

## Computer Networking How to

**C**ISCO

Asst. Prof. Suchart Khummanee.

## คำนำ

การศึกษาเกี่ยวกับระบบเครือข่ายในสมัยก่อนศึกษาได้จากตำรา เอกสารวิชาการ ซึ่งผู้เรียนจะได้แนวความคิด หลักการ และทฤษฎี ที่เกี่ยวกับระบบเครือข่าย ซึ่งส่งผลให้ผู้เรียนได้รับความรู้ในเชิงวิชาการ แต่ยังขาดทักษะในเชิงปฏิบัติซึ่งเป็นทักษะที่สำคัญที่จะทำให้ผู้เรียนเข้าใจในรายวิชา ดังกล่าวได้อย่างชัดเจน ปัจจุบันการศึกษาวิชาที่เกี่ยวข้องกับระบบเครือข่ายได้เปลี่ยนแปลงไปอย่างสิ้นเชิง เมื่อมีซอฟต์แวร์ที่เรียกว่าซอฟต์แวร์จำลองระบบเครือข่าย (Network Simulation) ซึ่งช่วยให้ผู้เรียนสามารถจำลองการทำงานของเครือข่ายให้เห็นภาพได้ชัดเจนมากขึ้น ส่งผลให้ผู้เรียนเข้าใจทฤษฎีที่เรียน เห็นภาพ สามารถทดสอบ และประยุกต์ตามความต้องการของผู้เรียนได้เป็นอย่างดี จากประสบการณ์ของผู้เขียนพบว่า ซอฟต์แวร์จำลองเครือข่ายช่วยให้ผู้เรียนมีความสนใจในการเรียน สนุกสนานในการเรียน และชอบเรียนในวิชาระบบเครือข่าย และป้อยครั้งส่งผลทำให้เกิดแรงบันดาลใจที่จะเป็นผู้ดูแลระบบเครือข่าย (Network Administrator) อย่างจริงจัง

ในหนังสือเล่มนี้ผู้เขียนเลือกเอาซอฟต์แวร์จำลองเครือข่ายมาถ่ายทอดความรู้ให้กับผู้ที่สนใจศึกษาเกี่ยวกับระบบเครือข่ายได้ศึกษา เนื่องจากมีผลดีตั้งที่กล่าวมาแล้วข้างต้น โดยเลือกใช้ Packet Tracer ซึ่งเป็นของบริษัท Cisco เนื่องจากซอฟต์แวร์ดังกล่าว มีส่วนเชื่อมต่อกับผู้ใช้ (GUI) ใช้งานง่าย อุปกรณ์มีให้เลือกใช้งานหลากหลาย ครอบคลุมเนื้อหา CCNA Exploration, CCNA Discovery, CCNA Security, CCNP (บางส่วน) มีคุณสมบัติบางอย่างดีมากๆ เช่น เชื่อมต่อเครือข่ายระหว่างผู้ใช้งานเข้าด้วยกัน (Multiuser), สร้างแบบฝึกฝนได้อิสระ (Activity Wizard), แสดงการทำงานของเครือข่ายอย่างละเอียดในระดับแพ็คเก็ต (Packet Sniffer), จำลองภารกิจการทำงานของโปรแกรมต่างๆ กำหนดโปรแกรมเพื่อทดสอบเครือข่ายได้อิสระ และรองรับโปรแกรมได้หลากหลาย

ในหนังสือนี้แบ่งออกเป็น 2 ส่วนคือ ส่วนแรก อธิบายความสามารถของ Packet Tracer, การติดตั้งใช้งาน, LAB การสอนพิกรเครือข่าย และเซิร์ฟเวอร์ (Scenario) ส่วนที่สอง อธิบายการสอนพิกรระบบเครือข่ายในระดับ Advanced โดยคำอธิบายอยู่ในรูปแบบของวีดีโอ (Workshop) โดยการบันทึกจากผู้เขียนจริง ผู้เขียนหวังว่าหนังสือเล่มนี้จะช่วยให้ผู้ที่สนใจด้านระบบเครือข่ายเกิดทักษะความรู้ ความชำนาญ และเรียนรู้ระบบเครือข่ายได้อย่างมีความสุข หากหนังสือเล่มนี้เกิดความผิดพลาดประการใด ผู้เขียนขออภัยไว้ ณ ที่นี้ด้วย หรือหากจะกรุณาแนะนำ หรือพบจุดบกพร่องสามารถส่งมาถึงผู้เขียนได้โดยตรงที่ suchart.k(@)msu.ac.th จักขอบพระคุณเป็นอย่างยิ่ง

ผู้เขียนขอสงวนลิขสิทธิ์ในหนังสือเล่มนี้เพื่อใช้เป็นวิทยาทานเท่านั้น ห้ามผู้ใด จำหน่าย พิมพ์เพื่อขาย ให้ดาวน์โหลดโดยคิดค่าบริการ หรือใช้ในเชิงพาณิชย์ทั้งสิ้น แต่อนุญาตให้แจกจ่ายได้

ผศ. สุชาติ คุ้มมะณี  
Suchart.k@msu.ac.th

พิมพ์เผยแพร่เมื่อ 15 ตุลาคม 2558

แก้ไขล่าสุด 15 ตุลาคม 2558

## สารบัญ

	หน้า
<b>บทที่ 1 เบื้องต้นเกี่ยวกับโปรแกรมจำลองเครือข่าย</b>	1
Simulation-Based Learning	2
คุณสมบัติและความสามารถของ Packet Tracer	2
<b>บทที่ 2 โปรแกรมจำลองเครือข่าย Packet Tracer</b>	17
ติดตั้งโปรแกรม Packet Tracer 5.3.x	17
เริ่มต้นการใช้งาน Packet Tracer	21
การจัดวางอุปกรณ์บนผังเครือข่าย (Workspace)	27
Creating a First Network	33
Devices and Modules	42
<b>บทที่ 3 How to Network Connectivity</b>	44
Scenario 1: เชื่อมต่อคอมพิวเตอร์ PC กับ PC	44
Scenario 2: เชื่อมต่อคอมพิวเตอร์ PC0, PC1 และ Laptop0 กับ HUB	45
Scenario 3: การวิเคราะห์แพ็คเก็ตอย่างละเอียด ตอนที่ 1	48
Scenario 4: การวิเคราะห์แพ็คเก็ตอย่างละเอียด ตอนที่ 2	53
Scenario 5: หลักการทำงานของ ARP โพรโทกอล	55
Scenario 6: เชื่อมต่อคอมพิวเตอร์ PC, Laptop กับ Switch L2 (เลเยอร์ 2)	59
Scenario 7: การติดตั้งเว็บเซิร์ฟเวอร์ (Web Server : HTTP)	62
Scenario 8: การติดตั้งโดเมนเนมเซิร์ฟเวอร์ (DNS)	67
Scenario 9: การติดตั้งอีซอชีพีเซิร์ฟเวอร์ (DHCP)	73
Scenario 10: การติดตั้ง SYSLOG เซิร์ฟเวอร์	79
Scenario 11: การติดตั้ง AAA/TACACS เซิร์ฟเวอร์	82
Scenario 12: การติดตั้ง NTP เซิร์ฟเวอร์	87
Scenario 13: การติดตั้ง EMAIL เซิร์ฟเวอร์ (SMTP/POP3)	90
Scenario 14: การติดตั้งเออฟทีพีเซิร์ฟเวอร์ (FTP)	96
Scenario 15: การติดตั้งทีเออฟทีพีเซิร์ฟเวอร์ (TFTP)	101
Scenario 16: การติดตั้ง Wireless Access Point	107
Scenario 17: การติดตั้ง Wireless Access Point (WEP Authentication)	110
Scenario 18: การคอนฟิก VLAN (บน switch 2900 series)	114
Scenario 19: การคอนฟิก VLANs และ Trunks (บน switch 2900 series)	117
Scenario 20: การคอนฟิก VTP (บน switch 2900 series)	120
Scenario 21: การคอนฟิก Switch L3 to L2 InterVLANs (Trunk Port)	123
Scenario 22: การคอนฟิก Switch L3 InterVLANs (Route VLAN)	126
Scenario 23: การคอนฟิก Switch L3 กับ Router และ Static Routing	128
Scenario 24: การคอนฟิกให้ Router ควบคุมสวิชต์ L3 หลายๆ ตัว	132
Scenario 25: การคอนฟิกให้สวิชต์ L3 ควบคุมสวิชต์ L3 หลายๆ ตัว	137

workshop 0: เป็องตันก่อนคอนฟิก

workshop 1: Introduction to Packet Tracer 5.3

workshop 2: How to Packet Tracer 5.3

workshop 3: การเพิ่ม/ลด อุปกรณ์

workshop 4: การใช้คำสั่ง IOS เป็องตัน

workshop 5: การเริ่มต้นคอนฟิกอุปกรณ์โดยผ่าน console

workshop 6: การคอนฟิกอุปกรณ์โดยผ่านโพรโทคอล Telnet

workshop 7: การคอนฟิกอุปกรณ์โดยผ่านโพรโทคอล Secure Shell

workshop 8: การคอนฟิก loopback interface

workshop 9: การคอนฟิก vlan บน switch L2

workshop 10: การคอนฟิก IP & Backup & Restore Configuration file บน Switch L2

workshop 11: การคอนฟิก vlan บน switch L3

workshop 12: การคอนฟิก static route บนเราเตอร์

workshop 13: การคอนฟิก static route บน Switch L3

workshop 14: การคอนฟิก static route ระหว่าง Router และ Switch L3

workshop 15: การเชื่อมต่อ Router ด้วยสาย Serial Interface

workshop 16: การเชื่อมต่อ Network บนโปรแกรม Packet Tracer เข้าด้วยกันโดยผ่าน Cloud (Multiuser)

workshop 17: การคอนฟิก Dynamic Routing (RIPv2)

workshop 18: การคอนฟิก Dynamic Routing OSPF(Single Area)

workshop 19: การคอนฟิก Dynamic Routing OSPF(Multiple Area)

workshop 20: การคอนฟิก OSPF Authentication

workshop 21: การคอนฟิก Dynamic Routing EIGRP

workshop 22: การคอนฟิก DHCP ข้ามเครือข่ายด้วย IP Helper

workshop 23: การคอนฟิกให้เราเตอร์ทำหน้าที่เป็น DHCP Server

workshop 24: การคอนฟิก OSPF กับ EIGRP โดยใช้ Redistribution

workshop 25: การคอนฟิก Standard ACL (1)

workshop 26: การคอนฟิก Standard ACL (2)

workshop 27: การคอนฟิก Standard ACL (3)

workshop 28: การคอนฟิก Extended ACL (1)

workshop 29: การคอนฟิก Extended ACL (2)

workshop 30: การคอนฟิก Extended ACL (3)

workshop 31: การคอนฟิก Link สำรอง โดยใช้ Floating Static Route

workshop 32: การคอนฟิก Static NAT

workshop 33: การคอนฟิก Static/Dynamic NAT ร่วมกับ ACL

workshop 34: การคอนฟิก Switch L3 ร่วมกับ Router

workshop 35: การคุณพิก BGP เปื้องต้น  
workshop 36: การใช้งาน Activity Wizard

Faculty of Informatics (MSU)

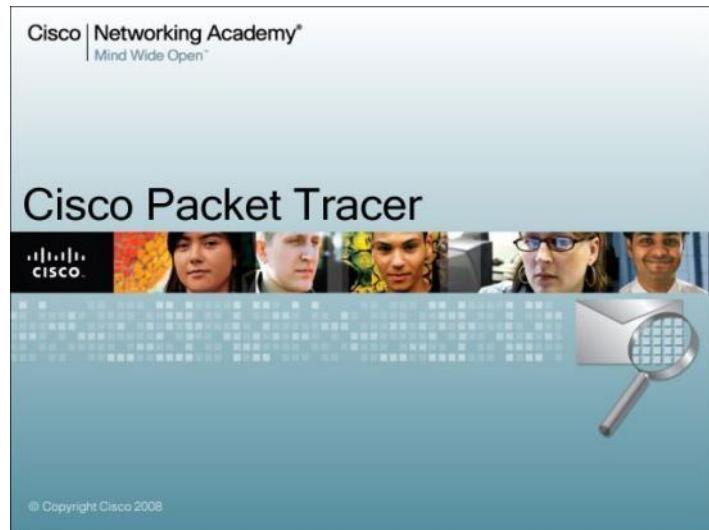
## บทที่ 1

### เบื้องต้นเกี่ยวกับโปรแกรมจำลองเครือข่าย

การจำลองการทำงานของระบบเครือข่าย (Network Simulation) และโปรแกรมจำลองเครือข่าย (Network Simulator) ทำหน้าที่จำลองการทำงานของอุปกรณ์เครือข่าย (Physical Device) เช่น เครื่องคอมพิวเตอร์ เครื่องเซิร์ฟเวอร์ เร��เตอร์ สวิตช์ สายนำสัญญาณ เป็นต้น และทำหน้าที่จำลองการทำงานของโพรโทคอลที่ใช้สื่อสารบนระบบเครือข่าย (Protocol) เช่น TCP/IP, UDP, RIP, OSPF, BGP, DHCP, DNS, HTTP เป็นต้น เป็นเทคโนโลยีใหม่ที่ทำงานในรูปแบบเสมือนจริง หรือ Virtual Packet Technology เพื่อช่วยในการออกแบบ วิเคราะห์ ติดตั้งระบบเครือข่าย เมื่อൺสถานะการณ์จริง ศึกษาพฤติกรรมการทำงานของระบบเครือข่าย ศึกษาการทำงานของโพรโทคอล วางแผนระบบเครือข่าย ปรับปรุงระบบเครือข่ายที่มีอยู่แล้วในองค์กร ลดระยะเวลาการเรียนรู้สร้างผู้ดูแลระบบเครือข่ายให้เกิดเชี่ยวชาญได้อย่างรวดเร็ว ลดต้นทุน ประหยัดเวลา ลดความเสี่ยง ทดสอบการทำงานก่อนติดตั้งอุปกรณ์จริง ค้นหาข้อผิดพลาดที่เกิดขึ้นในระบบเครือข่าย ช่วยในการวางแผนจัดซื้อ ประเมินราคาเบื้องต้น วางแผนในการเปลี่ยนแปลงเทคโนโลยี และเพื่อศึกษาทำการวิจัยในระดับสูง เป็นต้น

ถึงแม้ว่าโปรแกรมจำลองเครือข่ายจะมีคุณสมบัติที่เด่นมากหลายประการ แต่ก็ยังมีข้อเสีย อยู่หลายประการเช่นกัน คือ การจำลองไม่สามารถทดแทนการทำงานของอุปกรณ์จริงได้ 100 เปอร์เซ็นต์ ความสามารถของโปรแกรมจำลองขึ้นอยู่กับเจ้าของซอฟต์แวร์ว่าต้องการใส่คุณสมบัติอะไรเข้าไปให้ผู้ใช้งานได้บ้าง หรือคำสั่งในการทำงานไม่ครบ ดังนั้นโปรแกรมจำลองส่วนใหญ่จะมีประสิทธิภาพ และคุณสมบัติน้อยกว่าอุปกรณ์จริงเสมอ เว้นแต่ มีโปรแกรมจำลองบางประเภทที่ใช้ในทางวิจัย เช่น NS-2 ที่เน้นให้ผู้วิจัยสามารถสร้างโพรโทคอลขึ้นมาใหม่ได้ ข้อด้อยอีกประการหนึ่งคือ โปรแกรมจำลองส่วนใหญ่ทำงานอยู่ภายใต้ระบบแบบปิด (Closed System) คือไม่สามารถทำการส่งข้อมูลไปยังโปรแกรมจำลองตัวอื่นๆ ที่อยู่ต่างเครื่องกันได้ แต่ในปัจจุบันมีโปรแกรมจำลองหลายตัวได้พัฒนาให้มีความสามารถตั้งกล่าวแล้ว เช่น Packet Tracer เวอร์ชัน 5 ขึ้นไป

โปรแกรมจำลองเครือข่าย ที่นิยมใช้งานในปัจจุบันมีอยู่หลายยี่ห้อ โดยแต่ละยี่ห้อก็มีข้อเด่น ข้อด้อยที่แตกต่างกันไป สำหรับหนังสือเล่มนี้เลือกใช้ Packet Tracer เวอร์ชัน 5.3 ซึ่งทางบริษัทซิสโก้ (Cisco) เป็นผู้สร้างขึ้น เนื่องจากเหตุผลหลายประการในการเลือกใช้ เช่น โปรแกรม Packet Tracer มีอินเทอร์เฟสที่ง่ายต่อการใช้งาน โดยมีลักษณะการใช้งานแบบกราฟฟิก โปรแกรมมีอุปกรณ์ให้เลือกค่อนข้างมาก โดยมีตั้งแต่ การ์ดอินเตอร์เฟส เครื่องคอมพิวเตอร์ สายนำสัญญาณ สวิตช์ เร��เตอร์ DSL อุปกรณ์ประมวลผลแบบคลุ่มเมฆ ໄวเลส อื่นๆ อีกมาก โปรแกรมสามารถแสดงข้อมูลที่วิ่งบนเครือข่าย ได้อย่างละเอียด ทำให้ผู้ใช้งานเห็นภาพการทำงานของเครือข่ายได้เป็นอย่างดี โปรแกรมถูกพัฒนาอย่างต่อเนื่องและในอนาคตอาจจะครอบคลุมเนื้อหาเกี่ยวกับระบบเครือข่ายได้ทั้งหมด ปัจจุบันสามารถครอบคลุมเนื้อหาของ CCNA เกือบทั้งหมด และ CCNP บางส่วน โปรแกรมสามารถติดตั้งและใช้งานได้ทั้งระบบปฏิบัติการลินุกซ์และวินโดว์ส มีผู้ใช้งานเป็นจำนวนมาก ซึ่งในมหาวิทยาลัยส่วนใหญ่ๆ ทั่วโลกจะใช้สำหรับสอนเสริมในวิชาคอมพิวเตอร์เครือข่าย เครือข่ายชั้นสูง เป็นต้น ซึ่งจะกล่าวอย่างละเอียดสำหรับคุณสมบัติของ Packet Tracer ในหัวข้อถัดไป



โปรแกรม Packet tracer เป็นโปรแกรมประเภท Simulation-Based Learning คือ เป็นโปรแกรมที่ทำการสร้างสถานะการณ์จำลอง เพื่อทำให้ผู้เรียนเห็นภาพได้ชัดเจนขึ้น ทำให้ผู้เรียนและผู้สอนสามารถเรียนรู้ในการกระบวนการทำงานของเครือข่ายได้เป็นอย่างดี โปรแกรมดังกล่าวสนับสนุนให้ผู้เรียนผู้สอนสามารถทำงานร่วมกันเป็นทีม สร้างองค์ความรู้ใหม่ แก้ปัญหาที่มีความซับซ้อน ออกแบบระบบเครือข่าย กระตุ้นการเรียนรู้ เน้นให้สามารถทำงานได้จริง

คุณสมบัติและความสามารถของ Packet Tracer (version 5.3 ขึ้นไป)

Packet tracer มีความสามารถดังต่อไปนี้คือ

1. **Simulation** โปรแกรมมีความสามารถจำลองการทำงานของระบบปฏิบัติการ (IOS) และคำสั่งต่างๆ ที่ทำงานอยู่บนอุปกรณ์ของชิสโก้ได้เกือบสมบูรณ์แบบ สามารถจำลองการทำงานของโพรโทคอลที่ทำหน้าที่เราต์โพรโทคอล (Routing Protocol) อื่นๆ ให้ทำงานได้ เช่น RIP, OSPF, BGP เป็นต้น รวมถึงโพรโทคอลที่ถูกเราต์ด้วย เช่น FTP, HTTP, DNS, SMTP เป็นต้น

```

SiteB
Physical | Config | CLI |
IOS Command Line Interface
00:00:10: *OSPF 0 ADJCHG: Process 1, Nbr 192.168.0.226 on FastEthernet0/1 from Loading
to FULL, Loading Done
SiteB>ena
SiteB#sho ip rout
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

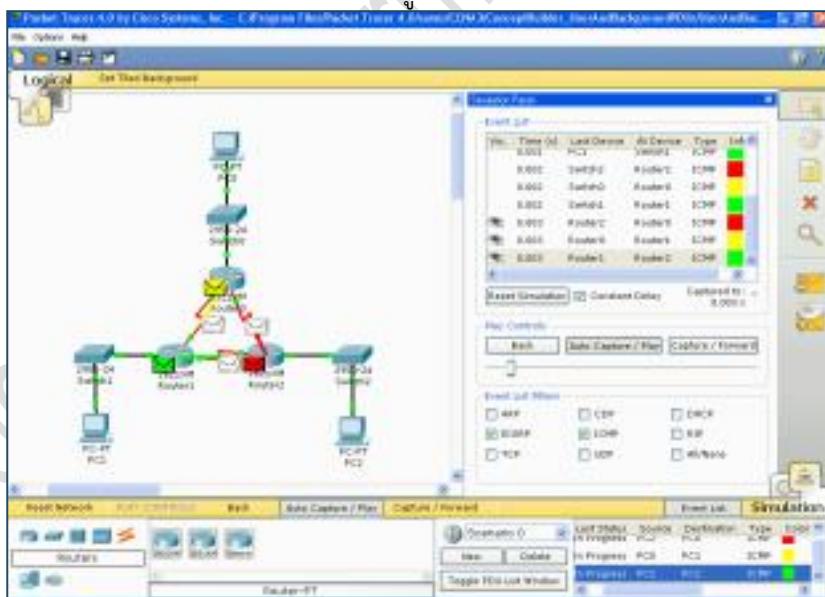
  192.168.0.0/24 is variably subnetted, 7 subnets, 3 masks
C    192.168.0.0/25 is directly connected, FastEthernet0/1
O    192.168.0.128/27 [110/129] via 192.168.0.229, 00:00:10, Serial0/1
C    192.168.0.160/27 is directly connected, FastEthernet0/0
O    192.168.0.192/27 [110/65] via 192.168.0.234, 00:00:20, Serial0/0
O    192.168.0.224/30 [110/128] via 192.168.0.229, 00:00:20, Serial0/1
C    192.168.0.228/30 is directly connected, Serial0/1
C    192.168.0.232/30 is directly connected, Serial0/0
SiteB#
00:00:45: *OSPF-5-ADJCHG: Process 1, Nbr 192.168.0.226 on FastEthernet0/1 from E
XCHANGE to FULL, Exchange Done
00:00:55: *OSPF-5-ADJCHG: Process 1, Nbr 192.168.0.234 on FastEthernet0/1 from E
XCHANGE to FULL, Exchange Done

