตอร์เน็ตวงจรสำรอง
ETH 6	: สำหรับ RB2011 Access Point Mode SSID: CAD-WiFi
ETH 7 – ETH10	: ปิดการใช้งาน (Disable)

การเชื่อมต่ออุปกรณ์เครือข่ายภายในสำนักงานตรวจบัญชีสหกรณ์ 58



ลักษณะการเชื่อมต่อระหว่างกรมตรวจบัญชีสหกรณ์กับสำนักงานตรวจบัญชีสหกรณ์ส่วนภูมิภาค ผ่านช่องทาง VPN

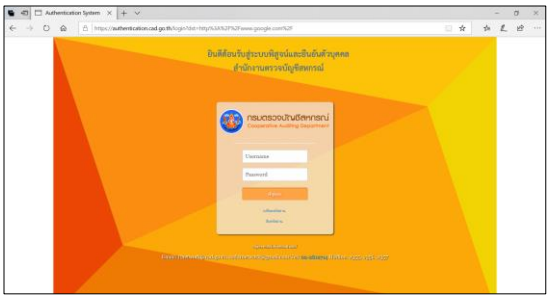
59



ระบบพิสูจน์ตัวตน Authentication System

60

- สามารถใช้งาน Username และ Password ของตัวเองได้ภายในสำนักงานตรวจบัญชีสหกรณ์ส่วนภูมิภาคทั้ง 87 สำนักงาน
- สามารถเปลี่ยนรหัสผ่านได้ด้วยตนเอง



ขั้นตอนการขอใช้งานระบบ Authentication System

- กรอกข้อมูลลงบนแบบฟอร์มขอชื่อผู้ใช้และรหัสผ่าน Authentication สำหรับหน่วยงานส่วนภูมิภาค
- Scan และส่งแบบฟอร์มไปที่ e-mail : netgrp@cad.go.th

ระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (log) ภายในสำนักงาน

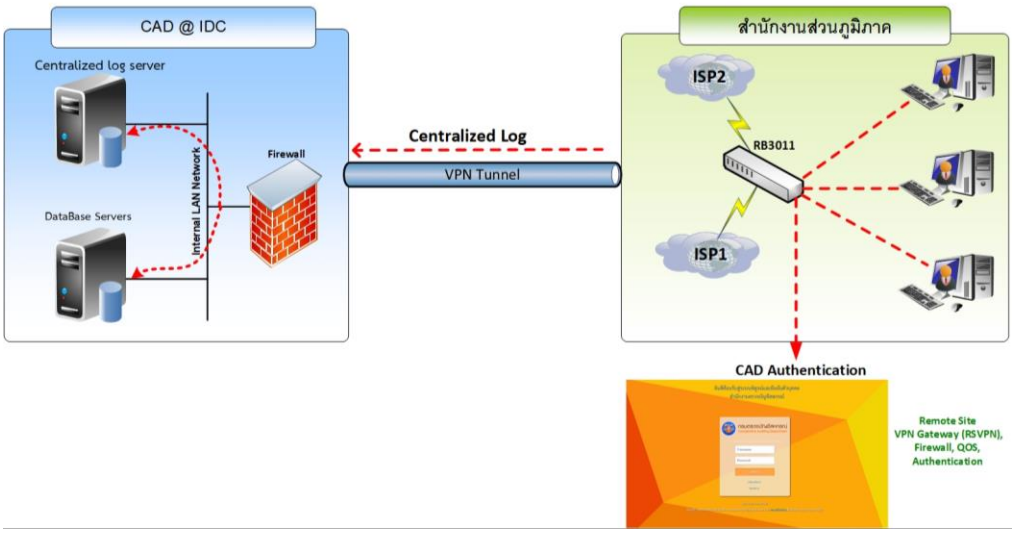
61

ระบบบริหารจัดการเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยมีการจัดเก็บที่ส่วนกลางแบบรวมศูนย์ และแยกออกจากการเก็บ Log Fileภายในเครื่องแม่ข่าย เนื่องจากการเก็บ Log File ในเครื่องแม่ข่ายในทุกวันนี้ถือว่าไม่ “Comply” ตาม พ.ร.บ. ฯ เนื่องจากเราไม่สามารถรักษาความถูกต้องของข้อมูล หรือ “Integrity” สำหรับ Log File ที่เก็บอยู่ในเครื่องแม่ข่ายได้ เพราะผู้ดูแลระบบ หรือ “System Administrator” สามารถเข้าถึง Log File ในเครื่อง และสามารถเข้าไปแก้ไข Log File ได้ นอกจากนี้แฮกเกอร์ หรือ MalWare อาจเข้ามาลบ Log File ในเครื่องได้ทุกเมื่อ ถ้าแฮกเกอร์สามารถเจาะเข้าเครื่องแม่ข่ายและยึดเครื่องแม่ข่ายได้สำเร็จ ทำให้ Log File ที่อยู่ในเครื่องแม่ข่ายนั้นขาดความน่าเชื่อถือในการดำเนินคดีในชั้นศาล (Admissibility in Court)

การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ หรือ Log File ที่ถูกต้องนั้น ควรต้องจัดเก็บแบบรวมศูนย์ที่ส่วนกลาง โดยแยกระบบออกเป็นอิสระจากเครื่องแม่ข่าย และระบบ Centralized Log Management ต้องสามารถป้องกันการเข้ามาแก้ไข Log File โดยไม่ได้รับอนุญาต อีกทั้ง ต้องสามารถเก็บ Log File ไว้ได้นานตามที่กฎหมายระบุไว้ คืออย่างน้อย 90 วัน เรียกว่า “Log Retention Period” ดังนั้น ฮาร์ดดิสก์ หรือระบบ Storage ของ Centralized Log Management System ต้องถูกออกแบบมาโดยเฉพาะใช้ในการเก็บ Log เท่านั้น

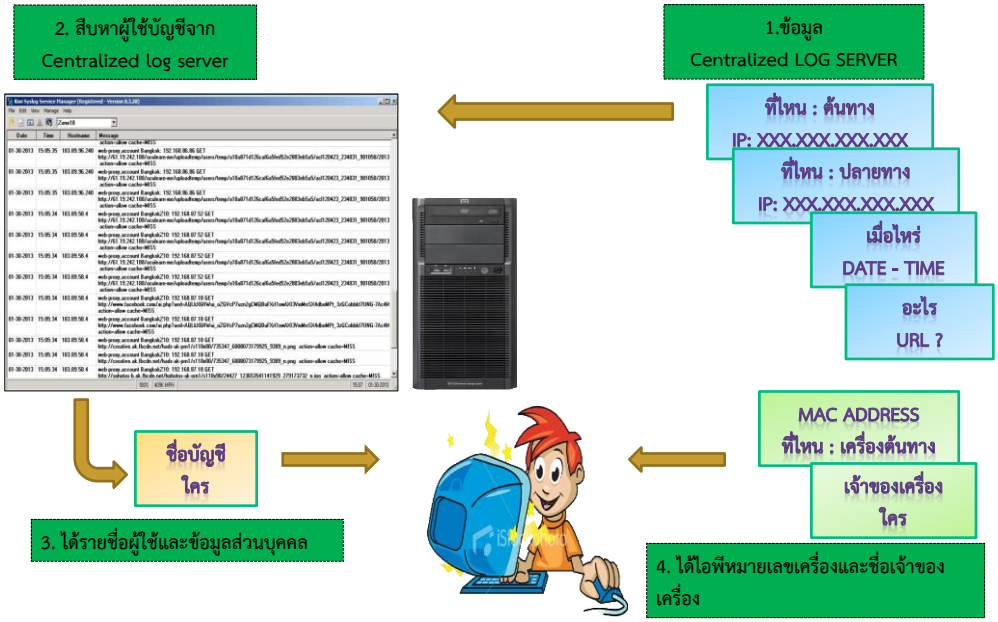
ระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (log) ภายในสำนักงาน

62



ขั้นตอนการตรวจสอบข้อมูล Centralized Log

63



แผนกู้คืนระบบเครือข่ายภายในสำนักงานฯ (Disaster Recovery Plan: DRP)

64

Disaster Recovery Planning

คือ การวางแผนเพื่อกอบกู้ระบบ IT ให้สามารถดำเนินงานต่อไปได้หลังเกิดภัยพิบัติ หรือ สามารถทำงานได้อย่างต่อเนื่องในขณะที่เกิดภัยพิบัติ ซึ่งมีขั้นตอนต่างๆ กล่าวคือ การจัดการประเภทของภัยพิบัติ การประเมินความเสี่ยง การวางแผนป้องกัน การตรวจวัดและบันทึกข้อมูล