```

Copy Paste

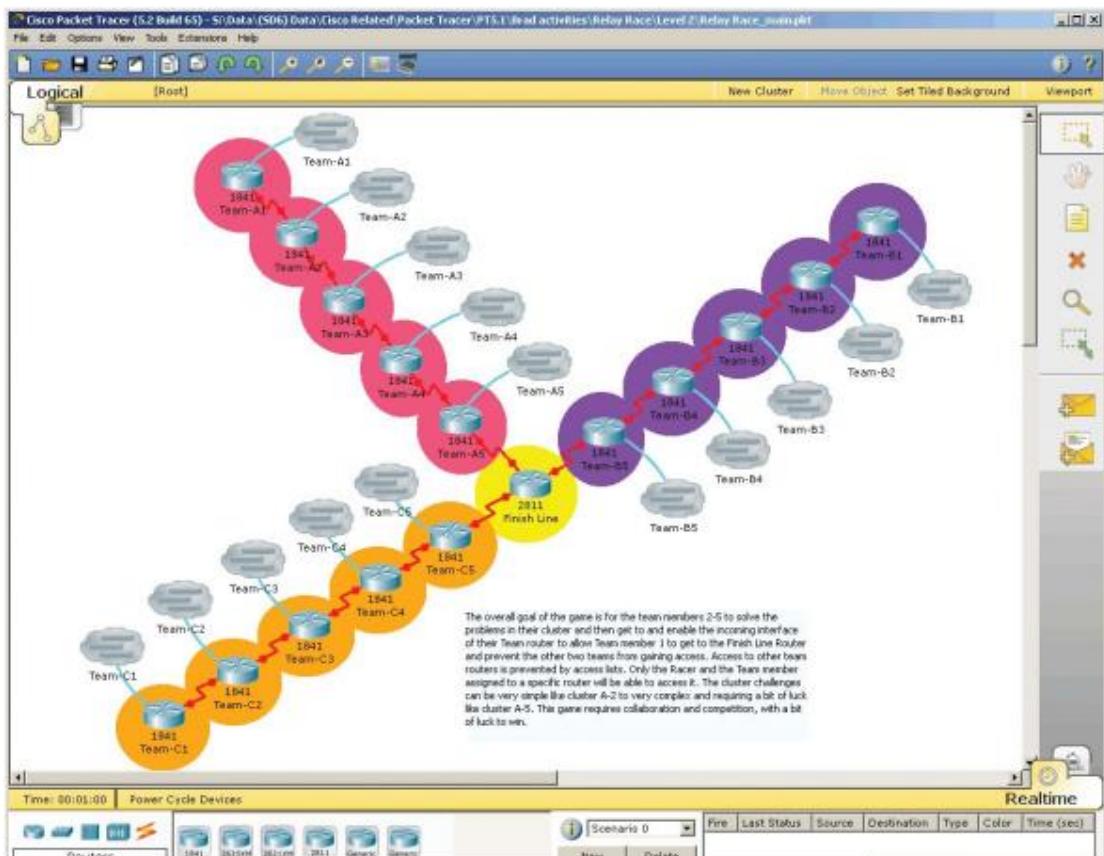
รูปที่ 1-1 จำลองการทำงานของ IOS

2. **Visualization** โปรแกรมมีความสามารถแสดงกระบวนการทำงานของเครือข่าย ในรูปแบบที่ง่ายต่อการทำความเข้าใจ เช่น แสดงเป็นรูปภาพ สี เสียง และมัลติมีเดีย



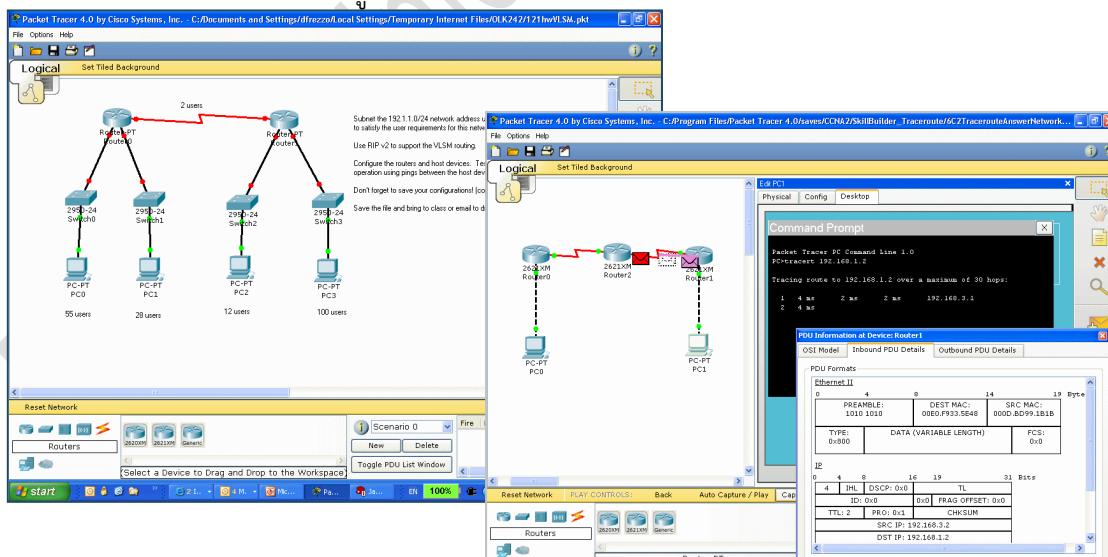
รูปที่ 1-2 แสดงการทำงานแบบ visualization

3. **Collaboration on Multiuser Activities** โปรแกรมมีความสามารถเชื่อมโยงเครือข่ายที่อยู่ต่างสถานที่กันให้สามารถเชื่อมต่อ กันได้



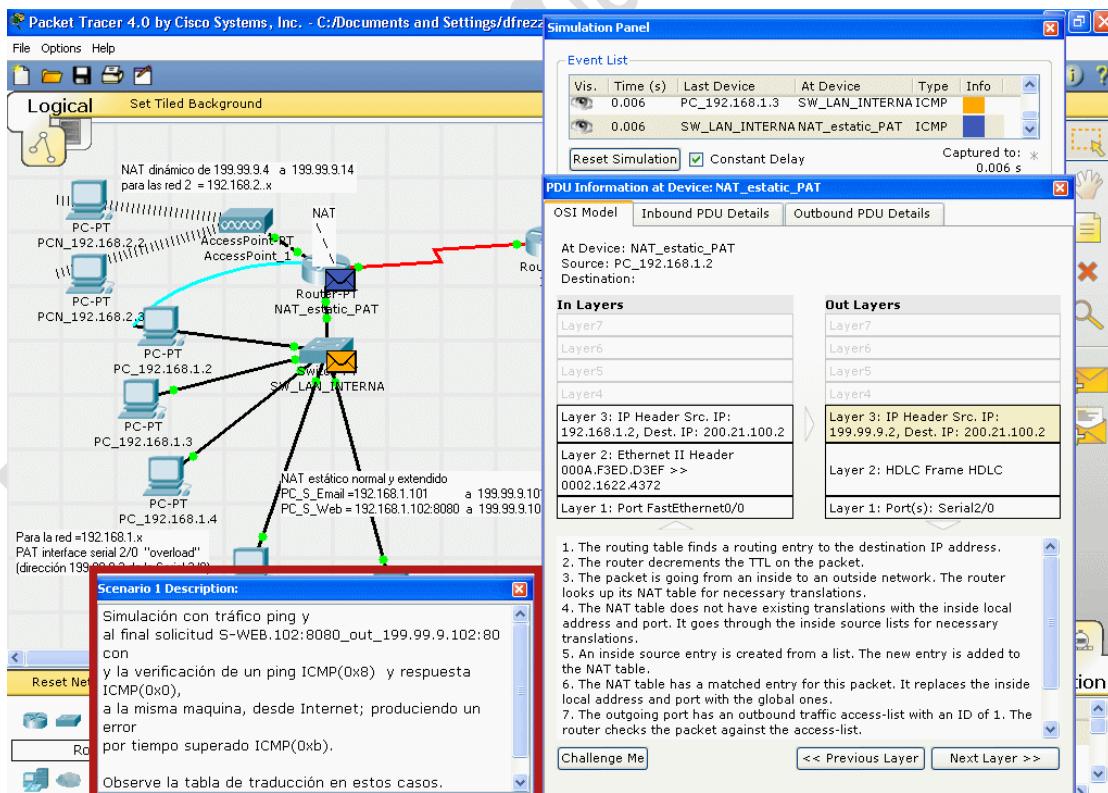
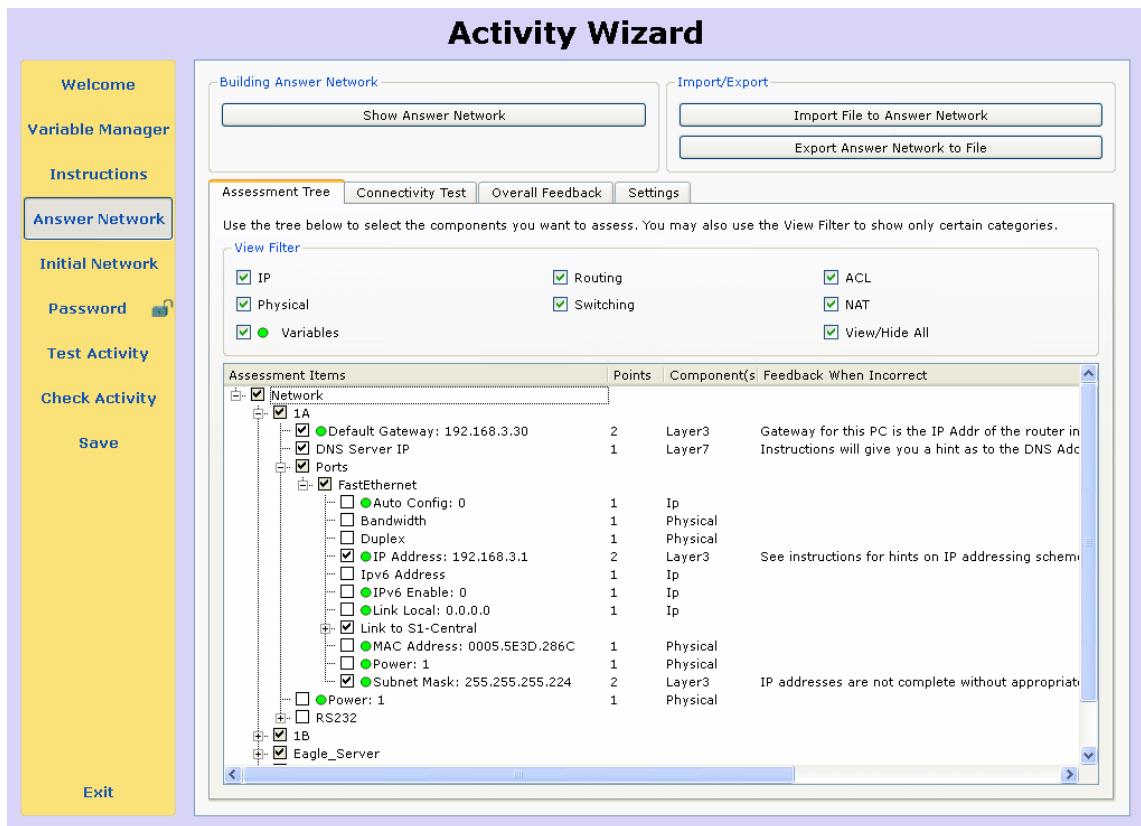
รูปที่ 1-3 แสดงการเขื่อมโยงเครือข่ายที่อยู่ต่างไซต์ (Collaboration)

#### 4. Homework and Pre-Lab รองรับและสนับสนุนให้ผู้เรียนสามารถทดสอบทำ LAB เกี่ยวกับเครือข่ายได้โดยสมบูรณ์



รูปที่ 1-4 แสดงการทดสอบ LAB เครือข่าย

#### 5. Activity Wizard คือ ผู้สอนหรือผู้ที่มีหน้าที่ในการสอนเกี่ยวกับระบบเครือข่ายสามารถสร้างสถานการณ์ในลักษณะเป็นขั้นๆ โดยผู้เรียนต้องทดสอบและแก้ปัญหาไปทีละขั้นๆ จนกว่าจะแก้ปัญหาได้ทั้งหมด ซึ่งโปรแกรมสามารถแสดงคะแนนที่ผู้เรียนแก้ปัญหานาในแต่ละขั้นตอนหรือทั้งหมดได้ โดยผู้สอนจะกำหนดค่าตอบไว้ก่อนร่วงหน้า



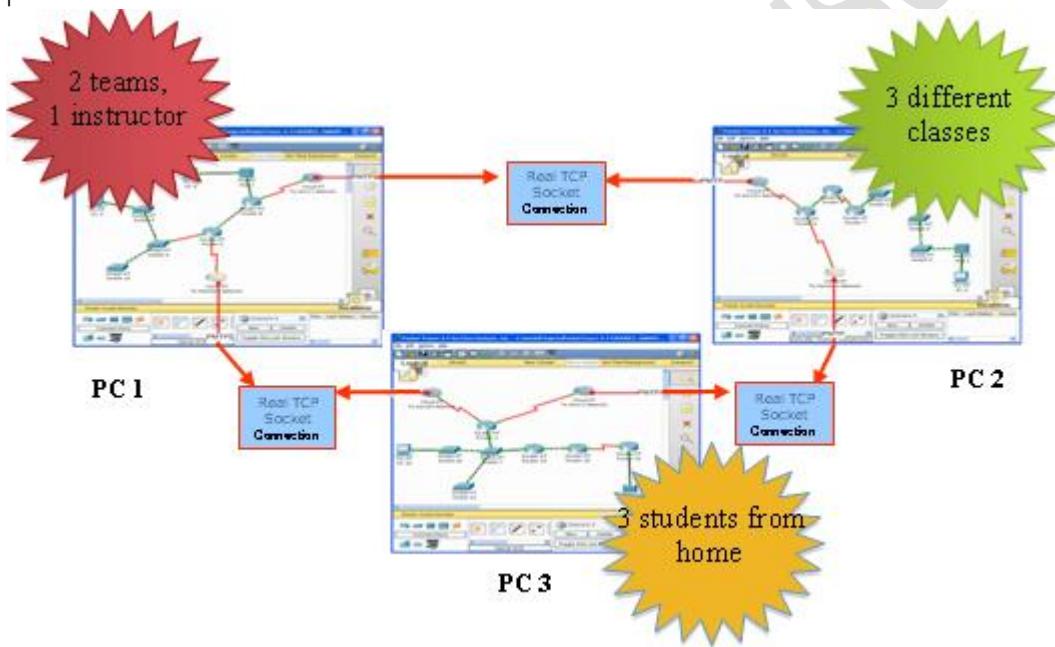
รูปที่ 1-5 แสดงการสร้าง LAB ด้วย Activity Wizard

6. Multiuser Functionality โปรแกรมมีความสามารถในการเข้ามาร่วมกับผู้เรียนรายอื่นๆ ซึ่งอยู่ที่ใดๆ ก็ได้ โดยผ่านพอร์ต TCP/IP ผ่านเครือข่ายอินเทอร์เน็ตได้เป็นอย่างดี ทำให้

ผู้เรียนสามารถสร้างกลุ่มเครือข่าย ทดสอบเครือข่ายขนาดใหญ่ ทดสอบการเชื่อมต่อที่ซับซ้อน สามารถแข่งขันกันระหว่างวิทยาในกลุ่มเครือข่ายได้

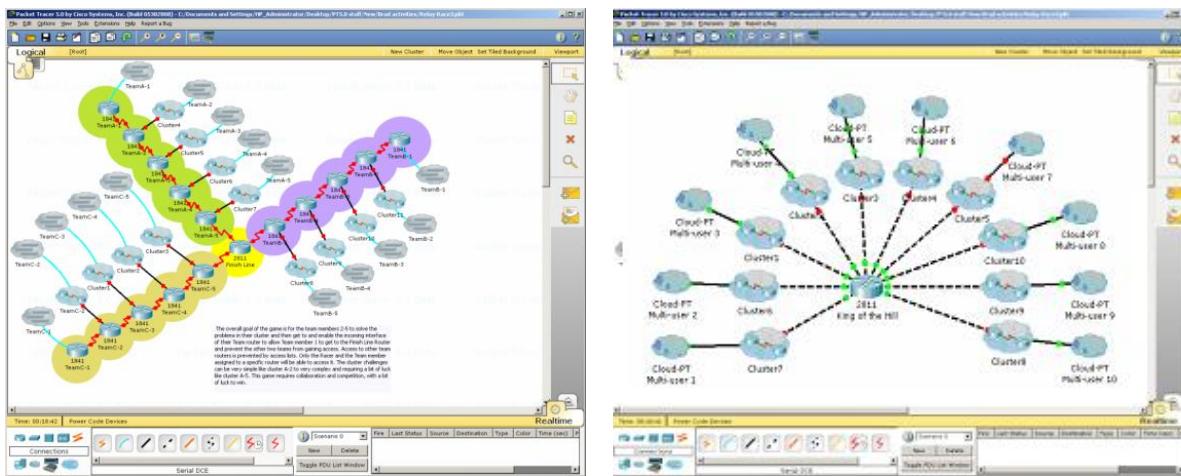


รูปที่ 1-6 แสดงการเชื่อมโยงเครือข่ายด้วย Packet tracer Multiuser Functionality จากตัวอย่างรูปที่ 1-7 สมมุติว่า มีการแข่งขันการออกแบบและเชื่อมต่อเครือข่ายระหว่าง 3 ทีม โดยแต่ละทีมอยู่ต่างสถานที่กัน เช่น ทีมที่หนึ่ง อยู่ที่มหาวิทยาลัย ทีมที่สองอยู่ที่ทำงาน และทีมที่สามอาจจะอยู่ที่บ้าน ผ่านโปรโตคอล Packet Tracer Messaging Protocol (PTMP) ใน packet tracer



รูปที่ 1-7 แสดงการเชื่อมโยงเครือข่ายระหว่าง 3 ทีมด้วยโปรโตคอล PTMP

7. Multiuser Games for Social Learning โปรแกรมมีคุณสมบัติในการเชื่อมโยงผู้ใช้ต่างๆ เข้าด้วยกัน จึงส่งผลให้ผู้เรียนและผู้สอนสามารถสร้างสรรค์เกมส์ ที่เกี่ยวข้องกับระบบเครือข่ายได้ ทำให้ผู้เรียนผ่อนคลายได้