ขั้นตอนการทำ Disaster Recovery Plan: DRP

65

- ขั้นตอนแรกคือ Risk Analysis เพื่อวิเคราะห์ความเสี่ยงว่าจะมีภัยพิบัติประเภทไหนบ้าง
- ขั้นตอนที่ 2 คือ Risk Classification เพื่อจำแนกกลุ่มหรือประเภทความเสี่ยงตามมุมมองต่างๆ เช่น ความเสี่ยงที่เกิดจากภายนอก (External Risk) ความเสี่ยงของข้อมูล (Data System Risk) ความเสี่ยงของการให้บริการ (Service System Risk) ความเสี่ยงของระบบพื้นฐาน (Infrastructure Risk) เป็นต้น
- ขั้นตอนที่ 3 คือ Disaster Effect Analysis เพื่อประเมินผลของภัยพิบัติว่ามีผลกระทบกับเราอย่างไรบ้าง โดยขั้นตอนนี้มักทำร่วมกับขั้นตอนที่สอง คือ เมื่อแบ่งแยกประเภทความเสี่ยงได้ชัดเจนแล้ว ก็จะวิเคราะห์ว่าภัยพิบัติจะก่อให้เกิดผลอะไรต่อมา
- ขั้นตอนที่ 4 คือ Disaster Recovery Plan การวางแผนปฏิบัติงานในกรณีเกิดภัยพิบัติ ได้แก่ แผนรับมือภัยพิบัติขั้นปกติ แผนรับมือภัยพิบัติขั้นรุนแรง แผนการปฏิบัติเมื่อไม่สามารถป้องกันภัยพิบัติได้ แผนการกอบกู้ระบบ และ แผนการเริ่มต้นระบบสนับสนุนใหม่ เช่น เมื่อประเมินแล้วพบว่าไม่มีพลังงานไฟฟ้าใช้แล้วในช่วงสุดท้ายของอุทกภัย ก็ควรมีอุปกรณ์สร้างพลังงานสำรองไว้ใช้งาน เป็นต้น

04

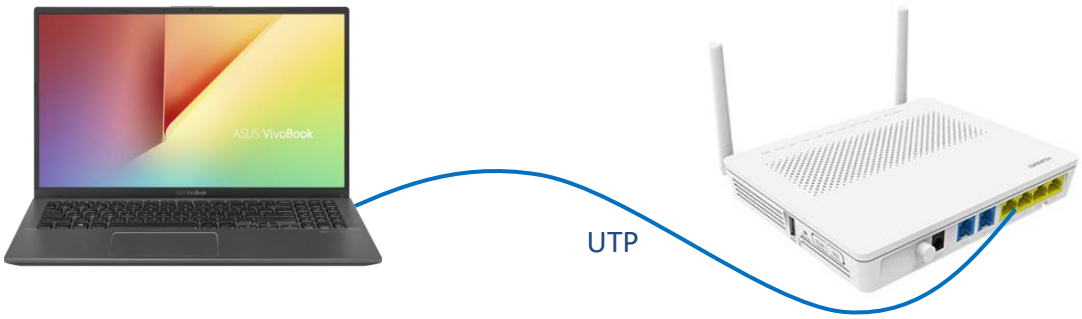
ความรู้พื้นฐานที่จำเป็นในการดูแลระบบเครือข่าย และการติดตั้งอุปกรณ์เครือข่าย

เพื่อให้ผู้เข้าอบรมได้มีความรู้ในการดูแลระบบเครือข่าย
รวมทั้งการติดตั้ง

ขั้นตอนการ Configuration อุปกรณ์ Router เบื้องต้น

67

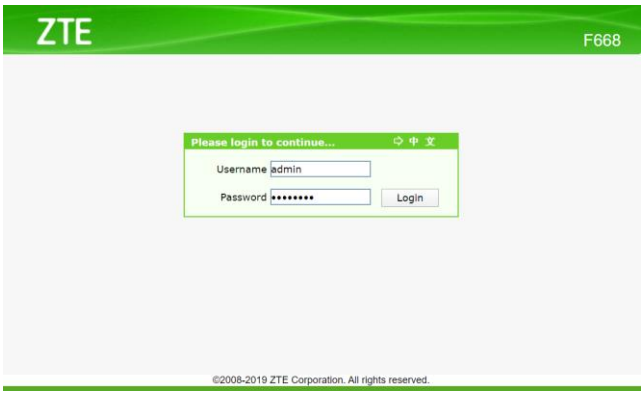
- เชื่อมต่อสาย UTP จากเครื่องคอมพิวเตอร์เข้า Port LAN ของอุปกรณ์ Router



ขั้นตอนการ Configuration อุปกรณ์ Router เบื้องต้น

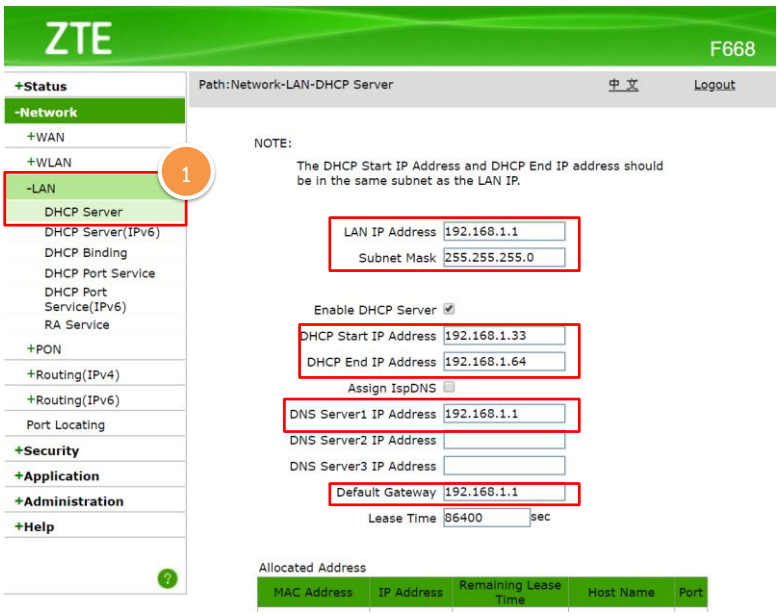
68

- เปิด Browser ขึ้นมาแล้วพิมพ์ IP Address ของอุปกรณ์ Router (ดูได้จาก Sticker ใต้อุปกรณ์)
- ให้กรอก Username, Password เพื่อเข้าสู่ขั้นตอนการตั้งค่า WAN



- การตั้งค่า WAN ไปที่เมนู Network > WAN
- กรอก Username, Password ที่ได้จากผู้ให้บริการ

69



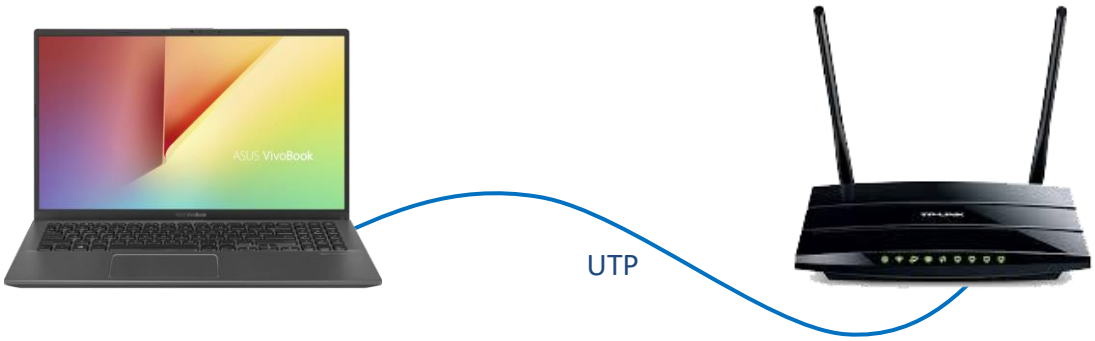
70

- การตั้งค่า DHCP และการจัดการ IP Address เป็นการจัดการและแจกจ่าย IP ไม่ให้ซ้ำกัน
- ไปที่เมนู Network > LAN > DHCP Server
- กำหนดค่า
  IP Address/Subnet ของอุปกรณ์
  IP Address เริ่มต้น
  IP Address สิ้นสุด