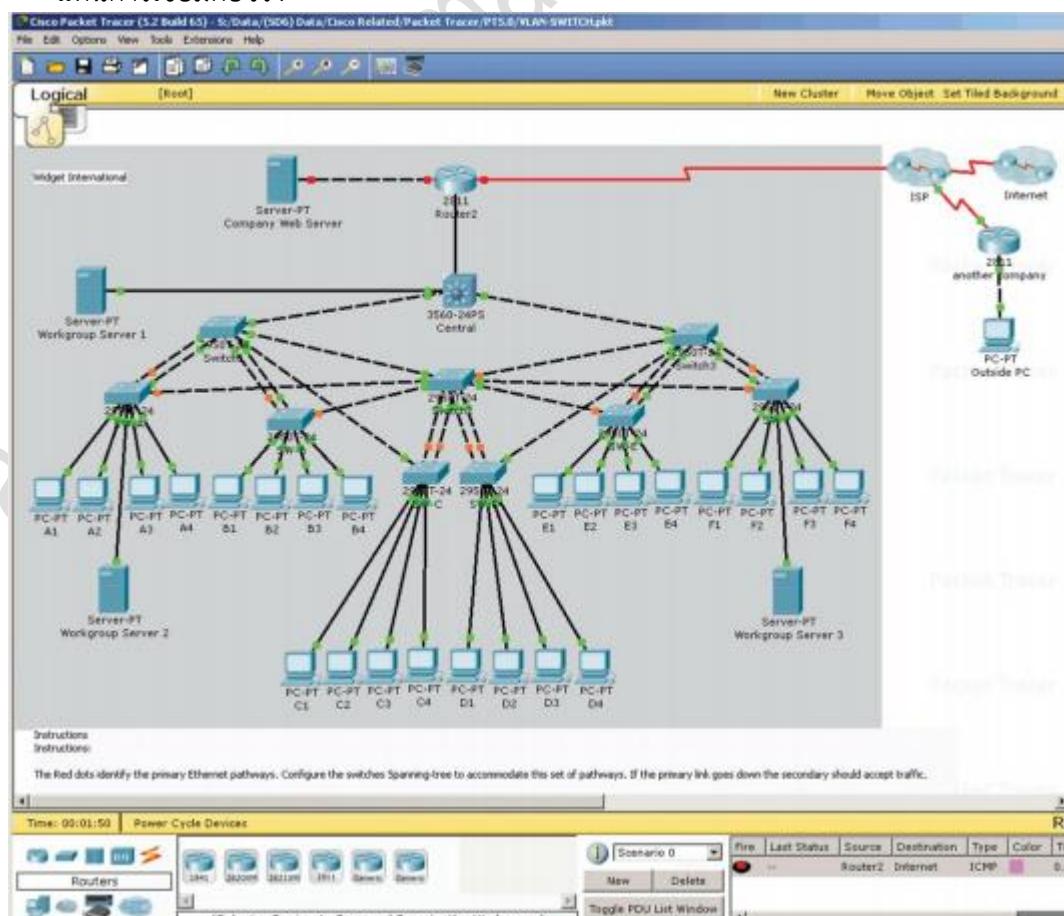
## เกมส์ Relay Race

## เกมส์ King of the Hill

รูปที่ 1-8 ตัวอย่างการสร้างสรรค์เกมส์ด้วย Packet Tracer

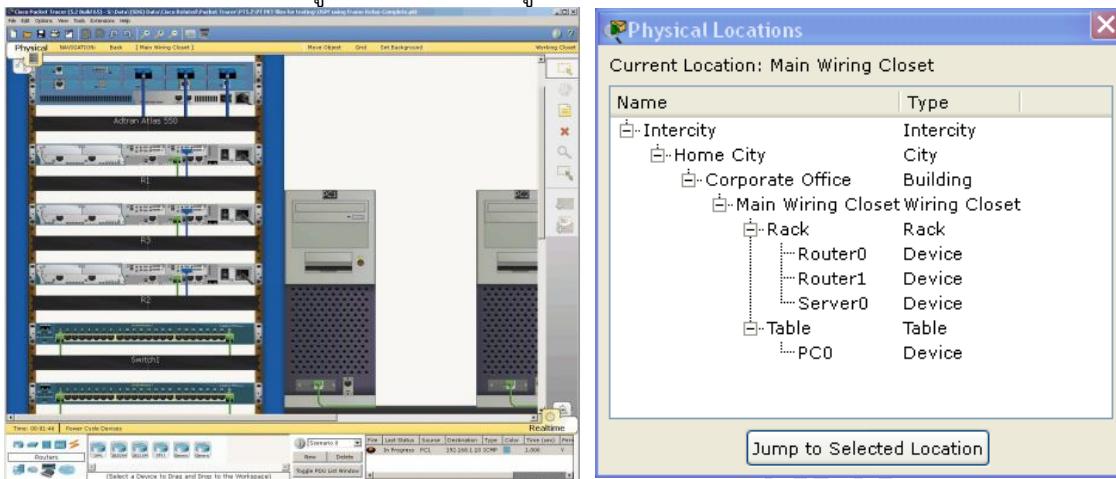
8. Logical and Physical Workspaces โปรแกรมออกแบบให้ผู้ใช้สามารถทำงานได้ 2 แบบคือ

- Logical Workspaces แสดงรูปการเชื่อมต่อเครือข่ายทางโลจิคอล แบบนี้ผู้ใช้สามารถสร้างรูปแบบการเชื่อมต่ออุปกรณ์ต่างๆ เช่น เครื่องคอมพิวเตอร์ เชิร์ฟเวอร์ สวิตช์ เรตเตอร์ สายนำสัญญาณ และอื่นๆ ในลักษณะที่เป็นรูปภาพสัญญาณลักษณ์ แทนการเชื่อมต่อจริง



รูปที่ 1-9 ตัวอย่างการเขียนต่อเน้น Logical

- Physical Workspaces แสดงรูปแบบการเชื่อมต่อทางกายภาพ โดยอ้างอิงกับตำแหน่งที่ตั้งของสถานที่ติดตั้งระบบเครือข่ายจริง เช่น สำนักงานที่ติดตั้ง สำนักงาน อาคาร ห้อง และ ตู้ Rack เป็นต้น ดังรูปที่ 1-10



ก. แสดงการเชื่อมต่ออุปกรณ์ภายในตู้ Rack

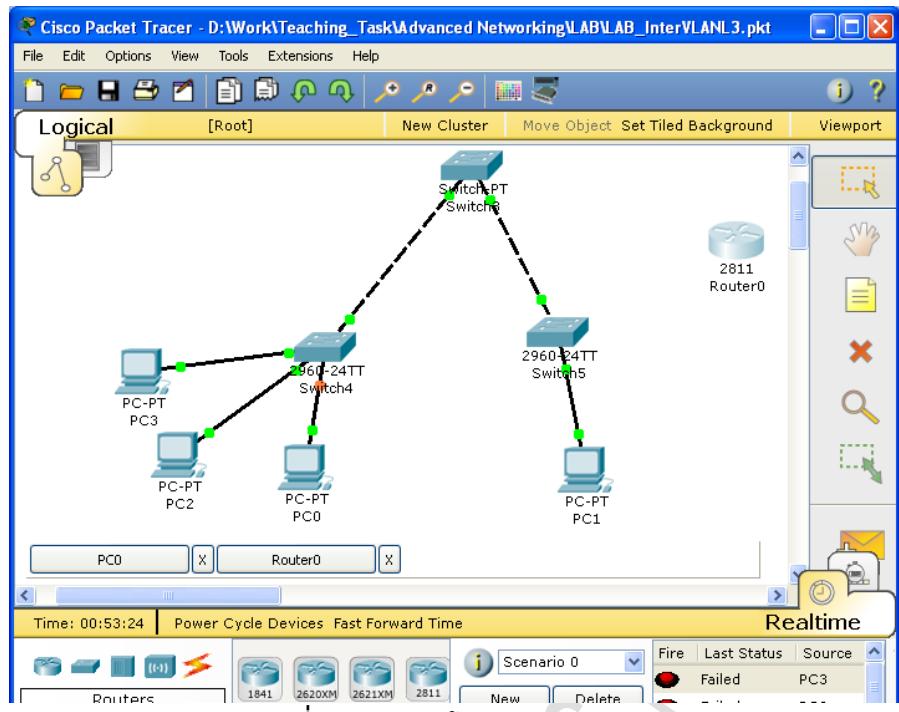
ข. แสดงการลำดับขั้นการเชื่อมต่อ

### รูปที่ 1-10 แสดงการเชื่อมต่อแบบ physical

จากรูปที่ 1-10 ก แสดงให้เห็นถึงรูปแบบการจัดวางอุปกรณ์เครือข่ายต่างๆ เช่น เซิร์ฟเวอร์ เร้าเตอร์ บน Rack cabinet และรูปที่ 1-10 ข แสดงลำดับที่ตั้งของอุปกรณ์ โดยเริ่มตั้งแต่เมือง หรือจังหวัด ต่อจากนั้นก็ค่อยๆ ขยับพื้นที่ให้เคลื่อนมาเรื่อยๆ เป็น อาคาร, ห้องเก็บอุปกรณ์, Rack, โต๊ะ, เร้าเตอร์ และอุปกรณ์เครือข่ายอื่นๆ ตามลำดับ

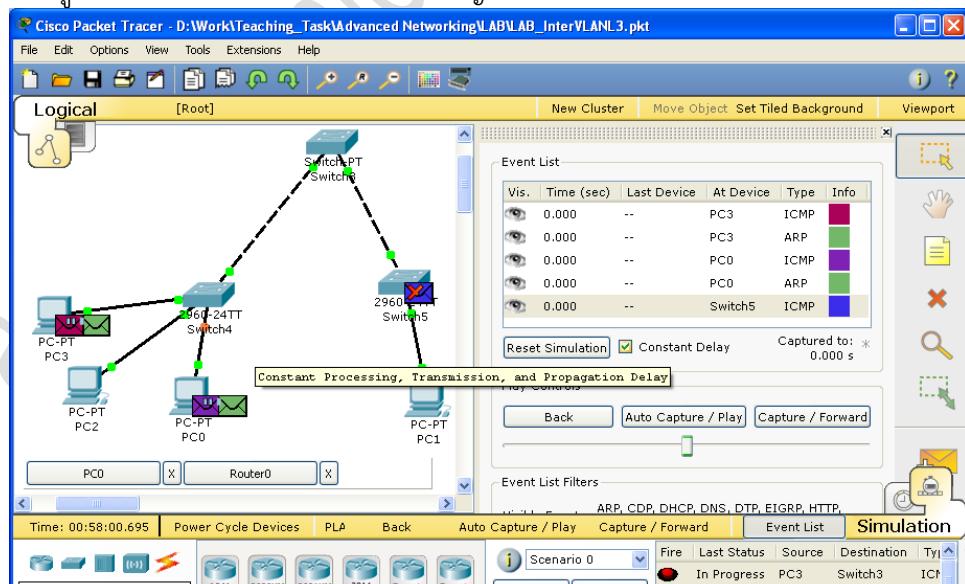
## 9. Real-Time and Simulation Modes โปรแกรมมีความสามารถแสดงผลการทำงานใน 2 รูปแบบคือ

- ใหม่ Real-Time ในโหมดนี้ผู้ใช้สามารถเลือกอุปกรณ์ต่างๆ ที่ต้องการ มาเชื่อมต่อกันในลักษณะรูปสัญญาณ หรือการวาดแผนผังเครือข่ายบนกระดาษ หรือ การใช้โปรแกรมประเภทเขียนผังเครือข่าย เช่น Visio, Smart draw เป็นต้น ซึ่งผู้ใช้ จะต้องเข้าใจเรื่องของสัญญาณของอุปกรณ์ต่างๆ ที่นำมาเชื่อมต่อกัน เช่น เร้าเตอร์ จะใช้สัญญาณทรงกลมแบบโดยมีลูกศรหัวเข้า 2 ทิศทางและหัวออก 2 ทิศทาง เป็นต้น ระหว่างการเชื่อมต่ออุปกรณ์ต่างๆ ลงบนโหมดนี้ อุปกรณ์จะแสดงสถานะการทำงานให้ผู้ใช้เห็นด้วย เช่น ไฟกระพริบสีเขียวแสดงการเชื่อมต่อสมบูรณ์ สีส้มแสดงกำลังเริ่มกระบวนการเชื่อมต่อ โปรแกรมจะแสดงชื่ออุปกรณ์ พอร์ตที่ทำการเชื่อมต่อ รวมถึงเสียงที่เกิดจากการเชื่อมต่อด้วย โหมด Real-Time นี้จะเป็นโหมดที่ผู้ใช้จะต้องเริ่มต้นวางแผนเครือข่ายก่อนเสมอ และใช้งานปอยที่สุดด้วย



รูปที่ 1-11 แสดงโหมด Real-Time

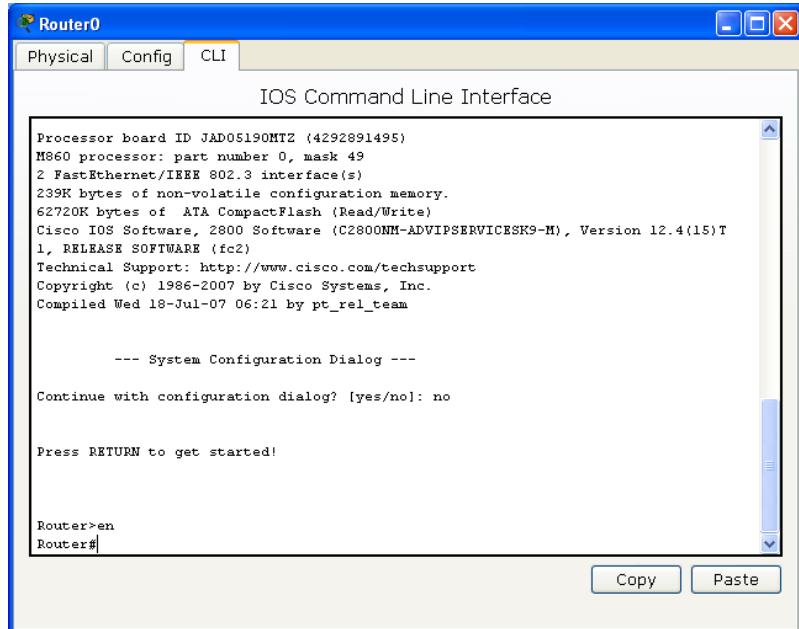
- โหมด Simulation ในโหมดนี้ผู้ใช้สามารถสร้างข้อมูล (packet) เข้าไปยังระบบเครือข่ายที่สร้างขึ้นแล้ว เพื่อเฝ้าดูและสังเกตุพฤติกรรมการทำงานของเครือข่ายที่ได้ออกแบบไว้ ซึ่งโปรแกรมจะแสดงผลการทำงานเป็นแบบอนิเมชัน สี เสียง ทำให้ผู้ใช้รู้สึกตื่นตัว ส่งผลให้เห็นภาพพิเศษทางการให้ของข้อมูลทั้งระบบ ซึ่งช่วยให้ผู้ออกแบบสามารถวิเคราะห์และแก้ปัญหาที่เกิดขึ้นได้อย่างรวดเร็ว



รูปที่ 1-12 แสดงโหมด Simulation

- User friendly Command Line Interface (CLI) โปรแกรมจัดเตรียมส่วนติดต่อ กับผู้ใช้งาน ผ่านทาง command line (คือการคีย์คำสั่งที่จะคำสั่งผ่านทาง console ในรูปแบบ text) สำหรับผู้เรียนที่ต้องการคีย์คำสั่งควบคุมเราเตอร์เหมือนกับเราเตอร์ของจริง และสำหรับผู้ใช้ที่ไม่คุ้นเคยในการคีย์คำสั่งแบบใช้ command line ก็สามารถคอนฟิกอุปกรณ์

ต่างๆ ได้เหมือนกันโดยผ่านทางกราฟพิกแทน แต่ก็จะมีข้อจำกัดและไม่คล่องตัวเมื่องานการใช้ CLI



รูปที่ 1-13 แสดงรูปแบบการสั่งงานด้วย command line (CLI)

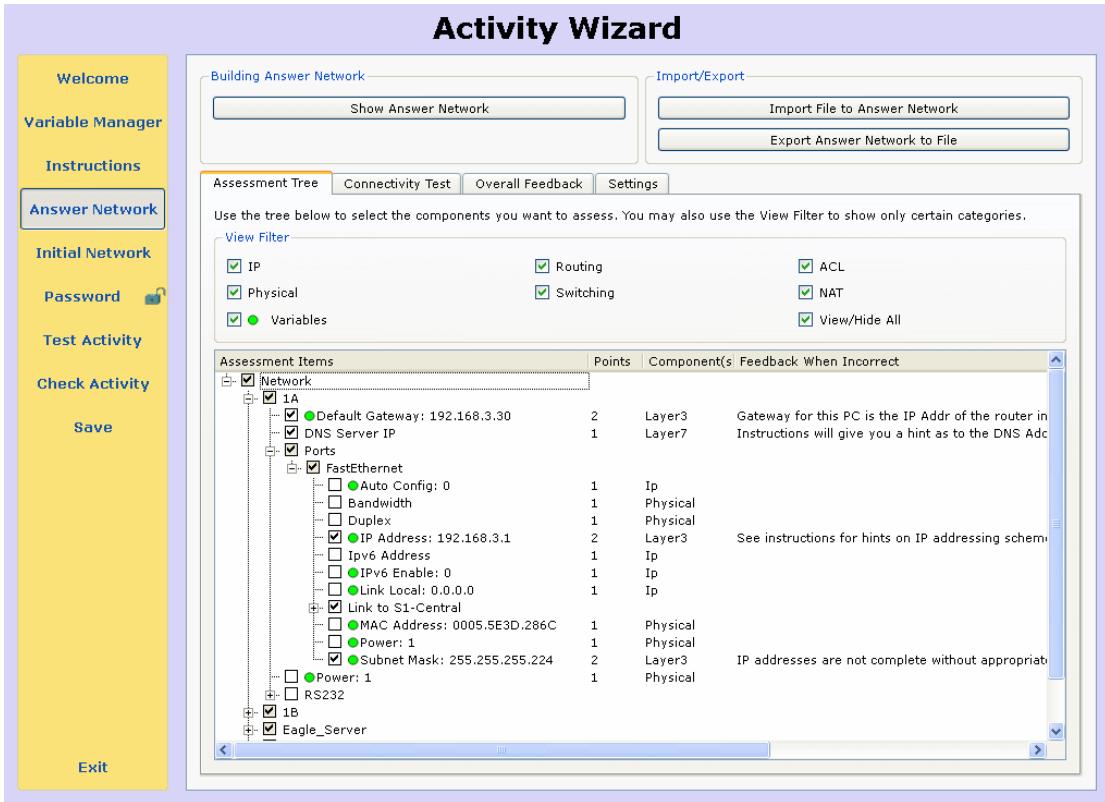
11. Global event list (packet sniffer) โปรแกรมสามารถรายงาน สถานะการเข้มต่อ ทิศทางการไหลของข้อมูล ชนิด เวลา จำนวน ของแพ็คเก็ตได้อย่างละเอียดผ่านทาง event list ทำให้ผู้เรียนเข้าใจการพัฒนาระบบการทำงานของแพ็คเก็ตได้เป็นอย่างดี

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit
●	In Progress	PC3	Switch3	ICMP	■■■■■	0.000	N	0	(edit)
●	In Progress	PC0	PC1	ICMP	■■■■■	0.000	N	1	(edit)
●	In Progress	Switch5	Switch3	ICMP	■■■■■	0.000	N	2	(edit)

รูปที่ 1-14 แสดงการทำงานของฟังก์ชัน event list(packet sniffer)

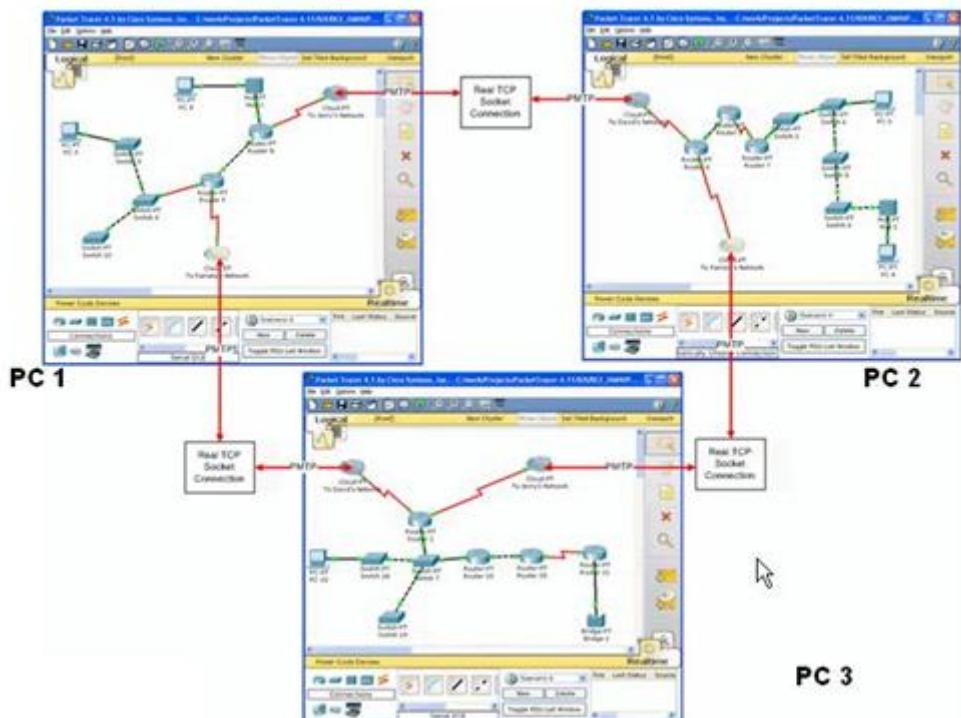
12. LAN, switching, TCP/IP, routing, and WAN protocols โปรแกรมรองรับการทำงานแบบเครือข่าย LAN, switching, โพรโทคอลทีซีพี-ไอพี, โพรโทคอลที่ทำหน้าที่ผลักดันให้โพรโทคอลอื่นๆ เดินทางไปบนเครือข่าย (routing protocol), และรองรับโพรโทคอลบางส่วนของการเชื่อมต่อระดับ WAN ด้วย ซึ่งรายละเอียดจะแสดงในหัวข้อ Packet Tracer ทำอะไรได้บ้าง

13. Activity Wizard, Lab grading โปรแกรมถูกออกแบบแบบขึ้นมาเพื่อใช้สำหรับการเรียนการสอน ด้านระบบเครือข่ายโดยเฉพาะ ดังนั้นจึงมีคุณสมบัติให้ผู้สอนสามารถสร้าง LAB ขึ้นมาใน ลักษณะ activity wizard คือ ผู้สอนจะเตรียม LAB ที่ถูกออกแบบไว้อย่างมีขั้นตอน โดย การกำหนดคำตอบที่ถูกต้องไว้ล่างหน้า) ผู้เรียนจะต้องปฎิบัติหรือแก้ปัญหาโจทย์ไปทีละขั้นๆ โดยไม่สามารถข้ามขั้นตอนได้ ทำให้ผู้สอนสามารถควบคุมแผนการสอน หรือสร้างบทเรียนที่ สอดคล้องให้กับผู้เรียนได้เป็นอย่างดี



รูปที่ 1-15 แสดงการสร้าง LAB ด้วย activity wizard

14. Multiuser functionality โปรแกรมจำลองเครือข่ายในสมัยก่อนมีข้อจำกัดประการที่สำคัญคือ จะจำลองเครือข่ายแบบ stand-alone ทำให้ผู้เรียนเห็นภาพการเชื่อมต่อเฉพาะที่ โดยมีโปรแกรมจำลองเครือข่ายเป็นตัวสร้างให้เท่านั้น ไม่สามารถทดสอบได้ว่า เครือข่ายที่ได้สร้างขึ้นจะสามารถทำงาน ในสถานการณ์จริงได้หรือไม่ แต่สำหรับ packet tracer ตั้งแต่เวอร์ชันที่ 5 เป็นต้นไป มีคุณสมบัติรองรับการเชื่อมตอกันระหว่างผู้เรียนแต่ละรายที่อยู่ต่างสถานที่ กันได้ โดยผ่านพอร์ต PTMP ซึ่งส่งผลให้ผู้เรียนแต่ละรายสามารถสร้างเครือข่ายเสมือน จริงซึ่งอนบนเครือข่ายอินเทอร์เน็ตอีกชั้นหนึ่ง ผู้เรียนแต่ละรายสามารถสร้างเครือข่ายภายใน หรือ local area network ของตนเองที่แตกต่างกันได้ และสามารถทดสอบเชื่อมต่อ เครือข่ายของตนเองที่สร้างขึ้นผ่านทางเครือข่าย WAN เข้าด้วยกัน



รูปที่ 1-16 แสดงการเชื่อมต่อระหว่างผู้ออกแบบเครือข่ายด้วยฟังก์ชัน multiuser

15. Multiple platform support โปรแกรม packet tracer มีความสามารถทำงานได้ทั้งหลายระบบปฏิบัติการ ปัจจุบันสามารถทำงานได้ทั้งวินโดวส์(2000, XP, Vista) และลินุกซ์ (Ubuntu, Fedora, Centos)
16. Multiple language support รองรับได้หลายภาษา
17. Integrated Help and Tutorials โปรแกรม packet tracer เวอร์ชัน 5.3.1 (ล่าสุด) ตัวเต็ม มีขนาดประมาณ 73.4 Mb จะรวมเอาโปรแกรมช่วยสอนที่อยู่ในรูปแบบของนิเมชันและคู่มือ การใช้งานไว้ด้วยในตัว ทำให้ผู้เรียนสามารถศึกษาได้ด้วยตนเอง
18. Supports Networking Academy Curricula โปรแกรม packet tracer นั้นถูกออกแบบมาเพื่อใช้สำหรับโครงการ Cisco Networking Academy ซึ่งทางบริษัทซิสโก้มีเนื้อหา ส่งเสริมให้สถาบันการศึกษาในประเทศต่างๆ ที่มีการเรียนการสอนด้านระบบเครือข่ายได้ใช้งาน และใช้สำหรับผู้ที่ต้องการสอบ certificate CCNA (หลักสูตร CCNA Discovery, CCNA Exploration, and CCNA Security) หรือ CCNP บางส่วน

#### Packet Tracer ทำอะไรได้บ้าง? (เวอร์ชัน 5.0 ขึ้นไป)

1. อุปกรณ์เราเตอร์ (Routers) รองรับอุปกรณ์เราเตอร์ตั้งแต่รุ่น 1841-2811 พร้อมกับ generic router ซึ่งผู้ใช้สามารถเพิ่มลดอุปกรณ์ได้ตามความต้องการ เช่น การ์ดเน็ตเวิร์คแบบต่าง (fiber, fast-ethernet, serial, Ethernet เป็นต้น)



2. อุปกรณ์สวิตช์ (Switches) รองรับอุปกรณ์สวิตช์ในระดับเลเยอร์ 2(2950-2960, generic switch สามารถเพิ่มลดอินเทอร์เฟสในการเชื่อมต่อได้เอง), เลเยอร์ 3 เตรียมไว้ให้ 1 ตัวคือ สวิตช์ 3560 ซึ่งมีคุณสมบัติในการทำ VLAN



3. ฮับ (Hubs) โปรแกรมสนับสนุนอุปกรณ์ชนิดฮับ รีพิทเตอร์ และสปริตเตอร์



4. ไวเลสแลน (wireless devices) สนับสนุนอุปกรณ์ไวเลสแลน access point ทั้งแบบมีเสา และไม่มีเสา



5. คอนเน็คชัน (connections) สนับสนุนสายนำสัญญาณที่ใช้สำหรับเชื่อมต่ออุปกรณ์เครือข่าย หลากหลายรูปแบบ เช่น สายแบบอัตโนมัติ (กรณีที่ผู้ใช้ตัดสินใจไม่ได้ว่าจะใช้สายชนิดใดใน การเชื่อมต่อ), สาย (console), สายตรง (copper straight-through) เป็นต้น



6. อุปกรณ์เชื่อมต่อปลายทาง (end devices) สนับสนุนอุปกรณ์เชื่อมต่อปลายทางหลาย ประเภท เช่น เครื่องคอมพิวเตอร์พีซี โน๊ตบุ๊ก เซิร์ฟเวอร์ ปรินเตอร์ VoIP โทรศัพท์ ทีวี ไวเลส เป็นต้น



7. โครงข่ายการเชื่อมต่อ WAN (WAN emulation) สนับสนุนโครงข่ายการเชื่อมต่อจำลองใน ระดับ WAN เช่น โครงข่ายแบบคลาวด์ (cloud) และ DSL เป็นต้น



8. ประกอบอุปกรณ์ใช้งานเอง (custom made devices) โปรแกรมสนับสนุนให้ผู้ใช้สามารถ เลือกและประกอบอุปกรณ์ได้ด้วยตนเองตามความต้องการ เช่น ต้องการเพิ่มการ์ดใหม่ให้กับ เราระบบ เพิ่มอุปกรณ์ไวเลสแลนให้เครื่องคอมพิวเตอร์พีซีเป็นต้น



9. เชื่อมโยงเครือข่ายระหว่างผู้ใช้เข้าด้วยกัน (multiuser connection) โปรแกรมมี ความสามารถในการเชื่อมต่อเครือข่ายระหว่างผู้ใช้ ผ่าน multiuser connection



10. สนับสนุนโพรโทคอล

Layer	Layer Cisco Packet Tracer Supported Protocols
Application	<ul style="list-style-type: none"> <li>FTP, SMTP, POP3, HTTP, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, ISR VOIP, SCCP config and calls ISR command support, Call Manager Express</li> </ul>
Transport	<ul style="list-style-type: none"> <li>TCP and UDP, TCP Nagle Algorithm &amp; IP Fragmentation, RTP</li> </ul>
Network	<ul style="list-style-type: none"> <li>BGP, IPv4, ICMP, ARP, IPv6, ICMPv6, IPSec, RIPV1/v2/ng, Multi-Area OSPF, EIGRP, Static Routing,</li> </ul>

	Route Redistribution, Multilayer Switching, L3 QoS, NAT, CBAL, Zone-based policy firewall and Intrusion Protection System on the ISR, GRE VPN, IPSec VPN
Network Access/Interface	<ul style="list-style-type: none"> <li>• Ethernet(802.3), 802.11, HDLC, Frame Relay, PPP, PPPoE, STP, RSTP, VTP, DTP, CDP, 802.1q, PAgP, L2 QoS, SLARP, Simple WEP, WPA, EAP</li> </ul>

### 11. คุณสมบัติเพิ่มขึ้นใหม่ในเวอร์ชันที่ 5.3 ดังต่อไปนี้

- รองรับหลักสูตร CCNA Discovery ซึ่งเป็นหลักสูตรที่เน้นการเชื่อมต่อเครือข่ายแบบ home networking และบริษัทขนาดเล็ก ซึ่งการเชื่อมต่อเครือข่ายไม่ซับซ้อน โดยเน้นรูปแบบการเชื่อมต่อดังต่อไปนี้
  - บริหารจัดการ อุปกรณ์ไวเลสแลน การจัดการไอพี และอุปกรณ์ปลายทาง
  - บริหารจัดการ ดีอี็นเอส (DNS) ดีอีซีพี (DHCP) ความปลอดภัยเครือข่ายไวเลสแลน เอฟทีพี (FTP) เอสเอ็มทีพี (SMTP) และป๊อบทรี (POP3)
  - บริหารจัดการโพรโทคอล OSPF แบบ multi-area, EIGRP และ BGP
  - บริหารจัดการ ISR VoIP, Call Manager Express
- รองรับหลักสูตร CCNA Exploration ซึ่งเป็นหลักสูตรที่เน้นการเชื่อมต่อเครือข่ายแบบเจาะลึกมากกว่าแบบ Discovery โดยเน้นหัวข้อดังต่อไปนี้
  - HTTP, DNS, DHCP, new FTP, SMTP, POP3
  - multiarea OSPF, EIGRP, new BGP
  - Linksys models, wireless security, 802.11
  - New PPPoE, enhanced IPsec, Cable and DSL enhancements
- รองรับหลักสูตร CCNP
  - multiarea OSPF, EIGRP, new BGP

### 12. คำถามที่น่าสนใจ

- a. Packet tracer คืออะไร? ตอบ packet tracer คือโปรแกรมที่ใช้สำหรับช่วยเหลือให้ผู้เรียนด้านระบบเครือข่าย สามารถมองเห็นภาพการทำงานของระบบเครือข่ายในรูปแบบ simulation และ visualization รวมถึงมีความสามารถในการสร้างบนเรียน การเชื่อมโยงเครือข่ายระหว่างไซต์ การแก้ปัญหาเป็นทีม เป็นต้น
- b. ใครใช้ Packet tracer ได้บ้าง? ตอบ Packet tracer สามารถใช้งานได้ฟรี สำหรับอาจารย์และนิสิตที่เรียนในหลักสูตร Cisco Networking Academy ซึ่งจะได้รับ account ให้สามารถดาวน์โหลดไปใช้งานได้ resource ทั้งหมดที่ cisco จัดเตรียมไว้ให้สำหรับหลักสูตรดังกล่าว
- c. เมื่อติดตั้ง packet tracer เวอร์ชันเดิมอยู่แล้วจำเป็นต้องเปลี่ยนหรือ upgrade เป็นเวอร์ชันใหม่หรือไม่? ตอบ แนะนำว่าควรใช้เวอร์ชันที่ใหม่กว่า
- d. สามารถใช้ activity ที่สร้างจากเวอร์ชันเก่า มาใช้กับเวอร์ชันใหม่ได้หรือไม่? ได้ เวอร์ชันใหม่สามารถรองรับ activity ที่สร้างจากเวอร์ชันเดิมได้ทั้งหมด

- e. สามารถใช้ activity ที่สร้างจากเวอร์ชันใหม่ ไปทำงานกับเวอร์ชันที่ต่ำกว่าได้หรือไม่? ตอบ ไม่ได้
- f. ผู้สอนหรือผู้เรียนนำเสนอ packet tracer ไปติดตั้งใช้งานที่เครื่องส่วนตัวได้ไหม? ตอบ ได้ เนื่องจากหลักสูตรดังกล่าวต้องการให้ผู้เรียนผู้สอนมีความเป็นอิสระในการใช้งาน ดังนั้นจึงอนุญาตให้นำไปติดตั้งในเครื่องของตนเองเพื่อทำ LAB หรือปฏิบัติได้
- g. โปรแกรม packet tracer ติดตั้งบนระบบปฏิบัติการอะไรบ้าง? ตอบ ติดตั้งได้ทั้ง Windows และลินุกซ์ เช่น Windows (Windows XP, Windows 2000, Vista Home Basic, and Vista Home Premium) and Linux (Ubuntu 7.10 and Fedora 7)
- h. เครื่องที่ต้องการติดตั้ง packet tracer จะต้องมีคุณสมบัติอย่างไร? ตอบ ในการติดตั้ง packet tracer เวอร์ชัน 5 ขึ้นไป เครื่องคอมพิวเตอร์ควรจะมีคุณสมบัติดังนี้คือ
- CPU: Intel Pentium 300 MHz or equivalent
  - OS: Microsoft Windows 2000, Windows XP, Vista Home Basic, Vista Home Premium, Fedora 7, or Ubuntu 7.10
  - RAM: 96 MB
  - Storage: 250 MB of free disk space
  - Screen resolution: 800 x 600 or higher
  - Macromedia Flash Player 6.0 or higher
  - Language fonts supporting Unicode encoding (if viewing in languages other than English)
  - Latest video card drivers and operating system updates
- i. Packet Tracer รองรับโพรโทคอล IGRP หรือไม่? ตอบ ใช่ゴài โพรโทคอล EIGRP แทน IGRP ดังนั้นใน packet tracer จึงไม่มี
- j. ผู้ใช้ที่ไม่ได้เรียนหลักสูตร Cisco Networking Academy จะใช้โปรแกรมหรือดาวน์โหลดโปรแกรม packet tracer ได้หรือไม่? ตอบ เมื่อพูดตามความหมายในลิขสิทธิ์แล้วตอบว่าไม่ได้ ต้องใช้เฉพาะผู้ที่เรียนในหลักสูตร หรือ alumni เท่านั้น แต่ถ้าผู้ที่สนใจและเห็นว่าโปรแกรมดังกล่าวมีประโยชน์ เป็นต้นอาจจะดาวน์โหลดได้จากเว็บทั่วไป (Google) เมื่อเห็นว่าโปรแกรมดังกล่าวมีความเหมาะสมที่จะใช้ในสถานศึกษาของตนก็ควรจะสมัครเป็นสมาชิกกับ Cisco Networking Academy เพื่อรับสิทธิประโยชน์อย่างอื่นมากมาย (สำหรับประเทศไทยสามารถอ่านข้อมูลเพิ่มเติมได้จาก <http://www.cisco.com/web/TH/index.html>)

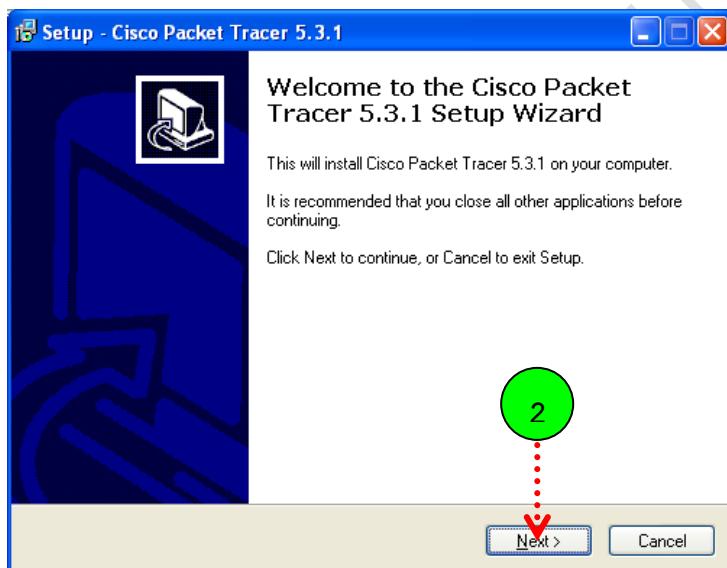
## บทที่ 2

### โปรแกรมจำลองเครือข่าย Packet Tracer

ในบทนี้จะอธิบายถึงการใช้งานโปรแกรม Packet Tracer เวอร์ชัน 5.3.1 ซึ่งเป็นเวอร์ชันที่ใหม่ล่าสุด (เดือนกันยายน 2010)

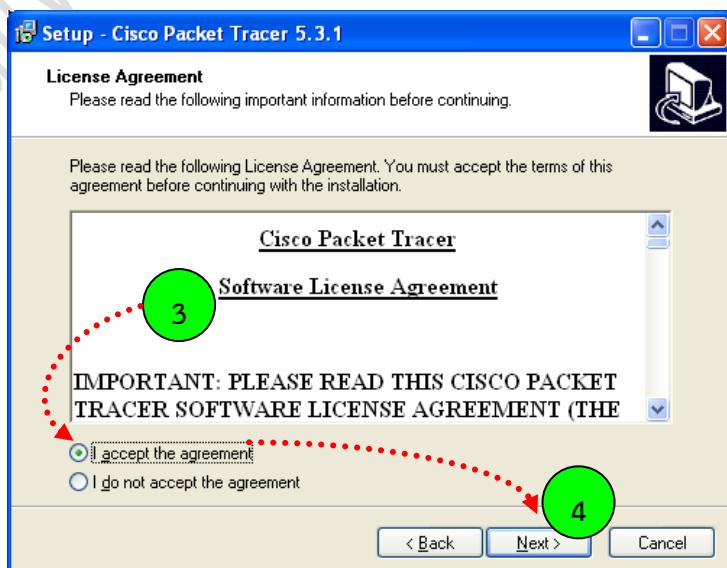
#### 1. ติดตั้งโปรแกรม Packet Tracer 5.3.x

- ขั้นตอนที่ 1 ดับเบิลคลิกไฟล์ PacketTracer531.exe
- ขั้นตอนที่ 2 โปรแกรมจะแสดงหน้าต่าง Welcome to the Cisco Packet Tracer 5.3.1 ให้คลิก Next>



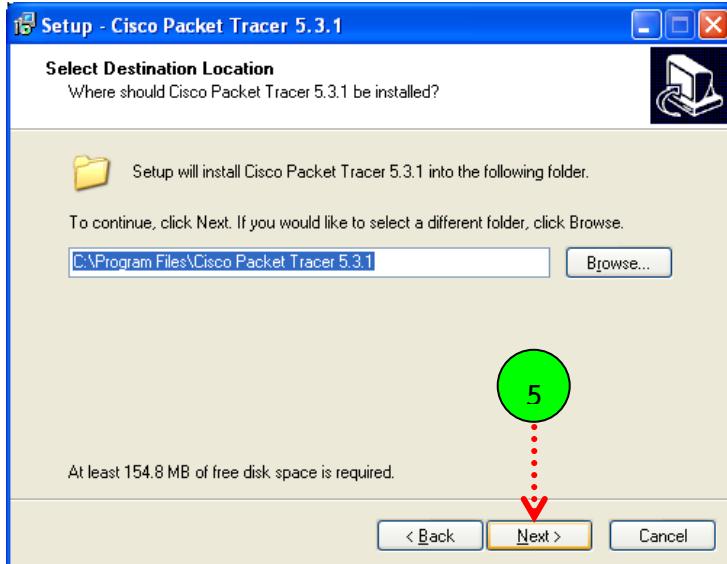
รูปที่ 2-1 แสดงขั้นตอนเริ่มต้นการติดตั้ง packet tracer

- ขั้นตอนที่ 3, 4 โปรแกรมแสดง license agreement ให้เลือก I accept a agreement ให้คลิก Next>



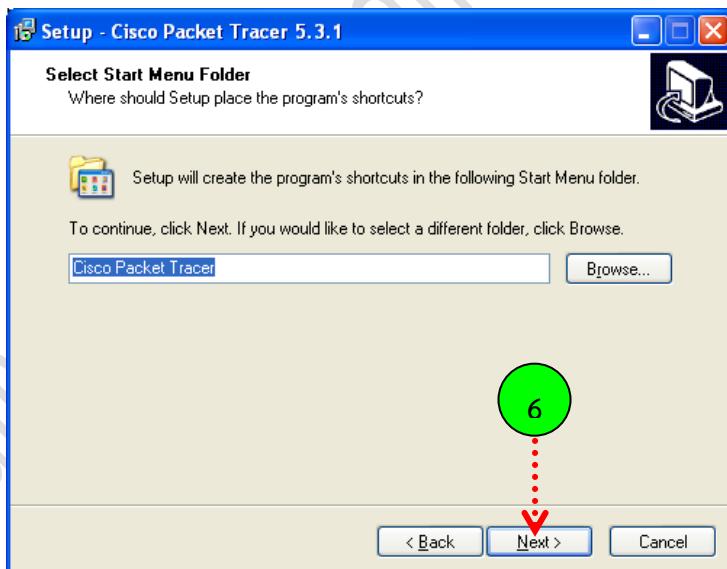
รูปที่ 2-2 แสดงลิขสิทธิ์โปรแกรม packet tracer

- ขั้นตอนที่ 5 โปรแกรมให้เลือกตำแหน่งที่ต้องการติดตั้งบนเครื่องคอมพิวเตอร์ ค่า default จะติดตั้งไว้ใน C:\Program Files ให้เลือก Next>



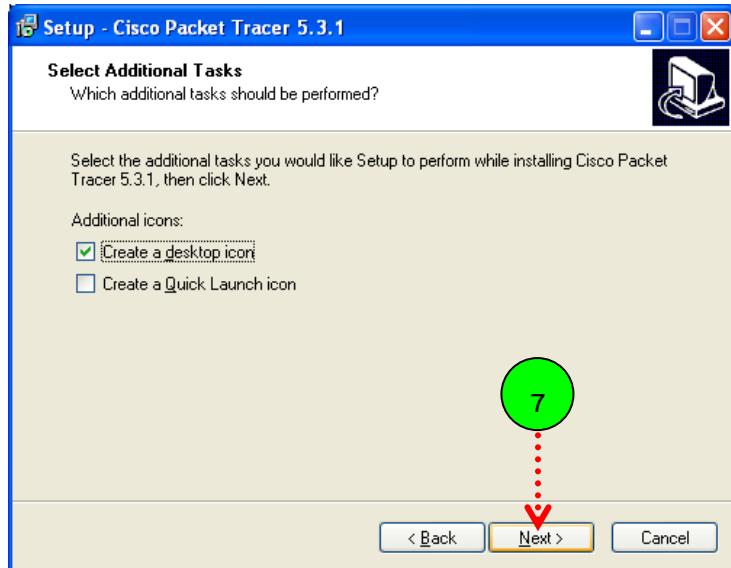
รูปที่ 2-3 เลือกตำแหน่งที่ต้องการติดตั้งโปรแกรม

- ขั้นตอนที่ 6 โปรแกรมถามว่าต้องการใช้ชื่อเมนูชื่อ Cisco Packet Tracer หรือไม่ ให้เลือก Next>