ขั้นตอนการ Configuration อุปกรณ์ Access Point เบื้องต้น

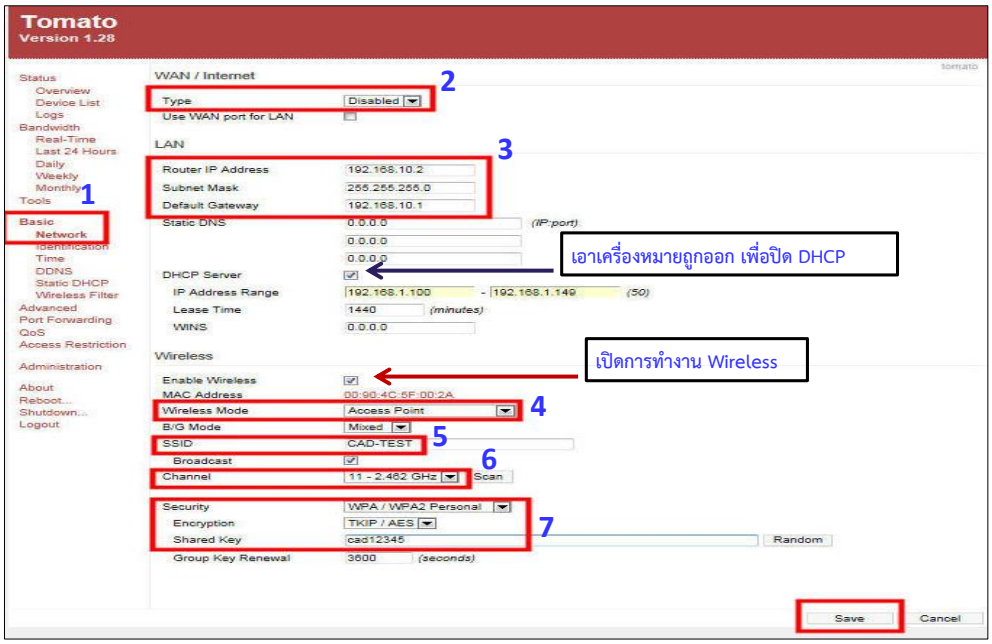
71

- เชื่อมต่อสาย UTP จากเครื่องคอมพิวเตอร์เข้า Port LAN ของอุปกรณ์ Access Point
- เปิด Browser ขึ้นมาแล้วพิมพ์ IP Address ของอุปกรณ์ Access Point (ดูได้จาก Sticker ใต้อุปกรณ์)
- ให้กรอก Username, Password เพื่อเข้าสู่ขั้นตอนการตั้งค่า Wireless



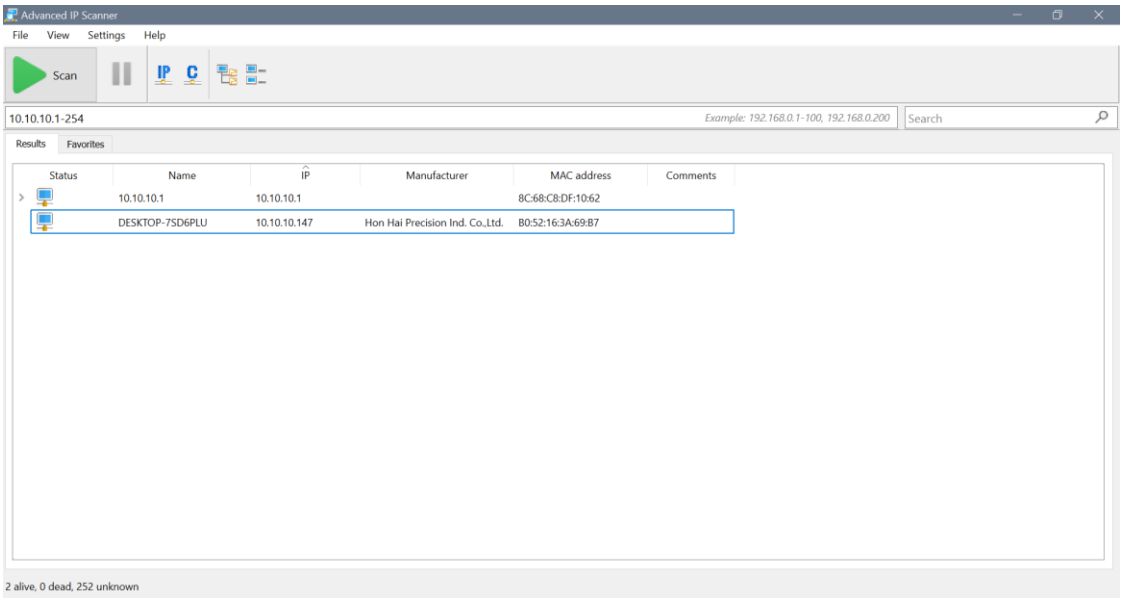
ขั้นตอนการ Configuration อุปกรณ์ Access Point เบื้องต้น

72



โปรแกรม Advanced IP Scanner

73



การรักษาความปลอดภัย (Security) ของ Access Point

74

WEP (Wired Equivalent Privacy)

ใช้การเข้ารหัสเพื่อช่วยป้องกันการรับข้อมูลไร้สายโดยไม่ได้รับอนุญาต WEP ใช้คีย์เข้ารหัสเพื่อเข้ารหัสข้อมูลก่อนที่จะส่ง เฉพาะคอมพิวเตอร์ที่ใช้คีย์เข้ารหัสเดียวกันเท่านั้นที่จะสามารถเข้าใช้เครือข่าย และถอดรหัสข้อมูลที่ส่งมาจากคอมพิวเตอร์เครื่องอื่น การเข้ารหัส WEP มีระดับความปลอดภัยสองระดับ โดยใช้คีย์ 64 บิต (บางครั้งเรียกว่า 40 บิต) หรือคีย์ 128 บิต (หรือ 104 บิต) เพื่อเพิ่มประสิทธิภาพการรักษาความปลอดภัย ควรใช้คีย์ 128 บิต หากคุณใช้การเข้ารหัส อุปกรณ์ไร้สายทั้งหมดบนเครือข่ายไร้สายของคุณจะต้องใช้คีย์เข้ารหัสที่ตรงกันด้วยการเข้ารหัส WEP สถานีไร้สายจะสามารถกำหนดค่าได้ถึง 4 คีย์ (ค่าดัชนีคีย์ได้แก่ 1, 2, 3 และ 4) เมื่อจุดเชื่อมต่อ (AP) หรือสถานีไร้สายส่งข้อความที่เข้ารหัสซึ่งใช้คีย์ที่บันทึกอยู่ในดัชนีคีย์ ข้อความที่ส่งจะระบุถึงดัชนีคีย์ที่ถูกใช้ในการเข้ารหัสเนื้อหาของข้อความ AP หรือสถานีไร้สายที่กำลังรับจึงสามารถรับคีย์ที่บันทึกอยู่ในดัชนีคีย์นั้นได้และใช้ในการถอดรหัสเนื้อหาข้อความที่เข้ารหัสไว้เนื่องจากอัลกอริธึมการเข้ารหัส WEP ถือเป็น *จุดอ่อน*สำหรับการโจมตีเครือข่าย ดังนั้นคุณจึงควรพิจารณาการใช้วิธีรักษาความปลอดภัยแบบ WPA-Personal หรือ WPA2-Personal

การรักษาความปลอดภัย (Security) ของ Access Point

75

WPA (Wi-Fi Protected Access)

➢**WPA-Personal**

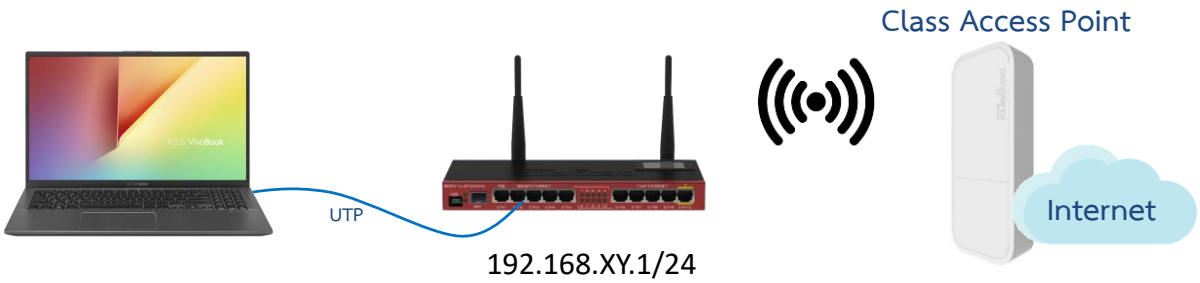
มุ่งหมายให้ใช้สำหรับสภาพแวดล้อมแบบในบ้านหรือธุรกิจขนาดเล็ก WPA Personal จำเป็นต้องใช้การกำหนดค่า pre-shared key (PSK) โดยผู้ใช้ที่จุดเชื่อมต่อและเครื่องลูกข่าย ไม่จำเป็นต้องใช้เซิร์ฟเวอร์การตรวจสอบความถูกต้อง รหัสผ่านชุดที่ป้อนที่จุดเชื่อมต่อจะต้องถูกนำมาใช้บนคอมพิวเตอร์เครื่องนี้และอุปกรณ์ไร้สายอื่นๆ ทั้งหมดที่เชื่อมต่อกับเครือข่ายไร้สาย ความปลอดภัยขึ้นอยู่กับความแข็งแกร่งและความลับของเครือข่าย รหัสผ่านที่ยาวช่วยรักษาความปลอดภัยเครือข่ายได้มากกว่ารหัสผ่านที่สั้น หากจุดเชื่อมต่อไร้สายหรือเราเตอร์ของคุณสนับสนุน WPA-Personal และ WPA2 Personal คุณควรเปิดใช้งานบนจุดเชื่อมต่อ และกำหนดรหัสผ่านแบบยาวที่ซับซ้อน WPA-Personal สามารถใช้ได้กับอัลกอริธึมการเข้ารหัสข้อมูล TKIP และ AES-CCMP