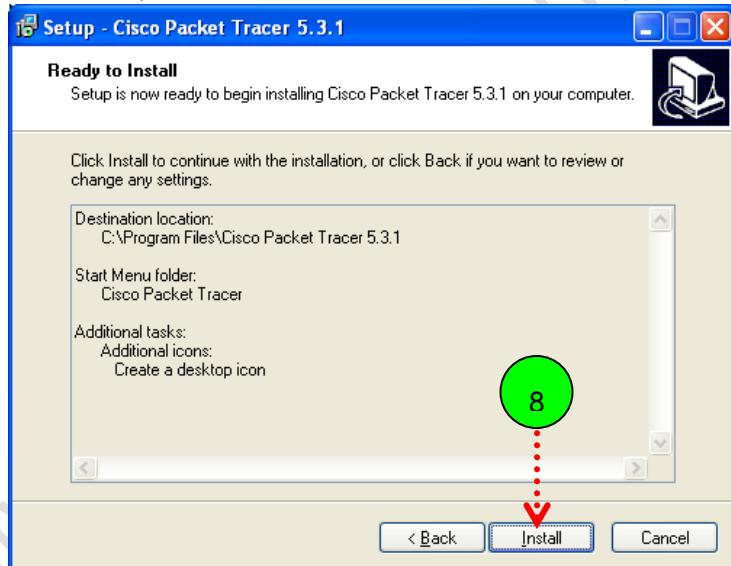
รูปที่ 2-4 เลือกชื่อเมนู

- ขั้นตอนที่ 7 select additional tasks เลือก Next>



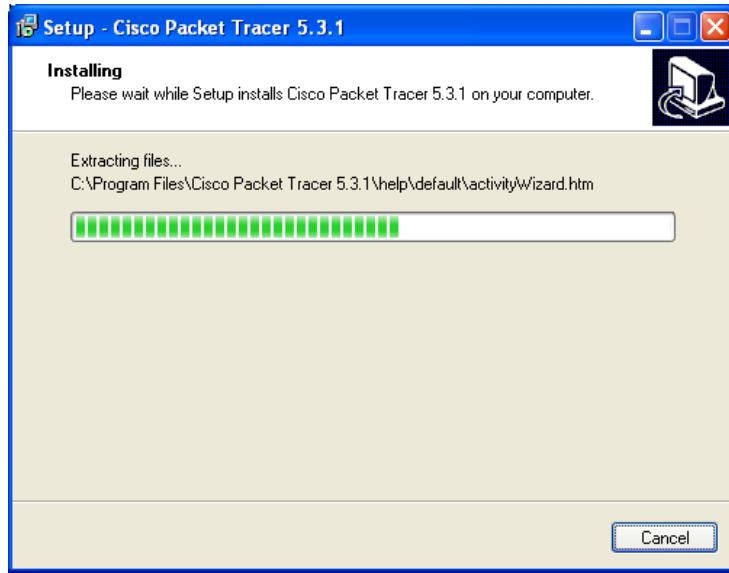
รูปที่ 2-5 สร้าง shortcut

- ขั้นตอนที่ 8 Ready to install เลือก Next>

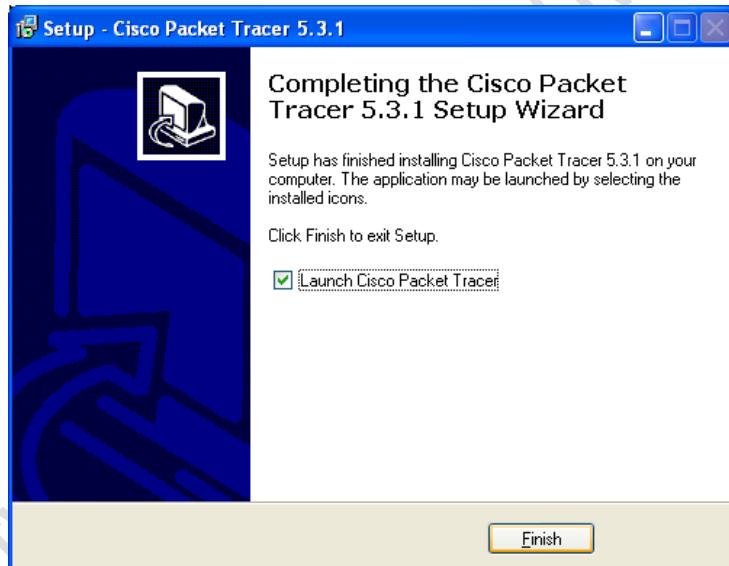


รูปที่ 2-6 เริ่มต้นการติดตั้งโปรแกรม

- ขั้นตอนที่ 9 โปรแกรมเริ่มทำการติดตั้ง โปรดรอสักครู่ เมื่อติดตั้งเสร็จ ให้เลือก Finish



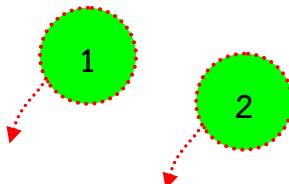
รูปที่ 2-7 ดำเนินการติดตั้งโปรแกรม packet tracer

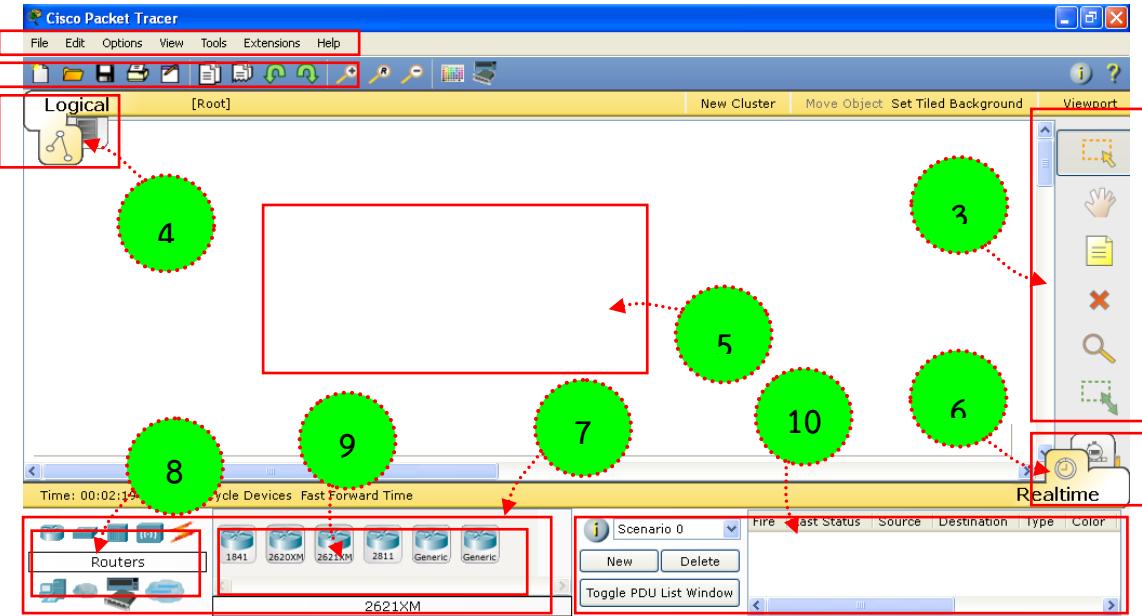


รูปที่ 2-8 ติดตั้งโปรแกรมเสร็จเรียบร้อย

## 2. เริ่มต้นการใช้งาน Packet Tracer

เมื่อผู้ใช้ทำการติดตั้งโปรแกรม packet tracer แล้ว ต้องการเรียกใช้งานโปรแกรม ให้เลือก Start ⇒ Programs ⇒ Cisco Packet Tracer ⇒ Cisco Packet Tracer





รูปที่ 2-9 โปรแกรม packet tracer 5.3.1  
ส่วนประกอบหลักของโปรแกรม Packet tracer 5.3.1 มี 10 ส่วนดังนี้

1. Menu Bar
2. Main Tool Bar
3. Common Tools Bar
4. Logical/Physical Workspace and Navigation Bar
5. Workspace
6. Realtime/Simulation Bar
7. Network Component Box
8. Device-Type Selection Box
9. Device-Specific Selection Box
10. User Created Packet Window

- Menu Bar เป็นเมนูหลักของโปรแกรมประกอบไปด้วยเมนูย่อยๆ ดังนี้



1. เมนู File ใช้สำหรับสร้างผังเครือข่าย (logical network) ใหม่, แก้ไขผังเครือข่ายที่เคยสร้างมาแล้ว, เปิดไฟล์ผังเครือข่ายที่เคยสร้างไว้แล้วมาทำงาน, บันทึกผังเครือข่าย (นามสกุลเป็น .pkt), พิมพ์ผังเครือข่าย เป็นต้น
2. เมนู Edit ใช้สำหรับ แก้ไขผังเครือข่าย เช่น ก็อปปี้, วางอุปกรณ์, ยกเลิกคำสั่งเดิม เป็นต้น
3. เมนู Options ใช้สำหรับกำหนดคุณสมบัติของโปรแกรม ประกอบไปด้วย

- Preferences ใช้สำหรับกำหนดการแสดงผลของโปรแกรม ประกอบไปด้วย แท็บ Interface, Administrator, hide และ font ตามลำดับ

คุณสมบัติในแท็บ Interface	
Show animation	แสดงภาพเคลื่อนไหวขณะทำงาน
Play sound	มีเสียงขณะมีการคลิกเลือกอุปกรณ์ต่างๆ
Show link lights	แสดงไฟกระพริบขณะที่อุปกรณ์กำลังเชื่อมต่อ
Show device labels	แสดงชื่อของอุปกรณ์ในผัง logical
Show port labels when mouse over	แสดงชื่อพอร์ตเมื่อเคลื่อนมาสู่ไปกล้อง
Show QoS stamps on packets	แสดงข้อมูลที่ถูก stamps เมื่อข้อมูลนั้นถูกทำ QoS
Enable cable length effects	เปิดใช้งาน cable length effects
Enable auto cable	เปิดใช้งาน auto cable
Show device dialog taskbar	แสดงชื่ออุปกรณ์ใน taskbar

ตารางที่ 2-1 แสดงคุณสมบัติในแท็บ Interface

คุณสมบัติในแท็บ Administrator	
Choose password	ตั้งรหัสผ่านค่าคอนฟิกที่ทำการปรับแต่งไว้ (ไม่ให้บุคคลอื่นมาแก้ไขค่าคอนฟิกในโปรแกรมในภายหลังได้)
Interface locking	เปิด/ปิดการใช้งานเมนูต่างๆ เช่น เมื่อคลิกเลือกที่ multiuser menu เมนูดังกล่าวจะไม่สามารถใช้งานได้
Write option to PT	อนุญาตให้ผู้ใช้งานสามารถเขียนลงใน folder ที่ติดตั้งโปรแกรม packet tracer ได้

ตารางที่ 2-2 แสดงคุณสมบัติในแท็บ Administrator

คุณสมบัติในแท็บ Hide	
Customize user experience	ซ่อนเมนู เมื่อผู้สอนไม่ต้องการให้ผู้เรียนใช้งาน เช่น ซ่อนแท็บ physical, CLI, Desktop เป็นต้น

ตารางที่ 2-3 แสดงคุณสมบัติในแท็บ Hide

คุณสมบัติในแท็บ Font	
Dialogs	ปรับแต่งตัวอักษร ขนาด การแสดงผลของฟอนต์ใน CLI และ headers
Workspace/activity wizard	ปรับแต่งตัวอักษร ขนาด การแสดงผลของฟอนต์ใน Workspace/activity wizard
General interface	ปรับแต่งตัวอักษร ขนาด การแสดงผลของฟอนต์ใน เมนู

	ต่างๆ เช่น File, tooltips เป็นต้น
Colors	ปรับแต่งสีการแสดงผลในการคอนฟิกอุปกรณ์ เช่น สีของตัวอักษรขณะคอนฟิก สีพื้นหลัง เป็นต้น

ตารางที่ 2-4 แสดงคุณสมบัติในแท็บ Font

- Uses profile เป็นการกำหนดข้อมูลผู้ออกแบบและคอนฟิกเครือข่ายว่าคือใคร

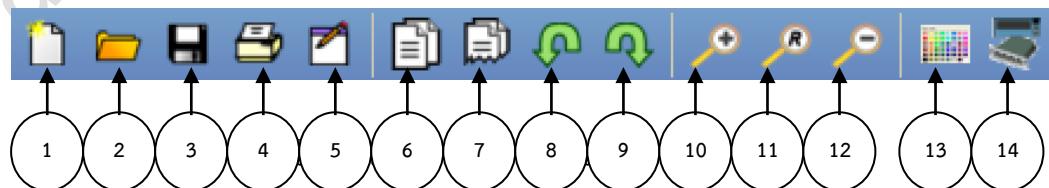
- Algorithm settings เป็นการกำหนดคุณสมบัติในการเชื่อมต่อระหว่างผู้ใช้งานต่างไซต์ เช่น กำหนดจำนวน connections, sessions เป็นต้น

4. เมนู view กำหนดการซูมภาพ ให้มีขนาด เล็ก หรือ ใหญ่ตามที่ผู้เรียนต้องการ และกำหนดการแสดงผลของแท็บ toolbar
5. เมนู tools ใช้สำหรับปรับแต่งสี ของปุ่ม หรือสีเส้น ที่เชื่อมต่อ
6. เมนู extensions เป็นเมนูที่ใช้กำหนดคุณลักษณะพิเศษของโปรแกรมดังต่อไปนี้

- Activity wizard ใช้สำหรับสร้างบทเรียนแบบ step by step (จะกล่าวอย่างละเอียดในหัวข้อ activity wizard)
- Multiuser กำหนดคุณลักษณะการเชื่อมต่อระหว่างผู้ใช้งานหลายคน (อ่านเพิ่มในหัวข้อ multiuser)
- IPC ใช้สำหรับอำนวยความสะดวกให้ผู้ใช้งานที่ต้องการสร้างโปรแกรมขึ้นเอง โดยทำงานร่วมกับ packet tracer ผ่านทางโพรโทคอล IPC(Inter-Process Communication)

7. เมนู help สำหรับช่วยเหลือผู้ใช้งาน ในการใช้งานโปรแกรม packet tracer ซึ่งมีทั้งแบบมัลติมีเดีย และแบบ text

- Main Tool Bar จัดเตรียมเครื่องมือที่ใช้งานบ่อยๆ ไว้ให้กับผู้ใช้งาน ประกอบไปด้วย



Main Tool Bar		
1. New	สร้างผังเครือข่ายใหม่	
2. Open	เลือกผังเครือข่ายเดิมที่สร้างไว้ขึ้นมาทำงานต่อ	
3. Save	บันทึกผังเครือข่ายที่สร้างขึ้น	
4. Print	สั่งพิมพ์ผังเครือข่าย	

5. Activity Wizard	สร้างบทเรียนแบบ step by step
6. Copy	คัดลอกอุปกรณ์
7. Paste	วางอุปกรณ์ที่คัดลอกลงบนผังเครือข่าย
8. Undo	ยกเลิกคำสั่งที่ทำงานหลังสุด
9. Redo	ทำคำสั่งหลังสุดอีกครั้ง
10. Zoom In	ขยายผังเครือข่าย
11. Zoom Reset	คืนสภาพของผังเครือข่ายให้มีขนาดเป็นค่า default
12. Zoom Out	ย่อผังเครือข่าย
13. Drawing Palette	ปรับแต่งสี ของปุ่ม หรือสีเส้น ที่เชื่อมต่อ
14. Custom Devices Dialog	เพิ่มลด template ใหม่

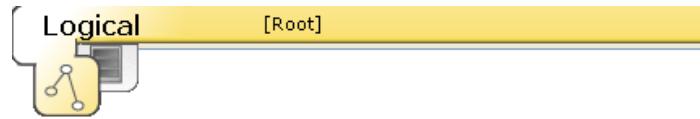
ตารางที่ 2-5 แสดง Main Tool Bar

- Common Tools Bar จัดเตรียมเครื่องมือที่ใช้งานบ่อยๆ กับพื้นที่ตรงกลาง workspace ซึ่งเป็นพื้นที่ที่ใช้เขียนผัง

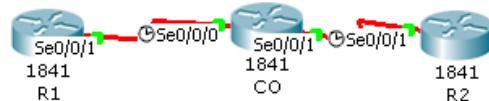
Common Tools Bar	
	เลือกอุปกรณ์
	เคลื่อนย้ายผังเครือข่าย
	บันทึกย่อ หรือ note บนผังเครือข่าย
	ลบอุปกรณ์ที่เลือก
	ตรวจสอบคุณสมบัติของอุปกรณ์ เช่น MAC table, ARP table เป็นต้น
	ลดและเพิ่มขนาดของอุปกรณ์
	ทดสอบการทำงานของเครือข่ายโดยเพิ่ม packet เข้าไปทดสอบ เช่น ping
	เพิ่ม packet เข้าไปทดสอบที่ชั้บชั้นชั้น

ตารางที่ 2-6 แสดง Common Tools Bar

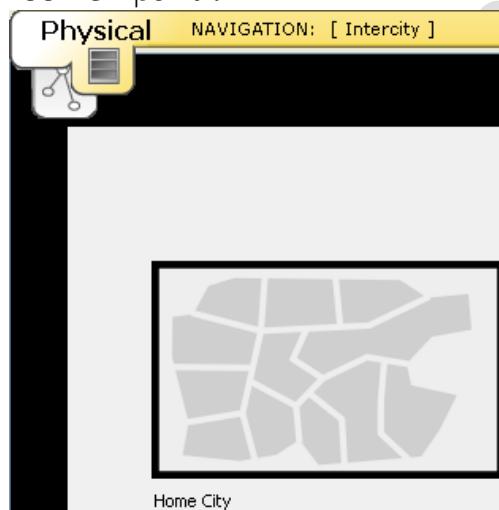
- Logical/Physical Workspace and Navigation Bar จัดเตรียมพื้นที่ใช้งานสำหรับสร้างผังเครือข่าย 2 แบบคือ logical(แสดงการเชื่อมต่อโดยใช้สัญรูปสัญลักษณ์) และ physical(แสดงการเชื่อมต่อทางกายภาพ เช่น สถานที่ติดตั้ง, Rack Cabinet เป็นต้น)



R1 and R2 are configured with GRE tunnels to CO. EIGRP is enabled on all three devices using AS number 60. Once the network converges, examine the routing tables and EIGRP neighbor tables. Because EIGRP is enabled on the 192.168.0.0/16 network adjacencies form over the Tunnel links that are established, but not over the directly connected networks.



รูปที่ 2-10 แสดงการเชื่อมต่อเครือข่ายบน logical workspace  
ในพื้นที่ logical workspace ผู้ใช้สามารถจัดกลุ่มอุปกรณ์ (cluster), กำหนดภาพพื้นหลัง, แสดงเครือข่ายแบบ view point ได้



รูปที่ 2-11 แสดงการเชื่อมต่อเครือข่ายบน Physical workspace

Physical workspace สามารถแสดงแผนที่ตั้งในลักษณะแบบ navigation คือ เริ่มจากพื้นที่ขนาดใหญ่ เช่น เมือง  $\Rightarrow$  อำเภอ  $\Rightarrow$  ตำบล  $\Rightarrow$  ตึ๊ก  $\Rightarrow$  ห้องเครือข่าย  $\Rightarrow$  ตู้ Rack หรือ ย้อนกลับจาก ตู้ Rack ไปถึง เมืองที่ได้เข่นกัน

- Workspace เป็นพื้นที่ที่ตรงส่วนกลางโปรแกรมที่ใช้สำหรับสร้างผังเครือข่าย
- Realtime/Simulation Bar ผู้ใช้สามารถเลือกโหมดในการทำงานได้ 2 แบบคือ โหมด Realtime แสดงการเชื่อมต่อแบบปกติ อุปกรณ์ทุกตัวจะแสดงสถานะการทำงานโดยมีลักษณะแบบทันทีทันใด เช่น มีการกระพริบ เป็นต้น โหมด Simulation แสดงทิศทางการไหลของข้อมูล ชนิดของแพ็คเก็ต ในรูปแบบอนิเมชัน



โหมด Realtime



โหมด Simulation

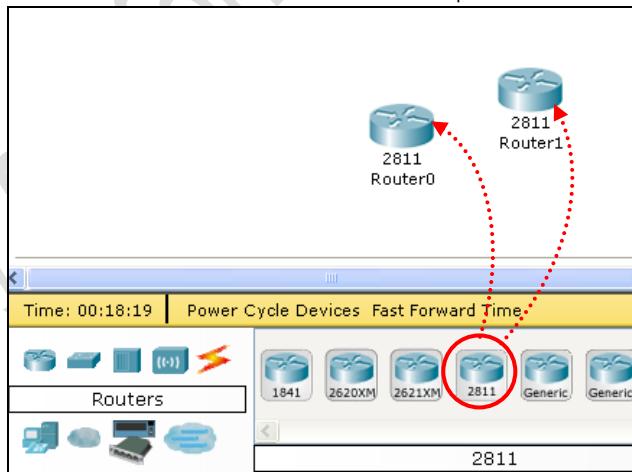
รูปที่ 2-12 แสดงการเลือกโหมด Realtime/Simulation

- Network Component Box จัดเตรียมอุปกรณ์ทั้งหมด รวมไว้ให้ผู้ใช้นำไปเชื่อมต่อ เป็นโครงสร้างเครือข่าย เช่น เร้าเตอร์ สวิตช์ สายนำสัญญาณ เป็นต้น
- Device-Type Selection Box แสดงกลุ่มของอุปกรณ์ เช่น กลุ่มอุปกรณ์เร้าเตอร์ สวิตช์ สายนำสัญญาณ ยัง ໄວเลสแลน เป็นต้น
- Device-Specific Selection Box แสดงรายการของอุปกรณ์ในแต่ละกลุ่ม ซึ่ง สอดคล้องกับ Device-Type เช่น เมื่อผู้ใช้เลือก Device-Type เป็น เร้าเตอร์ ใน Device-Specific จะปรากฏรายการการรุ่นต่างๆ ของเร้าเตอร์ ขึ้นมาให้ผู้ใช้เลือกใช้งาน
- User Created Packet Window เมื่อผู้ใช้ต้องการทดสอบเครือข่าย โปรแกรม packet tracer เตรียมเครื่องมือในการอำนวยความสะดวกให้คือ add PDU (สร้าง packet โดยผู้ใช้อิจ) เข้าไปในระบบเครือข่ายที่สร้างไว้ ผู้ใช้สามารถดู ข้อมูลที่ประมวลผลได้จากพื้นที่ตรงส่วน User Created Packet Window

### 3. การจัดวางอุปกรณ์บนพื้นผังเครือข่าย (workspace)

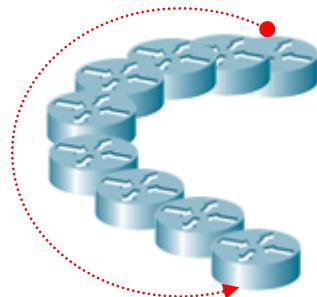
ในการจัดวางอุปกรณ์ต่างๆ บนพื้นผังเครือข่าย ผู้ใช้งานสามารถทำได้ง่ายๆ โดยการเลือก อุปกรณ์ที่ต้องการใช้งานวางลงบนพื้นที่ Workspace ในโหมด Realtime

- การวางแผนอุปกรณ์เร้าเตอร์
- เลือก ไอคอน Routers ตรงส่วน Device-Type (หรือกด CTRL+ALT+R พร้อมกัน) จะปรากฏไอคอนรายการเร้าเตอร์รุ่นต่างๆ ในส่วน Device-Specific ให้ผู้ใช้เลือก รุ่นของเร้าเตอร์ที่ต้องการแล้วลากนำไปวางบน workspace ได้ทันที ดังรูปที่ 2-13



รูปที่ 2-13 การวางแผนอุปกรณ์เร้าเตอร์

เมื่อผู้ใช้ต้องการจัดวางตำแหน่งของอุปกรณ์บน Workspace ให้เลือก select (หรือกดปุ่ม esc) ในส่วน Common Tools Bar ด้านขวาเมื่อแล้วคลิกลากอุปกรณ์ ไปยังตำแหน่งที่ต้องการได้ทันที

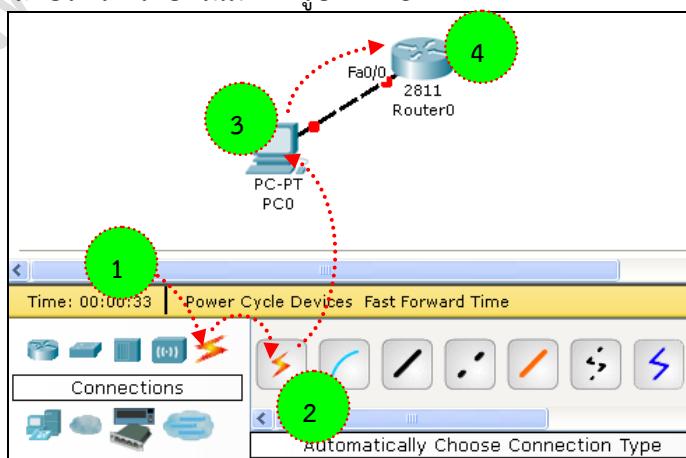


รูปที่ 2-14 การจัดวางอุปกรณ์บน workspace

เมื่อต้องการลบอุปกรณ์ออกจาก workspace ให้ผู้ใช้เลือก Delete (หรือกดปุ่ม del) ในส่วน Common Tools Bar ด้านขวาเมื่อ แล้วนำเมาส์วางทับอุปกรณ์ อุปกรณ์ ตัวดังกล่าวจะถูกลบพ้นที่, สำหรับการเคลื่อนย้ายผังเครือข่ายทั้งหมด ให้ผู้ใช้เลือก select และลากเส้นประล้อมรอบผังเครือข่ายทั้งหมดก่อน จากนั้นเลือก และลากไปยังตำแหน่งที่ต้องการ, ถ้าต้องการเขียน comment หรือคำอธิบายสั้นๆ ให้เลือก และไปวางยังจุดที่ต้องการอธิบายพร้อมกับเขียนคำอธิบายลงไป, สำหรับการย่อผังเครือข่ายให้เลือกหรือใหญ่ ผู้ใช้สามารถทำได้โดยการเลือกผัง เครือข่ายทั้งหมดก่อนด้วย select และเลือก และย่อขยายผังตามความต้องการ

- การเชื่อมต่ออุปกรณ์

สำหรับการเชื่อมต่ออุปกรณ์ผู้ใช้จำเป็นต้องเข้าใจถึงสายนำสัญญาณแต่ละประเภท ว่าใช้งานอย่างไร เช่น สาย Straight-through ใช้สำหรับเชื่อมระหว่างอุปกรณ์ปลายทาง เช่น คอมพิวเตอร์ โน็ตบุ๊ค ปรินเตอร์ แฟร์กซ์ เป็นต้น เข้ากับสวิตช์ ซึ่ง บางครั้งผู้ใช้ใหม่อาจจะไม่คุ้นเคย หรือไม่ทราบ ดังนั้น packet tracer จึงเตรียม เครื่องมือใหม่เอาไว้ช่วยเหลือคือ (Automatically choose connection type) เครื่องมือดังกล่าวจะช่วยเลือกชนิดของสายที่ใช้ในการเชื่อมต่อที่เหมาะสมสำหรับ อุปกรณ์แต่ละประเภทให้อัตโนมัติ ดังรูปที่ 2-15



รูปที่ 2-15 แสดงการเชื่อมต่ออุปกรณ์โดยใช้ automatically connection จากรูปที่ 2-15 แสดงการเชื่อมต่ออุปกรณ์ปลายทางคือ PC เข้ากับเราเตอร์ผ่าน พอร์ต FastEthernet 0/0 ซึ่งต้องใช้สายประเภท cross over (สายชนิดไขว้) ขั้นที่

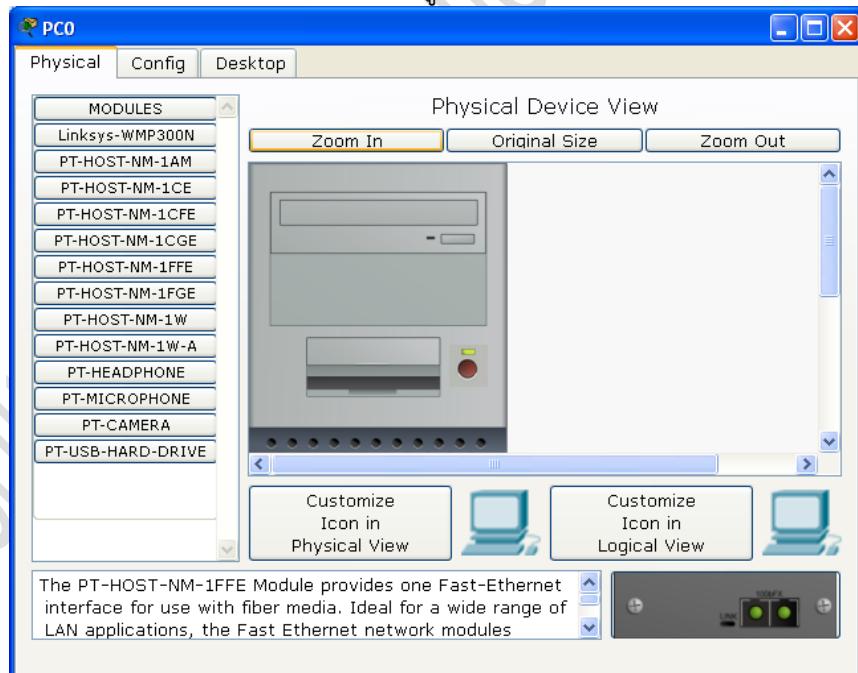
1 ให้เลือก  ในส่วน Device-Type ขั้นที่ 2 ให้เลือก automatically choose connection type ในส่วน Device-Specific ขั้นที่ 3 คลิกเลือกที่ตัวอุปกรณ์ (PC) แล้วลากไปยังเราเตอร์ โปรแกรมจะเลือกสายสัญญาณให้เองโดยอัตโนมัติ

- การคอนฟิกหรือปรับแต่งอุปกรณ์

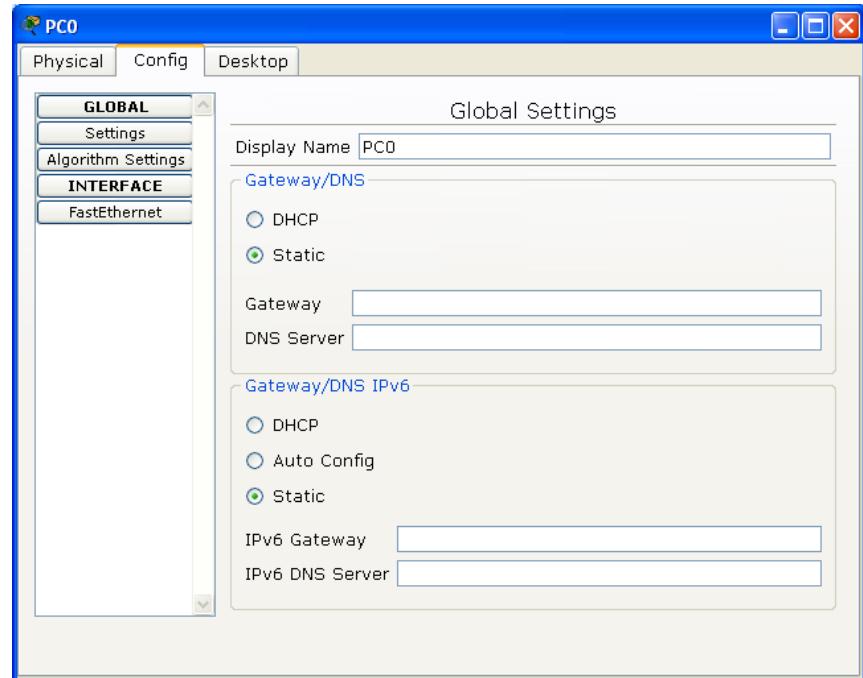
สำหรับการคอนฟิกคุณสมบัติเพิ่มเติมของอุปกรณ์ สามารถทำได้โดยการดับเบิลคลิกที่ตัวอุปกรณ์ได้โดยตรง ซึ่งจะปรากฏแท็บคล้ายๆ กัน 3 แท็บคือ แท็บ Physical, Config, Desktop (เมื่อเป็นอุปกรณ์ปลายทาง เช่น PC, Server) หรือ CLI (กรณีที่เป็นอุปกรณ์เครือข่าย เช่น สวิตช์ เราเตอร์)

#### การคอนฟิก PC และ Server

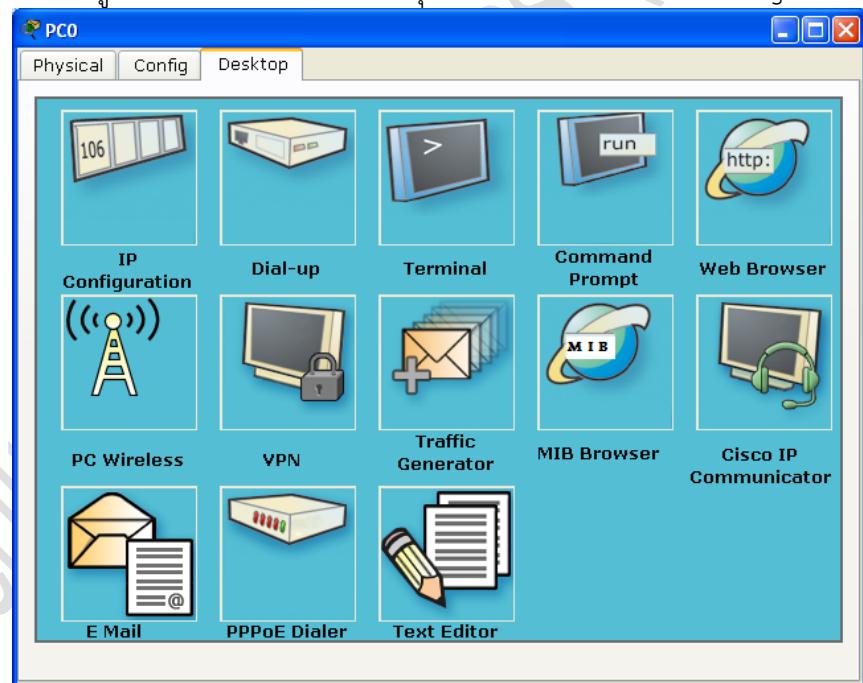
การคอนฟิก PC และ Server สามารถทำได้โดยดับเบิลคลิกที่ตัวอุปกรณ์ ในแท็บ Physical จะกำหนดคุณสมบัติทางด้านกายภาพ เช่น ชนิดของการ์ดเน็ตเวิร์ก แบบต่างๆ เช่น การ์ดโทรศัพท์ FastEthernet, Gigabit เป็นต้น ในแท็บ Config จะกำหนดคุณสมบัติในการเชื่อมต่อ เช่น หมายเลขไอพี subnet, gateway เป็นต้น แท็บ Desktop จัดเตรียมเครื่องมือต่างๆ (ในระดับแอพพลิเคชัน) ที่จำเป็นสำหรับทดสอบระบบเครือข่าย เช่น terminal, command prompt, web browser, wireless, e-mail เป็นต้น ดังรูปที่ 2-16, 2-17, 2-18 ตามลำดับ



รูปที่ 2-16 แสดงการกำหนดคุณสมบัติของ PC ในแท็บ Physical



รูปที่ 2-17 แสดงการกำหนดคุณสมบัติของ PC ในแท็บ Config

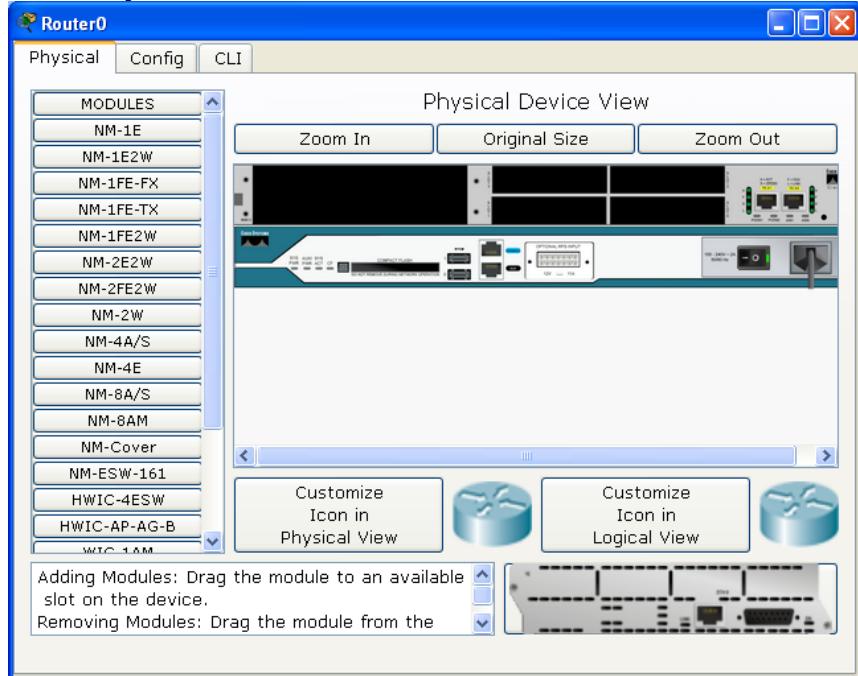


รูปที่ 2-18 แสดงแอพพลิเคชันที่เตรียมไว้ให้ใช้งานของ PC ในแท็บ Desktop

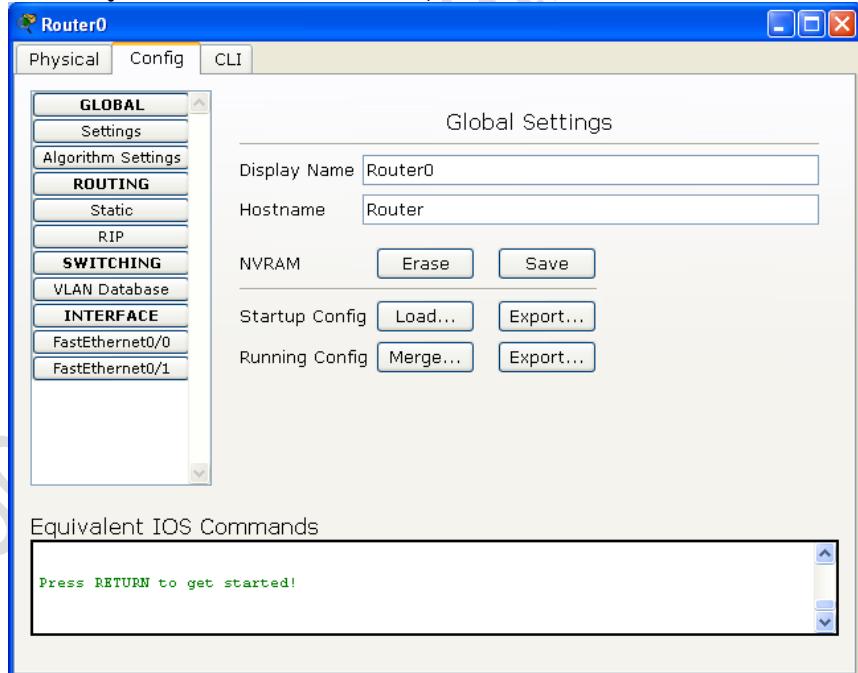
### การคอนฟิกสวิตซ์หรือเราเตอร์

การคอนฟิกสวิตซ์หรือเราเตอร์จะคล้ายกัน คือทำได้โดยดับเบิลคลิกที่ตัว อุปกรณ์ ในแท็บ Physical จะกำหนดคุณสมบัติทางด้านกายภาพ เช่น ชนิดของ การ์ดเน็ตเวิร์ก แบบต่างๆ การ์ดโทรศัพท์, FastEthernet, Gigabit เป็นต้น ในแท็บ Config จะกำหนดคุณสมบัติในการเชื่อมต่อ เช่น หมายเลขไอพีของแต่ละ อินเทอร์เฟส, โพรโทคอลเร้าติ้ง, VLAN เป็นต้น แท็บ CLI เป็นการควบคุมและ

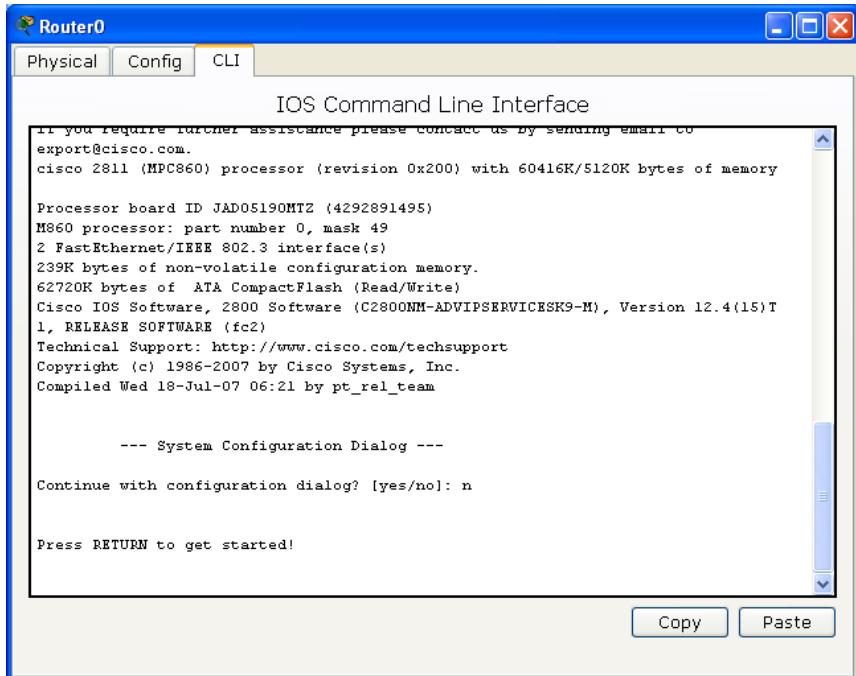
ปรับแต่งสวิตซ์หรือเราเตอร์โดยใช้การป้อนคำสั่งครั้งละ 1 บันทึก (command line) ดังรูปที่ 2-19, 2-20, 2-21 ตามลำดับ