➢**WPA2-Personal**

WPA2-Personal จำเป็นต้องใช้การกำหนดค่า pre-shared key (PSK) โดยผู้ใช้ที่จุดเชื่อมต่อและเครื่องลูกข่าย ไม่จำเป็นต้องใช้เซิร์ฟเวอร์การตรวจสอบความถูกต้อง รหัสผ่านชุดที่ป้อนที่จุดเชื่อมต่อจะต้องถูกนำมาใช้บนคอมพิวเตอร์เครื่องนี้และอุปกรณ์ไร้สายอื่นๆ ทั้งหมดที่เชื่อมต่อกับเครือข่ายไร้สาย ความปลอดภัยขึ้นอยู่กับความแข็งแกร่งและความลับของเครือข่าย รหัสผ่านที่ยาวช่วยรักษาความปลอดภัยเครือข่ายได้มากกว่ารหัสผ่านที่สั้น WPA2 เป็นการปรับปรุงต่อยอดจาก WPA และปรับใช้มาตรฐาน IEEE 802.11i อย่างสมบูรณ์ WPA2 สามารถใช้งานร่วมกับ WPA WPA2-Personal สามารถใช้ได้กับอัลกอริธึมการเข้ารหัสข้อมูล TKIP และ AES-CCMP

Internet Access LAB

76



Internet Access LAB

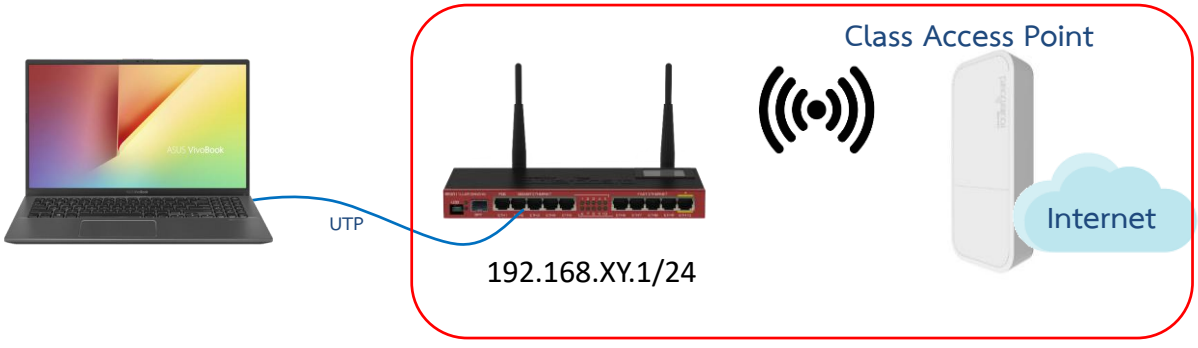
77

- Connect laptop to the router with a cable, plug it in any of LAN ports (2-5)
- Disable other interfaces (wireless) on yout laptop
- Make sure that Ethernet interface is set to obtain IP configuration automatically (via DHCP)

Internet Access LAB

78

- The Internet gateway of your class is accessible over wireless – it is an access point (AP)



Internet Access LAB

79

To connect to the AP you have to:

- Remove the wireless interface from the bridge interface (used in default configuration)
- Configure DHCP client to the wireless interface

Internet Access LAB

80

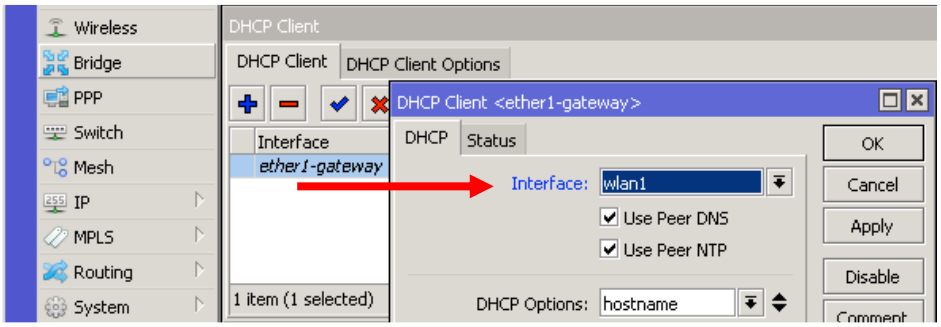
To connect to the AP you have to:

- Create and configure a wireless **security profile**
- Set the wireless interface to station mode
- And configure **NAT masquerade**

Internet Access LAB

81

Set DHCP client to the WiFi interface

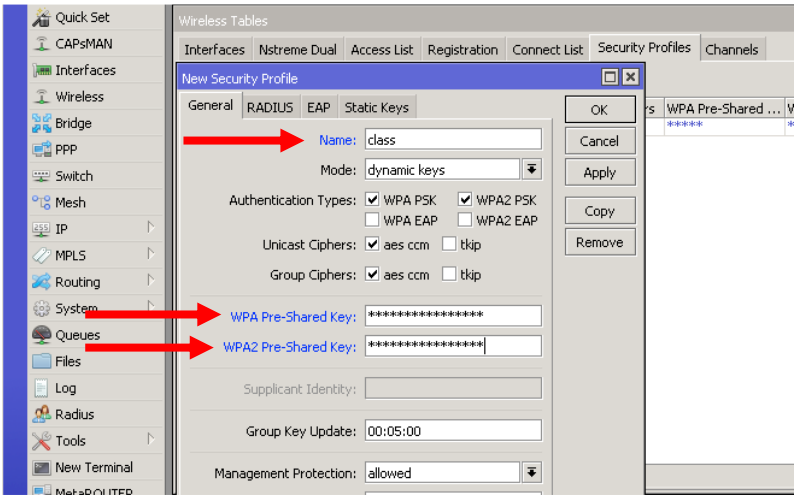


IP → DHCP Client

Internet Access LAB

82

Set Name and Pre-Shared Keys

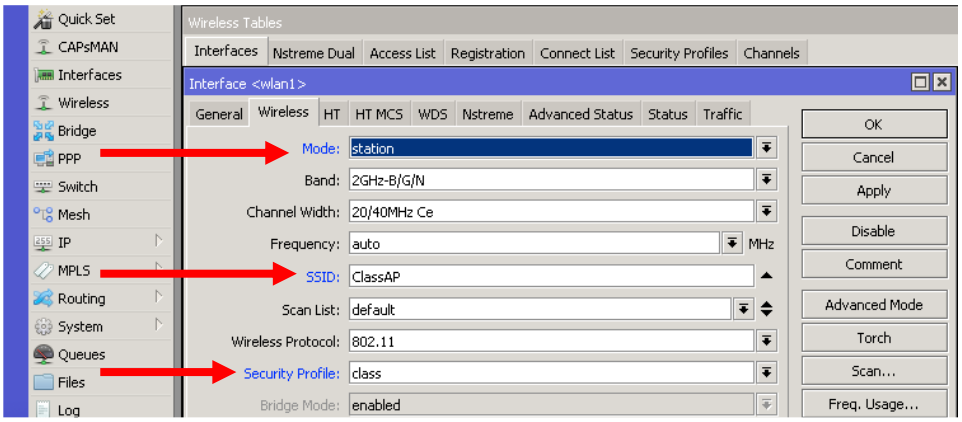


Wireless → Security Profiles

Internet Access LAB

83

Set Mode to 'station', SSID to 'ClassAP' and Security Profile to 'class'



Wireless →Interfaces

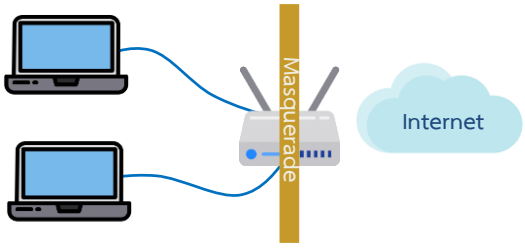
"Scan..." tool can be used to see and connect to available APs