รูปที่ 2-19 แสดงการกำหนดคุณสมบัติของ Router ในแท็บ Physical



รูปที่ 2-20 แสดงการกำหนดคุณสมบัติของ Router ในแท็บ Config

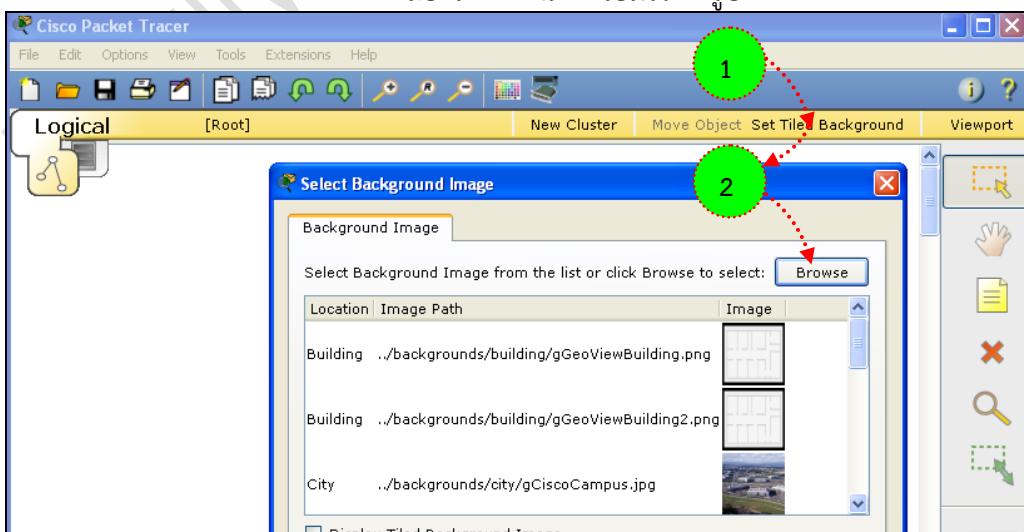


รูปที่ 2-21 แสดงการค-Onพิกเรเตอร์ด้วย command line ในแท็บ CLI

- การกำหนดพื้นหลังให้ผังเครือข่าย

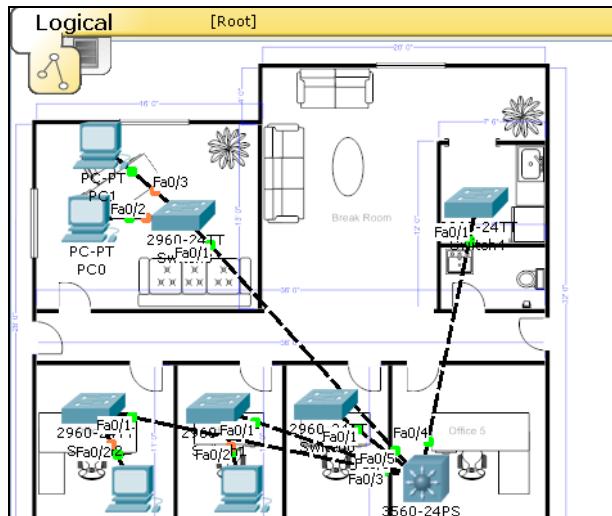
ในโหมด Realtime แท็บ Set Field Background ผู้ใช้สามารถกำหนดภาพของ background ได้เอง ซึ่งจะช่วยให้ผู้ออกแบบสามารถนำผังเครือข่ายในทาง logical วางทับช่องเข้ากับแผนที่เมืองหรือสำนักงานจะทำให้เห็นภาพระบบเครือข่ายได้ชัดเจนขึ้น สำหรับขั้นตอนการกำหนด background มีดังนี้

1. เลือกแผนที่ที่จะใช้วางระบบเครือข่ายจริง เช่น แผนที่เมือง ตึก หรืออาคาร ผังห้องภายในอาคารเป็นต้น (ควรเป็นนามสกุล .jpg หรือ .png)
2. ในแท็บ Logical เลือก Set Tiled Background ⇒ Browser  
⇒ เลือกภาพแผนที่เตรียมไว้ ดังรูปที่ 2-22



รูปที่ 2-22 กำหนด background ในผังเครือข่าย

3. วางแผนอุปกรณ์ลงในแผนที่ตามความต้องการ

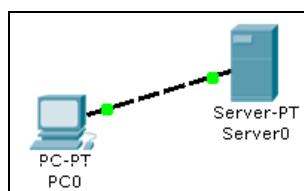


รูปที่ 2-23 วางแผนอุปกรณ์ลงบนแผนที่

#### 4. Creating a First Network

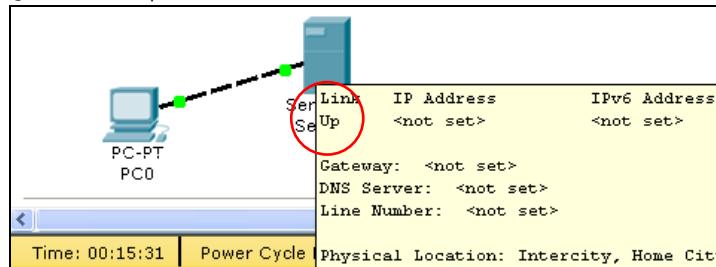
การออกแบบระบบเครือข่ายแต่เดิมนั้นผู้ออกแบบจะต้องเขียนผังในกระดาษ หรือเขียนด้วยโปรแกรมที่ใช้สำหรับออกแบบเครือข่ายโดยเฉพาะ เช่น Smart Draw, Visio, EDraw เป็นต้น จากนั้นก็ทดสอบติดตั้งจริง ผลของการติดตั้งจริงอาจจะไม่ตรงกับที่ออกแบบไว้ อาจเนื่องมาจากหลายสาเหตุ เช่น ผู้ใช้ปรับเปลี่ยนความต้องการ สถานที่ติดตั้งไม่อำนวย ปัญหากับโครงสร้างของอาคาร หรือไม่สามารถเข้ากันได้กับเครือข่ายเดิมที่ติดตั้งไว้แล้ว เป็นต้น ทำให้ผู้ออกแบบต้องมาปรับแก้ผังเดิมที่ได้ออกแบบไว้ให้เข้ากับงานจริงที่ได้ติดตั้ง ซึ่งเมื่อเทียบกับการออกแบบเครือข่ายในปัจจุบัน จะประหยัดเวลาได้มากเนื่องจาก การออกแบบและการทดลองเชื่อมต่อปัจจุบัน เป็นไปอย่างรวดเร็ว ทำให้ผู้ใช้สามารถลองเครือข่ายได้โดย ทำให้ลดขั้นตอนและเวลาได้มาก และประโยชน์ที่เห็นได้ชัดอีกประการหนึ่งคือ ผู้ออกแบบสามารถสร้างเครือข่ายจำลอง (Logical Network Prototype) ให้ลูกค้าเห็นร่วงหน้าก่อนได้ ว่าจะออกแบบเป็นลักษณะอย่างไร (คล้ายกับสร้างบ้านด้วยอย่างให้ผู้ซื้อได้เห็นก่อน นั่นเอง) นำมาเริ่มสร้างเครือข่ายแรกกันดีกว่าครับ

- เลือกอุปกรณ์เชื่อมต่อปลายทางในส่วน Device-Type เป็น End Devices  $\Rightarrow$  Device-Specific เลือก Generic PC และ Generic Server  $\Rightarrow$  ลากไปวางไว้ในส่วน workspace
- เลือก Connections  $\Rightarrow$  Copper Straight Through (เส้นสีดำไม่มีเส้นประ)  $\Rightarrow$  คลิกขวาที่ PC เลือก FastEthernet  $\Rightarrow$  ลากไปที่ Server คลิกขวา แล้วเลือก FastEthernet



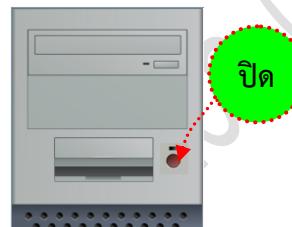
รูปที่ 2-24 เชื่อมต่อ PC กับ Server ด้วยสายแบบ Cross Over

- จากรูป 2-24 เมื่อใช้สายแบบ Copy Straight Through ลิงค์ที่เชื่อมต่อจะแสดงสถานะเป็นสีแดงแสดงว่า การเชื่อมต่อยังไม่สำเร็จ (เลือกสายเชื่อมต่อผิด) ให้เปลี่ยนเป็นสายแบบ Copper Cross Over แทน สถานะของลิงค์จะเป็นสีเขียวแสดงว่าใช้งานได้แล้ว เมื่อเลื่อนมาส์เซ็หัวไปใกล้เครื่อง PC หรือ Server จะมี message ว่าลิงค์ up

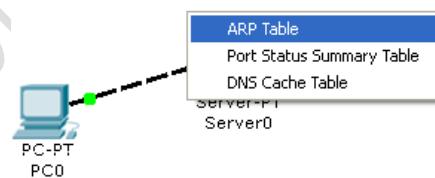


รูปที่ 2-25 แสดงสถานะลิงค์ up

- ทดสอบปิดเครื่องโดยการดับเบลคลิกที่เครื่อง PC หรือ Server ในแท็บ Physical กดปุ่ม power switch ลิงค์จะ down



- ทดสอบโดยการเปิด power switch อีกครั้ง ลิงค์จะกลับมาเป็น up อีกครั้ง จากนั้นทดสอบตรวจสอบค่าของเครื่อง PC และ Server โดยใช้ Inspect 🔎 คลิกที่เครื่องทั้งสอง ให้ทำการตรวจสอบ ARP Table, Port Status Summary Table และ DNS Cache Table



จากการทดสอบ ตาราง ARP, Port, DNS ในเบื้องต้นจะไม่มีค่าใดๆ เนื่องจากยังไม่มีการคอนฟิกเครื่อง PC และ Server

- ดับเบลคลิกเครื่อง PC ในแท็บ Config ให้ทดลองเปลี่ยนค่า Display name เป็น Pacman และ DNS Server เป็น 192.168.0.105, ที่ Interface เลือกอินเทอร์เฟสชนิด FastEthernet ให้กำหนด IP Address เป็น 192.168.0.110 แล้วทดสอบโดยใช้ Inspect (ยกเลิก Inspect ให้กดปุ่ม esc) อีกครั้ง ที่ Port Status จะปรากฏหมายเลข MAC Address และ IP Address เมื่อต้องการกำหนดค่า Bandwidth, Duplex, DHCP, IPv6 ก็สามารถกำหนดได้ในเมนูนี้ เช่นเดียวกัน การกำหนดค่า IP Address, Subnet Mask, Default Gateway, DNS Server สามารถกำหนดได้ในแท็บ Desktop ⇒ IP Configuration ได้เช่นเดียวกัน
- ขั้นตอนต่อไป ให้แก้ไขคอนฟิกเครื่อง Server โดยการดับเบลคลิกที่ Server ⇒ Config ⇒ เปลี่ยนชื่อในช่อง Display Name เป็น Web Server ⇒

FastEthernet กำหนด IP Address เป็น 192.168.0.105  $\Rightarrow$  ตรวจสอบ Port Status เป็น On  $\Rightarrow$  เลือก DNS แท็บ กำหนดในช่อง Name เป็น [www.firstlab.com](http://www.firstlab.com) type เป็น A Record และ ช่อง Address เป็น 192.168.0.105  $\Rightarrow$  คลิก Add สุดท้ายอย่าให้ตรวจสอบว่า DNS Service มีสถานะเป็น On หรือไม่

- ตรวจสอบเครื่อง Server อีกครั้ง โดยใช้ Inspect
- ขั้นตอนสุดท้ายให้ทำการบันทึกผังเครือข่ายโดยเลือก เมนู File  $\Rightarrow$  Save As..  $\Rightarrow$  เลือกตำแหน่งที่ต้องการบันทึก ตั้งชื่อเป็น Lab2-1.pkt และแสดงว่าเครือข่ายแรกเสร็จเรียบร้อยแล้วรับ

ทดลองสร้างข้อมูล (Add Simple PDU) เพื่อทดสอบการเชื่อมต่อในโหมด Realtime

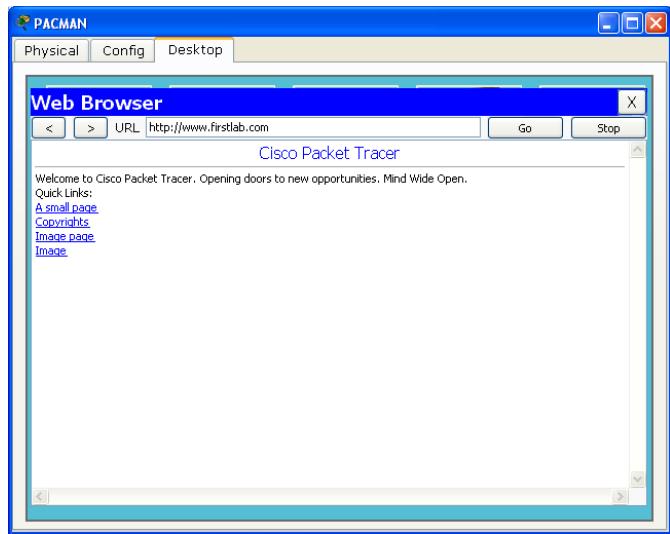
- คลิกเลือก Add Simple PDU ทางด้านขวาเมื่อ ซึ่งหมายถึง鄱โ拓โคลอนิดหนึ่งที่ใช้สำหรับทดสอบเครื่องปลายทางว่าทำงานอยู่หรือไม่ (เรียกว่า ping message หรือเรียกว่า echo request) คลิกที่เครื่อง PC 1 ครั้ง และคลิกที่เครื่อง Server อีก 1 ครั้ง เมื่อ ping สำเร็จจะมี message ที่เรียกว่า echo reply ตอบกลับมาจาก Server ให้ดูผลลัพธ์การทำงานได้ในส่วน User Created Packet Window อยู่ด้านขวาล่าง

Fire	Last Status	Source	Destination	Type	Color
●	Successful	PACMAN	Web Server	ICMP	■
●	Successful	PACMAN	Web Server	ICMP	■

โปรแกรมจะแสดงผลลัพธ์การ ping ใน Scenario 0 เสมอ ถ้าต้องการทดสอบผลลัพธ์แต่ละครั้งแยกกันให้สร้าง Scenario ใหม่ เช่น Scenario 1, 2, 3 (เพิ่ม scenario ใหม่โดยกดปุ่ม New และกดปุ่ม Delete เพื่อลบ) ตามลำดับ สำหรับข้อมูลที่แสดงใน Scenario จะแสดง Last Status ว่า Successful และว่าการทำงานสำเร็จ (จากตัวอย่าง Source=Pacman, Destination=Web Server, Type=ICMP เป็นต้น) ลองทดสอบ ping กลับทิศทางอีกครั้งว่าเป็นอย่างไร เป็นอันสิ้นสุดการทดสอบด้วยการใช้ Simple PDU (ping request/reply)

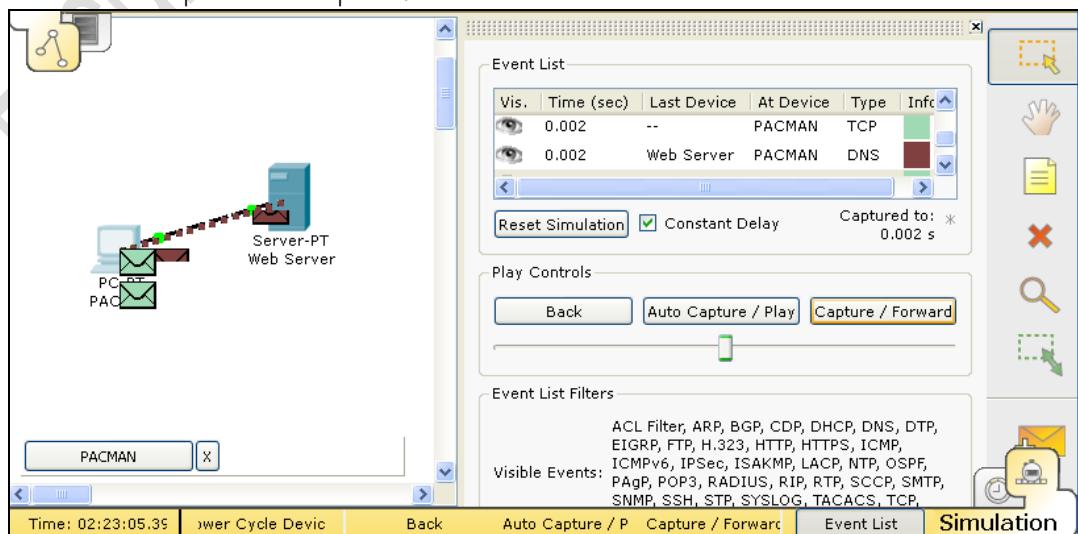
ทดสอบการทำงานของเว็บเซิร์ฟเวอร์ โดยใช้โปรแกรม Browser ที่ผ่านไฟล์แนบท้าย

- คลิกที่เครื่อง PC เลือกแท็บ Desktop  $\Rightarrow$  เลือก Web Browser  $\Rightarrow$  ในช่อง URL ใส่ข้อมูลเป็น [www.firstlab.com](http://www.firstlab.com) เสร็จแล้วกดปุ่ม go โปรแกรมจะแสดงข้อมูลใน Web Browser ดังรูปที่ 2-26



รูปที่ 2-26 ทดสอบการใช้งานเว็บเซิร์ฟเวอร์

- ทดสอบอีกครั้งโดยการป้อนข้อมูลใน URL [www.abc.com](http://www.abc.com) และกดปุ่ม Go โปรแกรม Browser จะแสดง Host Name Unresolved และแสดงว่าไม่สามารถค้นหาเว็บเซิร์ฟเวอร์ดังกล่าวได้
- ทดลองอีกครั้งโดยการใส่ข้อมูลในช่อง URL เป็นหมายเลข IP Address ของเครื่องเว็บเซิร์ฟเวอร์ คือ 192.168.0.105 และกดปุ่ม Go ผลปรากฏว่าสามารถแสดงผลได้ถูกต้อง
- ทดลองเปลี่ยนโหมดการทำงานเป็น Simulation ซึ่งในโหมดนี้ผู้ใช้สามารถควบคุมเวลาการทำงานได้ ส่งผลให้เวลาในการทำงานของโปรแกรมจะช้ากว่าปกติ และผู้ใช้ก็สามารถสังเกตพฤติกรรมของข้อมูลได้ชัดเจน เลือกที่เครื่อง PC  $\Rightarrow$  เลือกแท็บ Desktop  $\Rightarrow$  Web Browser  $\Rightarrow$  ใส่ในช่อง URL เป็น [www.firstlab.com](http://www.firstlab.com) กดปุ่ม Go  $\Rightarrow$  กลับไปยัง workspace  $\Rightarrow$  สังเกตที่ Event List จะปรากฏ โปรโตคอล DNS อยู่ และมีของจดหมายปรากฏบนเครื่อง PC ด้วย  $\Rightarrow$  เลือก Auto Capture/Play เมื่อต้องการเฝ้าดูแพ็คเก็ตแบบต่อเนื่อง หรือเมื่อต้องการเฝ้ามองทีละ step ให้เลือก Capture/Forward

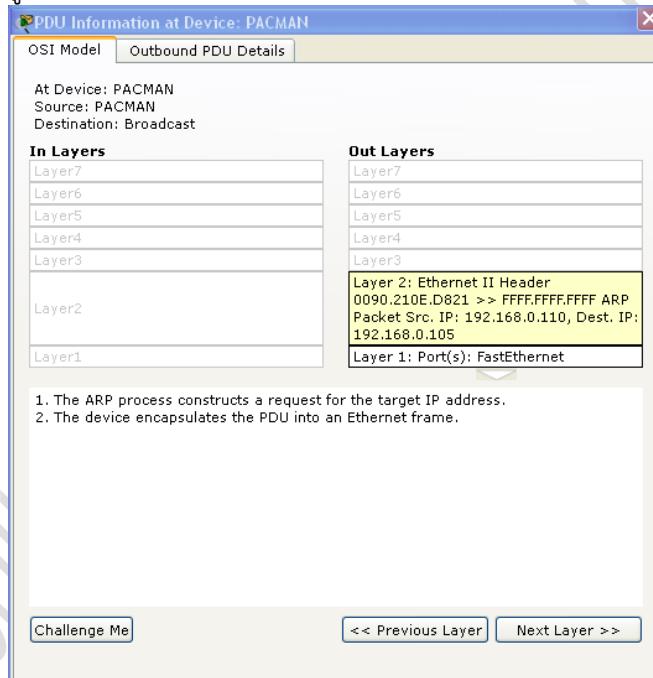


รูปที่ 2-27 ทดสอบการทำงานในโหมด simulation

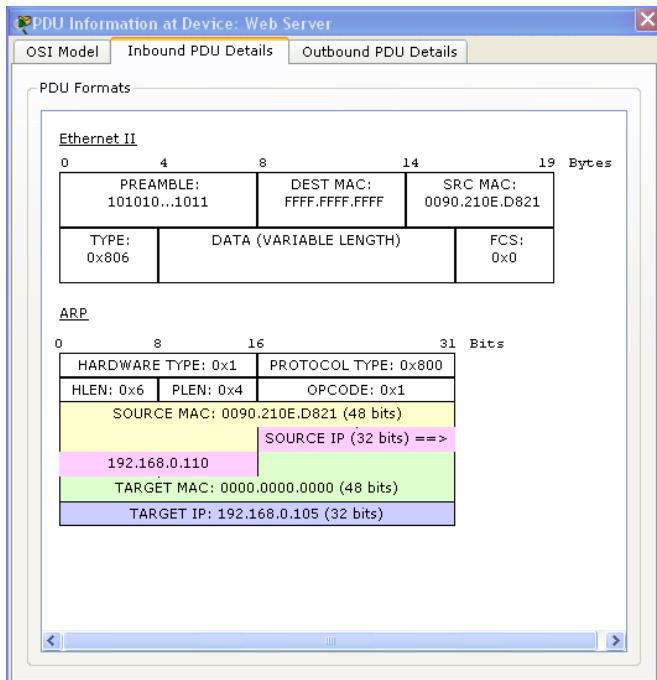
สังเกตุว่า ในการทดสอบครั้งนี้จะมีโปรโตคอลปรากฏใน Even List 2 ชนิดคือ DNS และ TCP (Web Server) เนื่องจากเครื่อง PC จะต้องสอบถามชื่อผ่าน Domain Name Server ก่อนเสมอ เพื่อแปลง URL ([www.firstlab.com](http://www.firstlab.com)) เป็นหมายเลข IP Address จากนั้น PC จึงใช้หมายเลข IP ที่ดังกล่าวเข้าใช้บริการเว็บเซิร์ฟเวอร์ต่อไป