Internet Access LAB

84

Private and Public Space

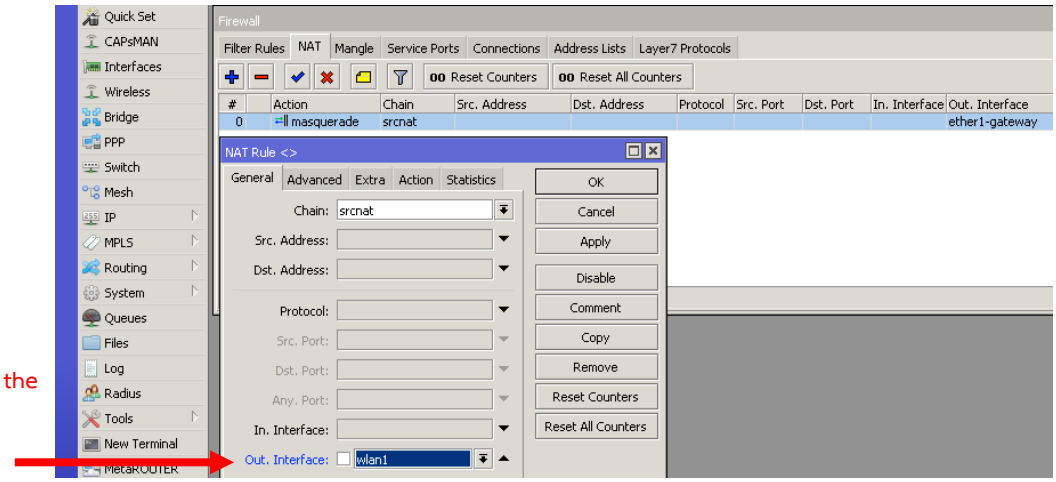
- **Masquerade** is used for Public network access, where private addresses are present
- Private networks include
  10.0.0.0 – 10.255.255.255,
  172.16.0.0 – 172.31.255.255,
  192.168.0.0 – 192.168.255.255



Internet Access LAB

85

Configure masquerade on the WiFi interface

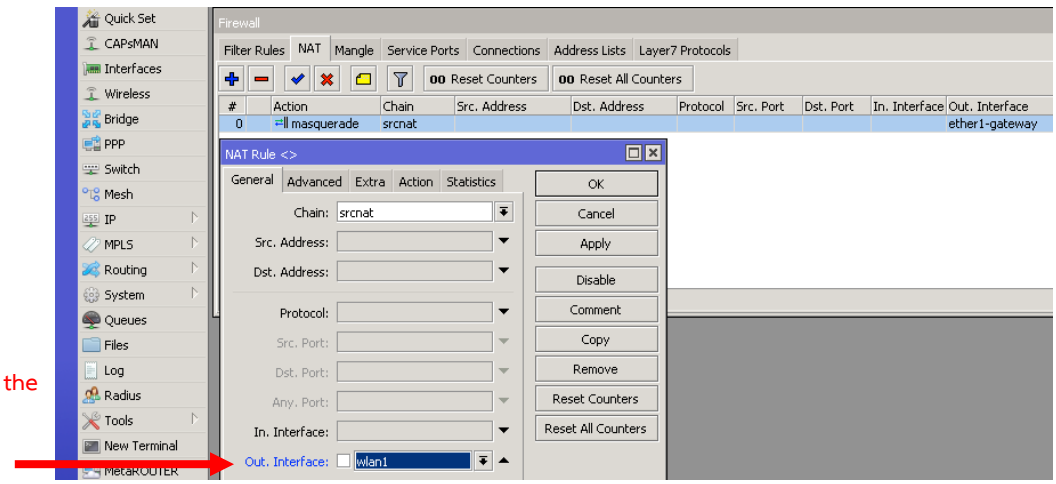


IP →Firewall →NAT

Internet Access LAB

86

Configure masquerade on the WiFi interface



IP →Firewall →NAT

Internet Access LAB

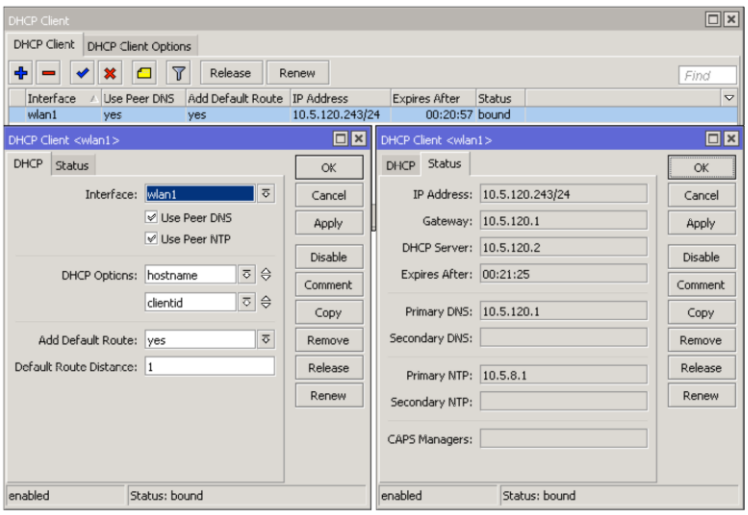
87

Configure DHCP

- Used for automatic acquiring of IP address, subnet mask, default gateway, DNS server address and additional settings if provided
- MikroTik SOHO routers by default have DHCP client configured on ether1(WAN) interface

Internet Access LAB

88



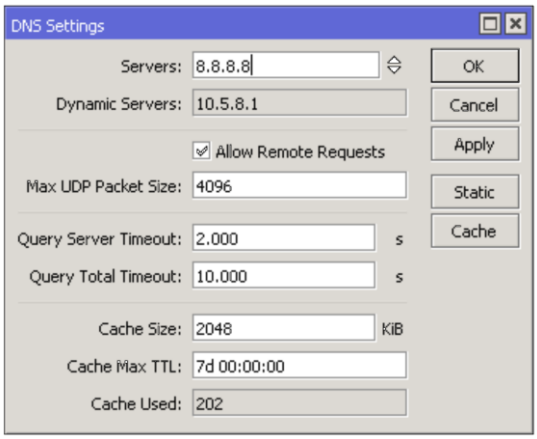
IP →DHCP Client

Internet Access LAB

89

DNS

- By default DHCP client asks for a DNS server IP address
- It can also be entered manually if other DNS server is needed or DHCP is not used



IP →DNS

DHCP Server

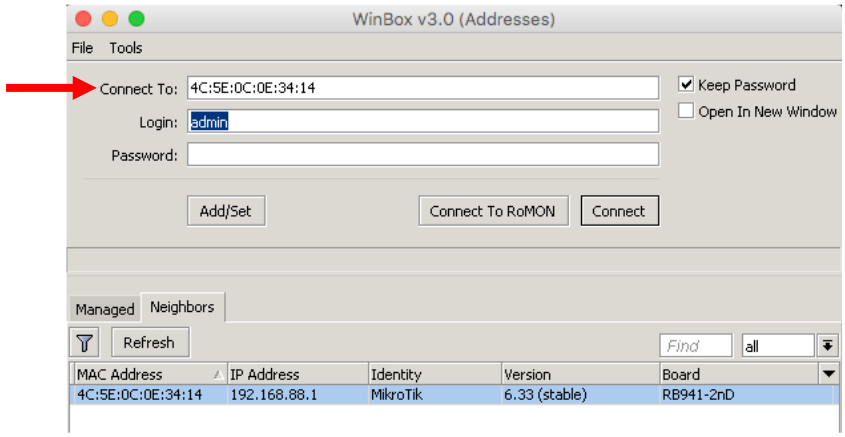
90

DHCP มาจาก Dynamic Host Configuration Protocol ซึ่งทำหน้าที่จ่าย IP ให้แก่เครื่องลูก (clients) โดยอัตโนมัติ สำหรับ Network ที่มีเครื่องลูกหลายเครื่อง การกำหนด IP ให้แต่ละเครื่องบางครั้งก็ยากในการจดจำ ว่ากำหนด IP ให้ไปเป็นเบอร์อะไรบ้างแล้ว พอมีเครื่องเพิ่มเข้ามาใน Network ใหม่ ต้องกลับไปค้น เพื่อจะ assign เบอร์ IP ใหม่ไม่ให้ซ้ำกับเบอร์เดิม DHCP Server จะทำหน้าที่นี้แทน โดยเครื่องลูกเครื่องไหนเปิดเครื่อง ก็จะขอ IP มายัง DHCP Server และ DHCP Server ก็จะกำหนด IP ไปให้เครื่องลูกเอง โดยไม่ซ้ำกัน

DHCP Server LAB

91

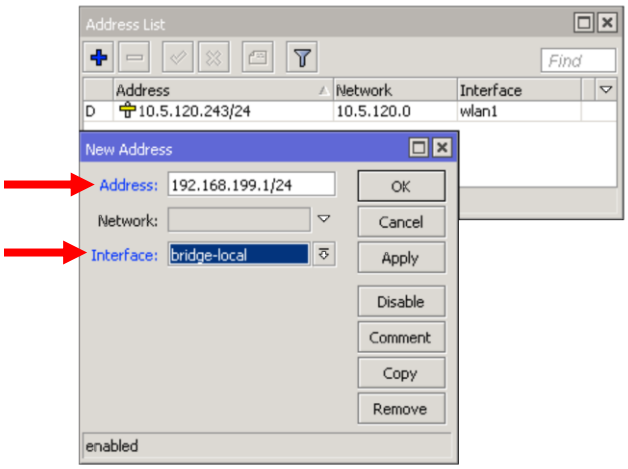
- Disconnect from the router
- Reconnect using the router's MAC address



DHCP Server LAB

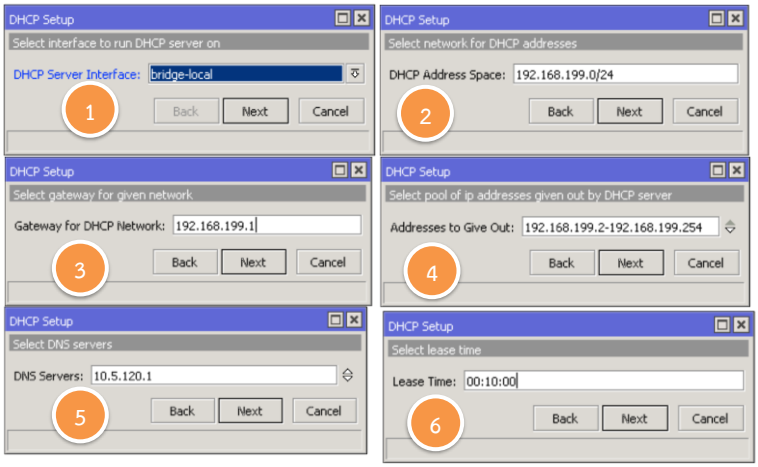
92

Add IP Address 192.168.XY.1/24 on the bridge interface



DHCP Server LAB

93



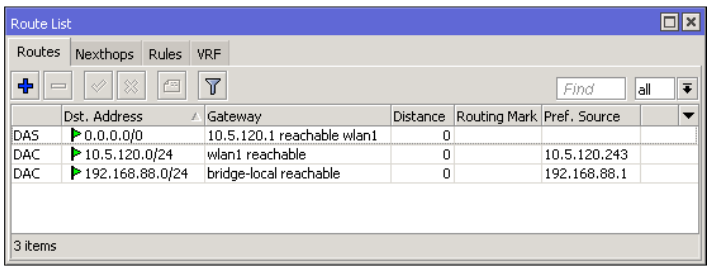
IP →DHCP Server →DHCP Setup

Static Route LAB

94

Routing

- Works in OSI network layer (L3)
- RouterOS routing rules define where the packets should be sent
- **Dst. Address**: networks which can be reached
- **Gateway:** IP address of the next router to reach the **destination**



IP →Routes

Static Route LAB

95

Routing

- If there are two or more routes pointing to the same address, the more precise one will be used
  - Dst: 192.168.90.0/24, Gateway: 1.2.3.4
  - Dst: 192.168.90.128/25, Gateway: 5.6.7.8
  - If a packet needs to be sent to 192.168.90.135, Gateway 5.6.7.8 will be used

Static Route LAB

96

- The goal is to ping your neighbor's laptop
- Static route will be used to achieve this
- Ask your neighbor the IP address of his/her wireless interface
- And the subnet address of his/her internal network (192.168.XY.0/24)

Static Route LAB

97

- Add a new route rule
- Set Dst. Address - your neighbor's local network address (eg.192.168.37.0/24)
- et Gateway - the address of your neighborâ€™s wireless interface (eg. 192.168.250.37)
- Now you should be able to ping your neighbor's laptop

Static Route LAB

98

- Team up with 2 of your neighbors
- Create a static route to one of your neighbor's (A) laptop via the other neighbor's router (B)
- Ask your neighbor B to make a static route to neighbor's A laptop
- Ping your neighbor' laptop

Static Route LAB

05

การตรวจเช็คและการแก้ไขปัญหาระบบเครือข่ายเบื้องต้น

เพื่อให้ผู้เข้าอบรมสามารถตรวจสอบและแก้ไขปัญหาระบบเครือข่ายเบื้องต้นได้

ปัญหาที่พบและวิธีการแก้ไขปัญหาเบื้องต้นบนระบบเครือข่าย 101

การตรวจสอบอุปกรณ์เครือข่ายภายในหน่วยงาน

อุปกรณ์ ONU/Router ISP

- Power - สถานะไฟ เขียว/ติดค้าง อุปกรณ์มีการเปิดติดปกติ
  - สถานะไฟ ไม่ติด แหล่งจ่ายไฟถูกตัดออก
- PON - สถานะไฟ ติดสีเขียว อุปกรณ์เชื่อมต่อกับอุปกรณ์ผู้ให้บริการปกติ
  - สถานะไฟ ติดกระพริบ อุปกรณ์พยายามติดต่อสื่อสารกับอุปกรณ์ผู้ให้บริการ
  - สถานะไฟ ดับ อุปกรณ์ไม่สามารถเชื่อมต่อกับอุปกรณ์ผู้ให้บริการได้
- LOS - สถานะไฟ ติด สีแดง สาย F/O ไม่ได้เชื่อมต่อหรือไม่มีการส่งสัญญาณ
  - สถานะไฟ ติดสีแดงกระพริบ ค่าส่งสัญญาณผิดปกติ
  - สถานะไฟ ดับ อุปกรณ์เชื่อมต่อสัญญาณปกติ

- LAN - สถานะไฟ ติด มีการเชื่อมต่อผ่าน Port LAN
  - สถานะไฟ ติดกระพริบ มีการรับ-ส่งข้อมูลผ่าน Port LAN
  - สถานะไฟ ดับ ไม่มีการเชื่อมต่อผ่าน Port LAN

ปัญหาที่พบและวิธีการแก้ไขปัญหาเบื้องต้นบนระบบเครือข่าย 102

อุปกรณ์ VPN Router (MikroTik RB3011)

- LAN - สถานะไฟ ติด มีการเชื่อมต่อผ่าน Port LAN
  - สถานะไฟ ติดกระพริบ มีการรับ-ส่งข้อมูลผ่าน Port LAN
  - สถานะไฟ ดับ ไม่มีการเชื่อมต่อผ่าน Port LAN

ข้อสังเกต

- หากสถานะไฟ LAN ไม่ติด แต่มีสาย UTP เชื่อมต่ออยู่บน Port แสดงว่าอุปกรณ์หรือเครื่องคอมพิวเตอร์ที่เชื่อมต่อปลายทางนั้นไม่ได้เปิดใช้งานหรือสายอาจจะหลุด

ปัญหาที่พบและวิธีการแก้ไขปัญหาเบื้องต้นบนระบบเครือข่าย

103

อุปกรณ์ Switch (Local Area Network : LAN)

- ไฟแสดงสถานะการทำงานของอุปกรณ์เมื่อมีการใช้งานจะมีไฟสีเขียวติดค้าง หรือกระพริบ
- หากไฟสถานะ Port ใด Port หนึ่งไม่ติด ให้ตรวจสอบว่าสายแลนต่อแน่นหรือไม่

ปัญหาที่พบและวิธีการแก้ไขปัญหาเบื้องต้นบนระบบเครือข่าย

104

กรณีที่	สถานการณ์การใช้งาน		สถานะ/สาเหตุ
	เว็บไซต์กรมตรวจฯ www.cad.go.th	เว็บไซต์ทั่วไป (google, youtube, pantip ฯลฯ)	
1	✓	✓	ระบบเครือข่ายอินเตอร์เน็ตและระบบ VPN ปกติ
2	✗	✗	ระบบเครือข่ายอินเตอร์เน็ตขัดข้อง/อุปกรณ์กระจายสัญญาณเครือข่ายขัดข้อง
3	✓	✗	เว็บไซต์ภายนอก หรือ ระบบอินเตอร์เน็ตบางส่วนเข้าไม่ได้
4	✗	✓	อาจเกิดจากระบบ VPN ขัดข้อง เนื่องจากเว็บไซต์และระบบสารสนเทศของกรมตรวจบัญชีสหกรณ์ใช้งานผ่านช่องทางของระบบ VPN

ปัญหาที่พบและวิธีการแก้ไขปัญหาเบื้องต้นบนระบบเครือข่าย

105

วิธีแก้ไขปัญหาเบื้องต้น

ถ้าระบบอินเตอร์เน็ตมีปัญหา วิธีตรวจสอบสถานะฯ มีดังนี้

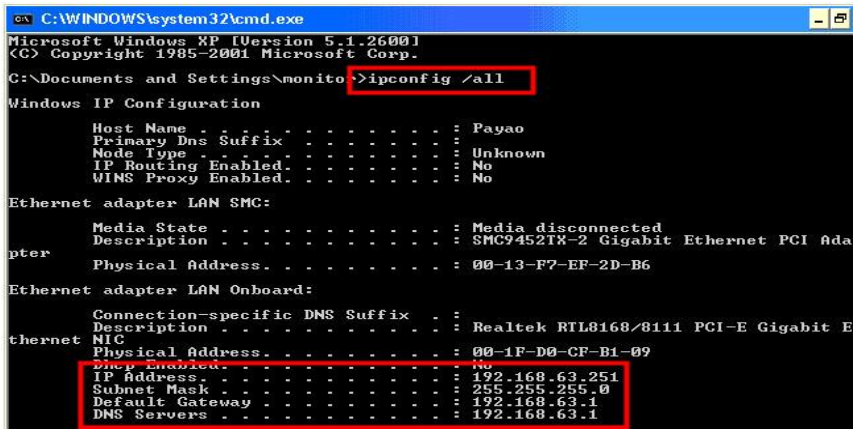
- กรณี ข้อที่ 2. ให้ตรวจสอบ สถานะไฟ Internet บนอุปกรณ์ของผู้ให้บริการว่าเป็นปกติหรือไม่ หรือ ปิด-เปิด อุปกรณ์ Rotuer ของผู้ให้บริการอินเตอร์เน็ต ใหม่ ถ้ายังไม่สามารถใช้งานได้ ติดต่อ จนท.กรมตรวจฯ หรือ แจ้ง CAT-TOT-TRUE-3BB ในพื้นที่บริการนั้นๆ
- กรณี ข้อที่ 3 - 4 ให้ติดต่อ จนท. กรมตรวจฯ โดยตรง
- ตรวจสอบดูว่า Internet ใช้งานไม่ได้ 1 เครื่อง หรือใช้งานไม่ได้ทั้งห้อง
- กรณีใช้งานไม่ได้เครื่องเดียว ให้เช็คสาย Lan จากเครื่อง PC ไปยัง Switch ดูว่าเป็น Port ไหน ลองทำการเปลี่ยน Port ดู
- ทำการตรวจเช็คค่า Config ดูว่าได้รับ IP Address ปกติหรือไม่ สถานะปกติจะได้รับ เช่น IP: 192.168.10.1
- ทำการทดสอบ Ping Gateway ดูว่า status เป็น Reply หรือ Request เช่น ping 192.168.10.1
- ทำการทดสอบ Ping DNS ดูว่า status เป็น Reply หรือ Request ทำการทดสอบ Service DNS โดยใช้คำสั่ง nslookup เช่น nslookup www.google.co.th หรือ nslookup www.cad.go.th

  ping www.google.co.th (ซึ่งจะอยู่ในเนื้อหาถัดไป)

คำสั่งต่างๆ บนเครื่องคอมพิวเตอร์ที่ใช้ในการแก้ไข และตรวจสอบปัญหาระบบเครือข่าย

106

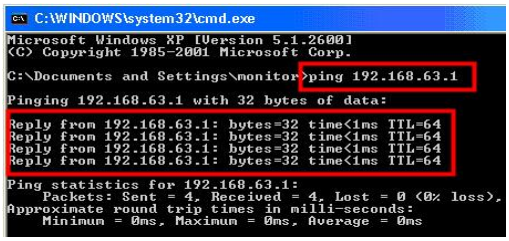
- **ipconfig** เป็นคำสั่งที่ใช้แสดง **IP Address, Subnet Mask, Default Gateway** หากใช้กับพารามิเตอร์ /all จะให้รายละเอียดเพิ่มเติมเกี่ยวกับ Physical Address, DHCP Server, DNS Server ฯลฯ



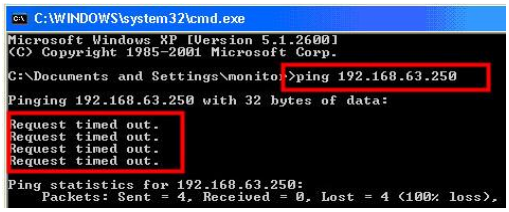
ping คำสั่ง ping จะส่งข้อมูล ICMP ประเภท "echo request" ไปยังเป้าหมาย และรายงานผลว่าเป้าหมายตอบกลับมาหรือไม่ ใช้เวลาส่ง-รับข้อมูลกี่มิลลิวินาที

107

Reply from " หมายความว่า เราสามารถติดต่อกับเป้าหมายปลายทางได้"



Request timed out " หมายความว่า เราไม่สามารถติดต่อกับเป้าหมายปลายทาง"



ค่า TTL: Time To Live คือเวลาที่ packet สามารถอยู่บนระบบได้ เพื่อไม่ให้มี packet ตกค้างอยู่บนระบบ โดยให้หมดอายุไปเอง ถ้า Packet ไม่สามารถเดินทางถึงปลายทาง

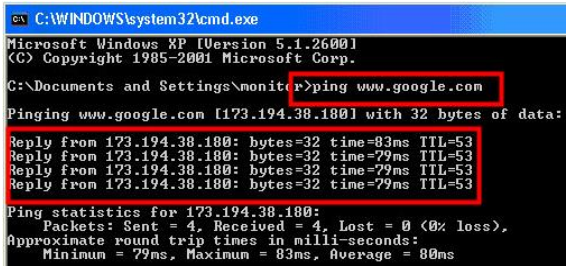
ตัวอย่าง.

- TTL = 64 เป็นระบบปฏิบัติการ (Operating System: OS) Linux หรือ Router ขนาดเล็ก
- TTL = 128 เป็นระบบปฏิบัติการจำพวก X 86 (Operating System: OS) เช่น Microsoft Windows
- TTL = 254 เป็น Router ขนาดกลาง , ใหญ่

ค่า TTL จะลดลงตามจำนวน Router ที่ packet วิ่งผ่าน

ทดสอบด้วยการ ping ไปเว็บไซต์ภายนอก

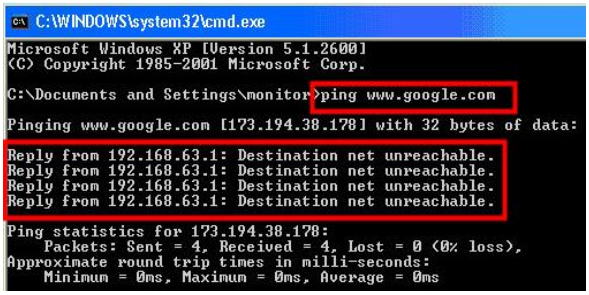
108



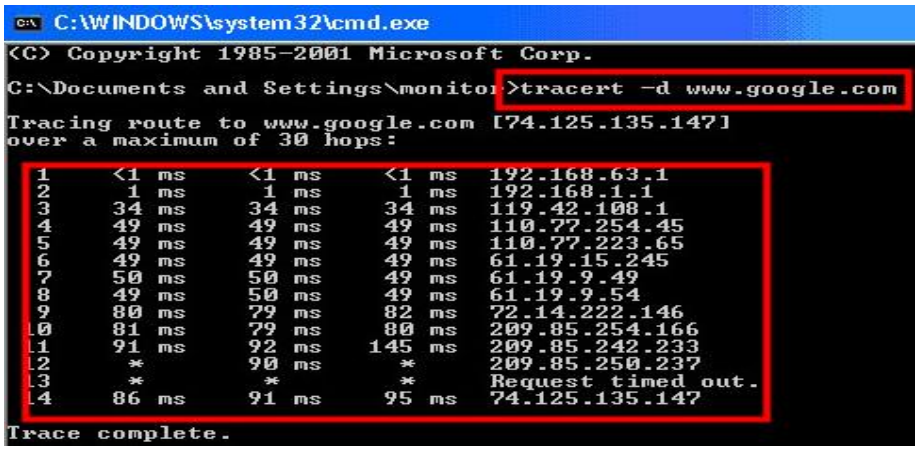
Reply from " หมายความว่า เราสามารถติดต่อกับเป้าหมายปลายทางได้"

Reply from 192.168.63.1 Destination net unreachable.

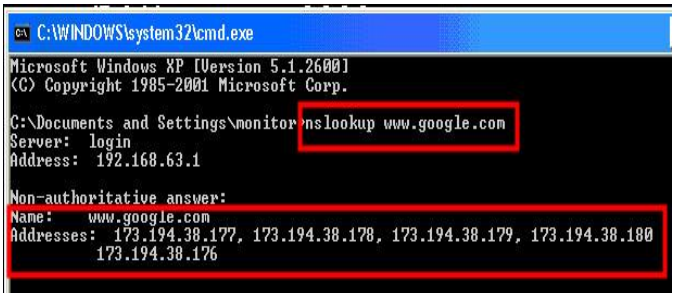
ไม่สามารถส่งข้อมูลและรับข้อมูลได้ ปัญหานี้จะเกิดกับ SNR ต่ำๆ หรือการเชื่อมต่อมีปัญหาหลุดบ่อย



tracert (ตาม ด้วย ip หรือชื่อเครื่องเป้าหมาย) เป็นคำสั่งที่ใช้ในการตรวจสอบว่าจากเครื่องเราไปถึงเครื่องเป้าหมายมันผ่าน เราท์เตอร์ตัวไหนบ้าง พูดง่ายๆว่าใช้เช็คเส้นทาง โดยใช้คุณสมบัติของ Time To Live (TTL) ในการทำงาน



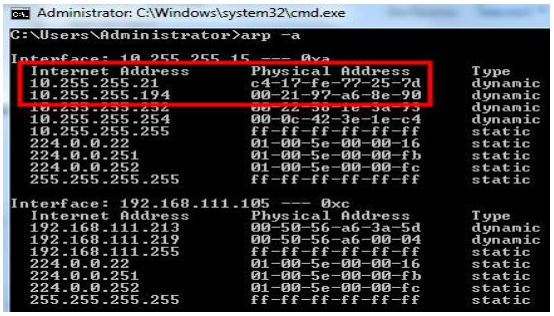
nslookup (ตามด้วย ip หรือชื่อเครื่องเป้าหมาย) ใช้ตรวจสอบข้อมูลเกี่ยวกับ DNSของเครื่องเป้าหมาย



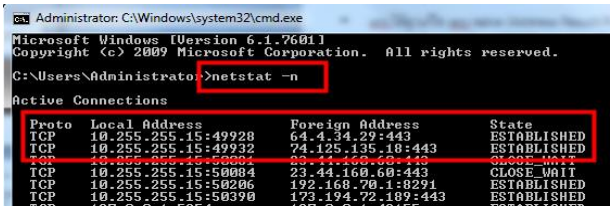
nslookup
www.google.com
(ตรวจสอบว่าเว็บไซต์นี้มี IP Address อะไร)

nslookup 31.13.79.7
(ตรวจสอบว่า IP Address นี้เป็นของเว็บไซต์อะไร

arp ใช้ดู/แก้ไข arp table (Address Result Protocol) คือตารางที่แสดงการแปลงค่า IP เป็น Physical Address โดยพารามิเตอร์ที่สั่งให้แสดงตารางคือ -a (พิมพ์ arp -a)



netstat เป็นคำสั่งที่ใช้แสดงการเชื่อมต่อผ่านเครือข่ายทั้งขาเข้าและขาออกจากเครื่องของเรา



CLOSE_WAIT_รอการตัด connection
TIME_WAIT _รอการตอบกลับจาก เครื่องที่ติดต่อ
ESTABLISHED connect สำเร็จและกำลังใช้งานอยู่

06

ความรู้พื้นฐานเกี่ยวกับเทคโนโลยี Cloud Computing และรูปแบบภัยคุกคามต่าง ๆ

เพื่อให้ความรู้ความเข้าใจเกี่ยวกับเทคโนโลยี Cloud Computing ซึ่งเป็นเทคโนโลยีใหม่ในปัจจุบัน รวมถึงแนวทางการป้องกันภัยคุกคามที่เกิดจากการแพร่ระบาดของไวรัสคอมพิวเตอร์ และสามารถแก้ไขปัญหาได้ทันท่วงที

113

What

is cloud computing?

114

Cloud Computing

is

“a mechanism for delivering scalable business services that execute on a decentralized computing fabric composed of commodity software and hardware”

NIST

cloud computing
definition

Cloud Computing

is

“a model for enabling ubiquitous, convenient,
on-demand network access to a
shared pool of configurable computing resources”

Essential Characteristics

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

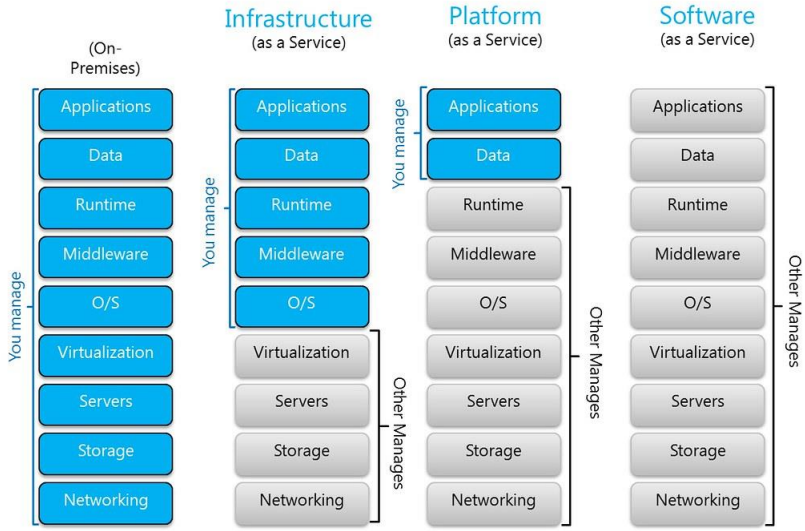
Service Models

- Infrastructure-as-a-service
- Platform-as-a-service
- Software-as-a-service

119

Service Models	Consumer Activities	Provider Activities
SaaS	Uses application/service for business process operations.	Installs, manages, maintains, and supports the software application on a cloud infrastructure.
PaaS	Develops, tests, deploys, and manages applications hosted in a cloud system.	Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment, and administration tools to platform consumers.
IaaS	Creates/installs, manages, and monitors services for IT infrastructure operations.	Provisions and manages the physical processing, storage, networking, and the hosting environment and cloud infrastructure for IaaS consumers.

120

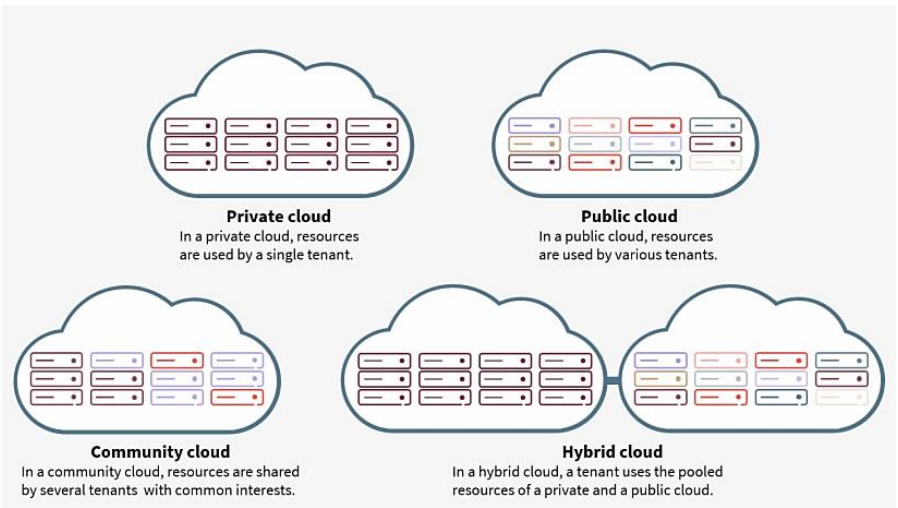


121

Deployment Models

- ✧ Private Cloud
- ✧ Public Cloud
- ✧ Hybrid Cloud
- ✧ Community Cloud

122



Why

use cloud computing?

Better

- ✧ Focus on your core business
- ✧ Infrastructure becomes SEP (Someone Else's Problem)

Faster

- ✧ Infrastructure on demand
- ✧ Provision via API, not phone calls
- ✧ Snapshot, clone and go. Repeat

Cheaper

- ✧ Reduced need for capital
- ✧ OpEx not CapEx
- ✧ Barrier to entry is much lower

129

Virus

is

"a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code"

130

Type of Virus

- ✧ Resident vs. non-resident viruses
- ✧ Macro virus
- ✧ Boot sector virus
- ✧ Email virus

131

Virus Effects

virus, spyware
social engineering

132

Virus Effects

✧ acquisition of hard disk space or central processing unit (CPU) time
✧ accessing and stealing private information
✧ corrupting data, displaying political, humorous or threatening messages on the user's screen
✧ spamming their e-mail contacts, logging their keystrokes, or even rendering the computer useless

133

Virus Prevention

- ✧ Anti-virus Software
- ✧ Security Practices

134

Spyware

is

"a software that aims to gather information about a person or organization, without their knowledge, and send such information to another entity without the consumer's consent"

135

Spyware Effects

✧ create significant unwanted CPU activity, disk usage, and network traffic.

✧ stability issues, such as applications freezing, failure to boot, and system-wide crashes

✧ causes difficulty connecting to the Internet

136

Spyware Prevention

✧ Anti-spyware Software

✧ Security Practices

137

Social Engineering

is

"the psychological manipulation of people into performing actions or divulging confidential information"

138

Social Engineering

- ✧ Phishing / Smishing
- ✧ Spam
- ✧ Impersonation
- ✧ Pretexting / Vishing
- ✧ Water holing
- ✧ Baiting
- ✧ Tailgating / Piggybacking

Social Engineering Protections

- ✧ delete any request for personal information or passwords
- ✧ reject requests for help or offers of help
- ✧ set your spam filters to high
- ✧ secure your devices
- ✧ always be mindful of risks

Thank You