### สำรวจเนื้อในของแพ็คเก็ต

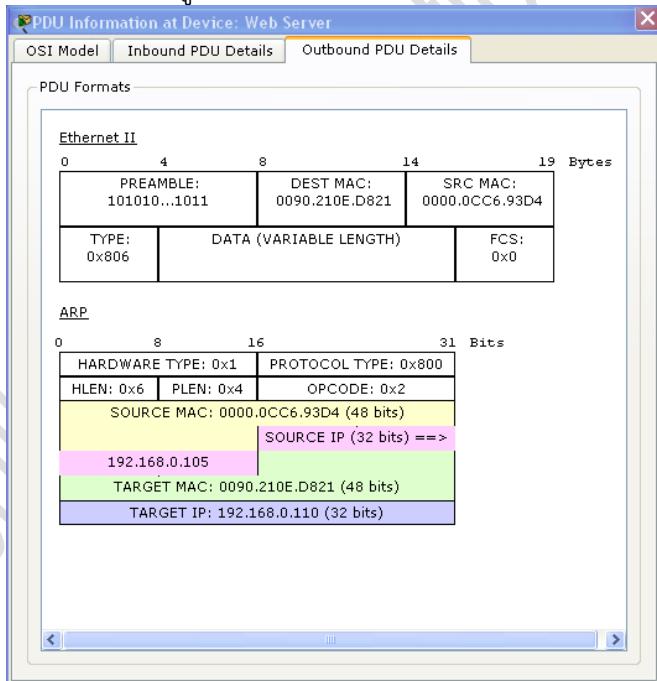
ในหัวข้อนี้จะแสดงข้อมูลภายในแพ็คเก็ตว่ามีหน้าตาเป็นอย่างไร เริ่มต้นโดยคลิกเลือกที่ โหมด Simulation (อย่าลืมกดปุ่ม Reset Simulation เพื่อเคลียร์ค่าข้อมูลเดิมก่อน) ทดสอบ Add Simple PDU (ping) จากเครื่อง PC ไปยัง Server อีกครั้ง เมื่อโปรแกรมแสดงการส่งแพ็คเก็ต เป็นลักษณะของจดหมาย  ให้คลิกที่ช่องดังกล่าว สีของช่องจดหมายในแต่ละช่องแสดงถึงโปรโตคอลในแต่ละเลเยอร์ที่ทำงานอยู่ภายใต้ OSI Model ตัวอย่าง เช่น สีม่วงคือ โปรโตคอล ICMP ที่กำลังทำงานอยู่ในชั้นของ Network Layer หรือ สีเขียวหมายถึงโปรโตคอล ARP ที่ทำงานอยู่ในระดับเลเยอร์ data link (เลเยอร์ 2 ใน OSI Model แทนสีเหลืองแสดงถึงกำลังทำงานที่ชั้นดังกล่าว) เมื่อผู้ใช้ต้องการดูข้อมูลอย่างละเอียดให้คลิกเลือกที่แท็บ Inbound/Outbound PDU Details



รูปที่ 2-28 โปรโตคอล ARP ทำงานที่เลเยอร์ที่ 2 (data link) ใน OSI Model

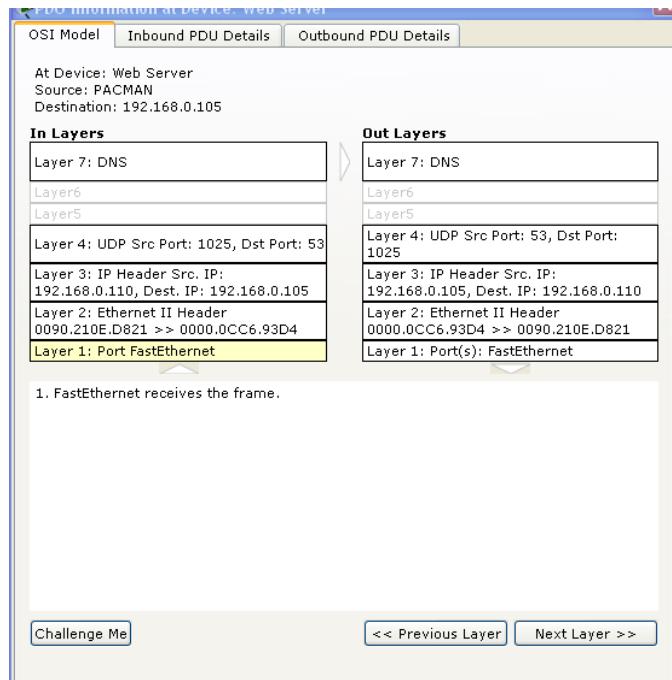


รูปที่ 2-29 แสดงข้อมูลอย่างละเอียดภายในโปรโตคอล ARP และ โปรโตคอล Ethernet ในทิศทาง  
ข้อมูลเข้า Inbound PDU Details



รูปที่ 2-30 แสดงข้อมูลอย่างละเอียดภายในโปรโตคอล ARP และ โปรโตคอล Ethernet ในทิศทาง  
ข้อมูลออก Outbound PDU Details

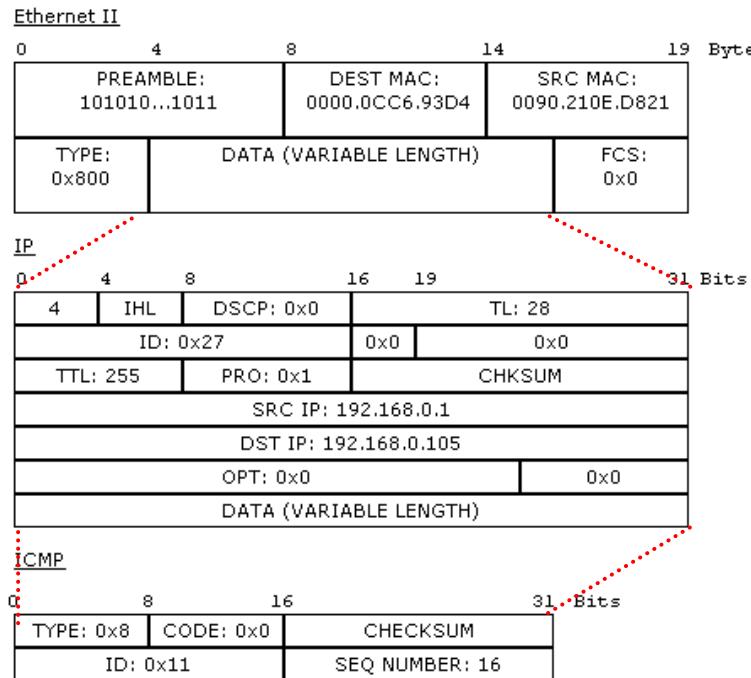
ทดลองอีกครั้งโดยการเลือกแท็บ Desktop ในเครื่อง PC  $\Rightarrow$  Web Browser ใส่ข้อมูลในช่อง URL เป็น [www.firstlab.com](http://www.firstlab.com) และคลิก Go จากนั้นให้กลับไปที่ workspace อีกครั้ง แพ็คเก็ตจะหยุดอยู่ให้ผู้ใช้เลือก Capture/Forward เพื่อผลักดันให้แพ็คเก็ตเคลื่อนที่ออกจากเครื่อง PC ให้สังเกตุว่ามีช่องสินลักษณะซึ่งเป็นแพ็คเก็ตของ DNS เกิดขึ้นมาก่อน อาศัยโปรโตคอล UDP (ชั้นที่ 4) พอร์ต 53 แพ็คเก็ต DNS นั้นทำงานถึงระดับที่ 7 ของ OSI Model ดังรูปที่ 2-31



รูปที่ 2-31 แสดงข้อมูลโปรโตคอล DNS อาศัยโปรโตคอล UDP/IP ในการส่งข้อมูล ในทำนองเดียวกันเมื่อคดปุ่ม Capture/Forward ไปเรื่อยๆ พ้อมฯ กับสังเกตแพ็คเก็ตที่วิ่งไปวิ่งมาทุกๆ แพ็คเก็ตจะพบว่า แต่ละโปรโตคอลทำงานในชั้นของ OSI Model ที่ต่างกัน ดังนี้

Protocol	Layer1	Layer2	Layer3	Layer4	Layer5	Layer6	Layer7
ICMP(ping)	Port	MAC	IP+ICMP	-	-	-	-
DNS	Port	MAC	IP	UDP(53)	-	-	DNS
HTTP	Port	MAC	IP	TCP(80)	-	-	HTTP
HTTPS	Port	MAC	IP	TCP(443)	-	-	HTTPS
DHCP	Port	MAC	IP	UDP(67,68)	-	-	DHCP

ตารางที่ 2-7 ตัวอย่างโปรโตคอลที่ทำงานแตกต่างกันในแต่ละชั้นบน OSI Model  
 จากตารางที่ 2-7 สังเกตว่าโปรโตคอล ICMP (ping) จะทำงานเพียงแค่ชั้นที่ 3 ใน OSI Model เท่านั้น โดยเริ่มต้นที่ เครื่อง PC ทำการสร้างแพ็คเก็ต ICMP จากนั้นส่งออกไปยัง port (ในที่นี้คือ FastEthernet ทำงานในเลเยอร์ที่ 1) ในระดับเลเยอร์ที่ 2 จะอาศัยโปรโตคอล Ethernet ใน การผลักดันให้แพ็คเก็ตเคลื่อน ไปยัง Next Hop โดยอาศัย MAC Address ในการค้นหาที่อยู่ของ โหนดหรือ Hop เพื่อบ้าน โดยมีข้อมูลในเลเยอร์ที่ 3 เป็นผู้กำหนดเส้นทางที่จะไป (กำหนดโดยใช้ หมายเลข IP Address) ในเลเยอร์นี้จะมีโปรโตคอล IP เป็นผู้ผลักดันแพ็คเก็ตในการหาเส้นทาง และ ภายในแพ็คเก็ตของ IP ก็จะมี โปรโตคอล ICMP ซ้อนอยู่ข้างในอีกที เพื่อทำหน้าที่ตรวจสอบเครื่อง ปลายทางว่าอยู่หรือไม่ สังเกตุเห็นว่าในแต่ละแพ็คเก็ตจะมีโปรโตคอลทำงานอยู่หลายตัว แต่ละตัว ทำงานคนละหน้าที่กัน ไม่ก้าวถ่ายกันเลย

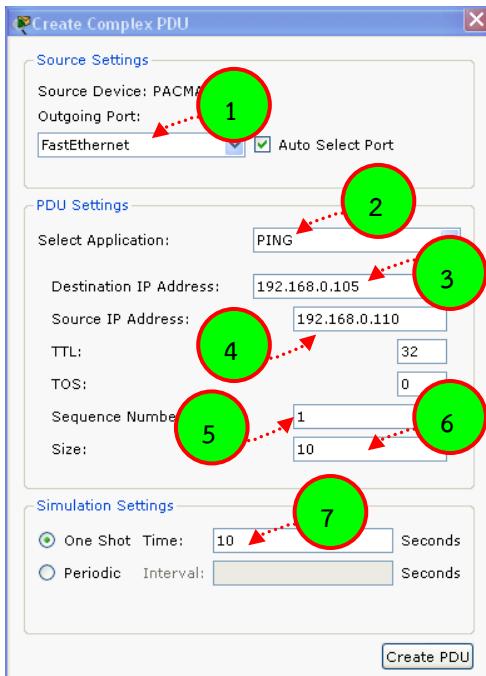


รูปที่ 2-32 แสดงความสัมพันธ์ของโปรโตคอลภายนอกและแพ็คเก็ตของ ICMP

### การใช้งาน Add Complex PDU

ในหัวข้อก่อนๆ ได้ทำการทดสอบเครือข่ายโดยใช้ Add Simple PDU ซึ่งเป็นการทดสอบโดยใช้โปรโตคอล ICMP (ping) เท่านั้น เมื่อผู้ใช้ต้องการทดสอบเครือข่ายในขั้นที่สูงขึ้น ให้ใช้เครื่องมือที่ชื่อว่า Add Complex PDU ซึ่งเตรียมโปรโตคอลให้ผู้ใช้ทดสอบเครือข่ายได้หลายแบบ เช่น ทดสอบด้วย DNS, Finger, FTP, HTTP, HTTPS, IMAP, POP, NETBIOS, SFTP, SMTP เป็นต้น ซึ่งมีขั้นตอนดังนี้

- เลือกหมวดได้ทั้งแบบ Realtime และ Simulation  $\Rightarrow$  เลือก Add Complex PDU  $\Rightarrow$  คลิกไปที่ตัวอุปกรณ์ที่ต้องการให้สร้างแพ็คเก็ตในการทดสอบ  $\Rightarrow$  ปรากฏ Dialog Create Complex PDU  $\Rightarrow$  ในช่อง Outgoing Port ให้เลือก อินเทอร์เฟสการต่อที่ต้องการส่งข้อมูลออกไปยังเครือข่าย (เช่น เลือก FastEthernet)  $\Rightarrow$  ในแท็บ PDU Setting เป็นการกำหนดคุณสมบัติในการสร้างแพ็คเก็ต ในช่อง Selection Application ให้เลือกโปรโตคอลที่ต้องการสร้าง เช่น ICMP  $\Rightarrow$  คุณสมบัติของโปรโตคอลแต่ละตัวจะกำหนดไม่เหมือนกัน ในที่นี้อยู่กตัวอย่างเฉพาะ ICMP เท่านั้น



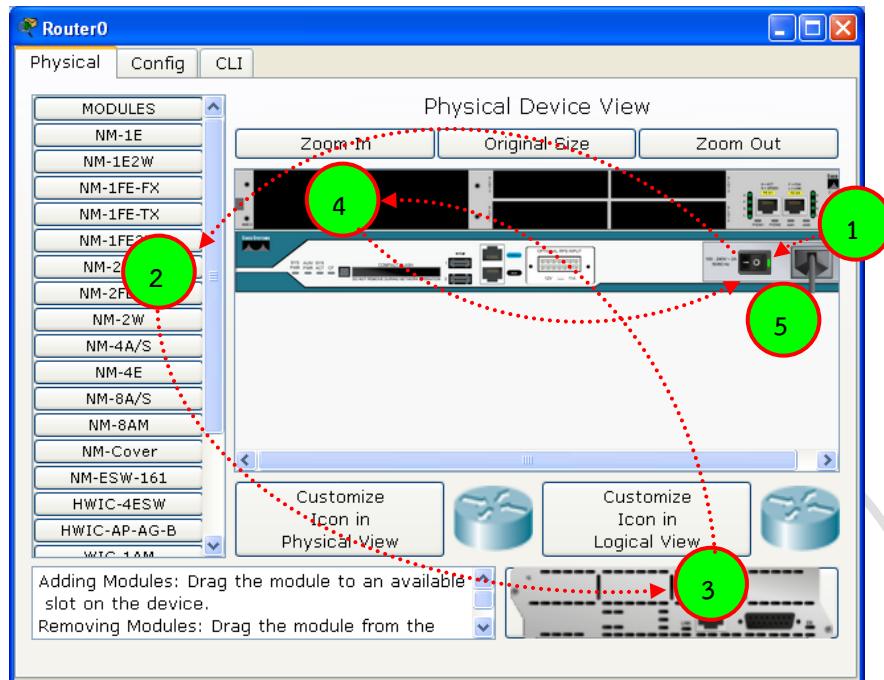
รูปที่ 2-33 แสดงการกำหนดค่าใน PDU

1. เลือกอินเทอร์เฟสที่ต้องการส่งแพ็คเก็ตออกสู่เครือข่าย (เลือกเป็น FastEthernet)
2. เลือก Application ที่ต้องการใช้ทดสอบ (PING)
3. กำหนดหมายเลข IP ปลายทางที่ต้องการทดสอบ (เช่น 192.168.0.105)
4. กำหนดหมายเลข IP ต้นทางที่ทดสอบ (เช่น 192.168.0.110)
5. กำหนดลำดับของแพ็คเก็ตที่ใช้ทดสอบ (เป็นจำนวนเต็ม)
6. กำหนดขนาดของแพ็คเก็ต (เป็นจำนวนเต็ม ค่า default=0)
7. กำหนดเวลาในการแสดงผลแต่ละครั้งเมื่อทำงานในโหมด Simulation

เมื่อกำหนดคุณสมบัติครบถ้วนแล้ว (ถ้ากำหนดไม่ครบจะมี Dialog เตือนว่ายังกำหนดไม่ครบ) ให้เลือก Create PDU และคลิกที่ปุ่มที่ใช้ทดสอบ เช่น PC จะปรากฏของจดหมาย ต่อไปให้เลือก Capture/Forward เมื่อต้องการสังเกตุพฤติกรรมของแพ็คเก็ตทีละ step แต่ถ้าต้องการทดสอบอย่างต่อเนื่องให้ใช้ Auto Capture/Play แล้วทำการทดสอบเหมือนที่อธิบายไว้แล้ว

## 5. Devices and Modules

โดยปกติอุปกรณ์เครือข่ายทุกๆ ตัวสามารถเพิ่ม/ลด อุปกรณ์ใหม่ได้ เช่น การติดต่อเว็บเซอร์ฟเวอร์ต่างๆ จาวา ໄวเลสแลน เป็นต้น สำหรับใน packet tracer ก็เช่นเดียวกัน ผู้ใช้สามารถเพิ่ม/ลด อุปกรณ์ ต่างๆ ได้เช่นเดียวกัน มีขั้นตอนดังนี้ เลือกแท็บ Physical  $\Rightarrow$  ปิดสวิตช์เครื่อง  $\Rightarrow$  คลิกแล้วลาก อุปกรณ์เดิมออกจากเครื่อง (ในกรณีที่ไม่มีพอร์ต หรือ slot ว่างเหลืออยู่) หรือ เลือก Module ทางด้านขวาเมื่อที่เหมาะสมมากว่างไว้ในพอร์ตหรือ slot ที่ว่าง (ในกรณีที่มีพอร์ต หรือ slot ว่างเหลืออยู่)  $\Rightarrow$  เปิดเครื่อง



รูปที่ 2-34 แสดงการเพิ่ม/ลด Module

1. เลือกแท็บ Physical แล้วปิดเครื่อง
2. เลือก Module ที่ต้องการในแท็บ Modules
3. ลากอุปกรณ์ที่ปรากฏทางด้านล่างขวาไปใส่ใน slot ที่ว่าง (กรณีเอา Module ออกให้เลือก Module ที่ต้องการเอาออกจากมาวางที่ด้านล่างขวา)
4. วางอุปกรณ์ลงยัง slot ที่ว่างและเข้ากันได้พอดี
5. เปิดเครื่องอีกรั้ง

Feature ของ packet tracer ยังมีอีกมากมาย ซึ่งสามารถอ่านเพิ่มเติมได้จาก Contents หรือ Tutorials ในบทนี้แนะนำเฉพาะคุณสมบัติบางอย่างที่ผู้เรียนเห็นว่าควรจะรู้ในเบื้องต้น ก่อน สำหรับคุณสมบัติอื่นๆ จะค่อยๆ เพิ่มเติมทีละเล็กๆ น้อยๆ ใน บทที่ 3 How to Network Connectivity ต่อไป

### บทที่ 3

#### How to Network Connectivity

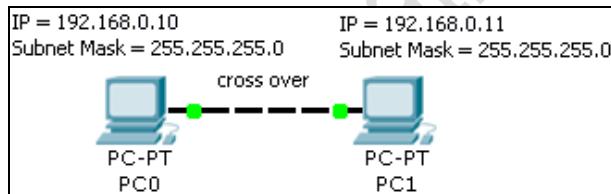
ในบทนี้จะอธิบายถึงวิธีการออกแบบและติดตั้งเครือข่ายโดยใช้โปรแกรม Packet Tracer เวอร์ชัน 5.3.x ในลักษณะแบบ step by step โดยแบ่งออกเป็น Scenario ย่อย ๆ เพื่อเป็นพื้นฐานในการสร้างระบบเครือข่ายขนาดใหญ่ๆ ในบทต่อไป ผู้อ่านสามารถเลือก Scenario ที่สนใจได้โดยไม่จำเป็นต้องเริ่มตั้งแต่ Scenario 1 (ในกรณีที่มีพื้นฐานด้านเครือข่ายอยู่แล้ว) แต่ถ้าเป็นผู้ที่เริ่มต้นเรียนเกี่ยวกับคอมพิวเตอร์เครือข่าย ผู้เขียนแนะนำว่าควรเริ่มอ่านและลงมือปฏิบัติตัวโดยตนเอง โดยเริ่มตั้งแต่ Scenario ที่ 1 ไปเรื่อยๆ ตามลำดับ



#### Scenario 1: เชื่อมต่อคอมพิวเตอร์ PC กับ PC

คำอธิบาย :

สำหรับการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ 2 เครื่อง เช่น PC กับ PC, PC กับ Notebook หรือ PC กับ Server ไม่จำเป็นต้องใช้อุปกรณ์เครือข่ายเพิ่มเติม เช่น สวิตช์ หรือ อุปกรณ์ที่จำเป็นต้องใช้คือ การต่อเน็ตเวิร์คและสายไขว้ (Cross Over) ก็เพียงพอต่อการเชื่อมต่อ แผนผังการเชื่อมต่อ :



รายการอุปกรณ์ :

1. เครื่อง PC 2 เครื่อง พร้อมการ์ดเน็ตเวิร์คชนิด FastEthernet
2. สายนำสัญญาณชนิดไขว้ (Cross Over)

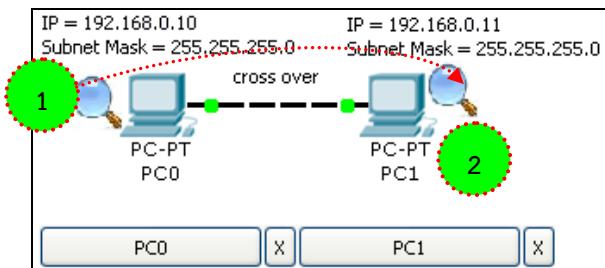
ขั้นตอนการเชื่อมต่อ :

1. เลือก End Devices (ในส่วน Device-Type)
2. เลือก Generic (ในส่วน Device-Specific) และลากมาวางใน workspace ให้ครบ 2 เครื่อง (โดยปกติจะมีชื่อเป็น PC0, PC1, PCn ตามลำดับ)
3. เลือก Connections (ในส่วน Device-Type)
4. เลือก Automatically Choose Connection Type (ในส่วน Device-Specific) และคลิกที่เครื่อง PC0 และลากไปคลิกที่ PC1 โปรแกรมจะเลือกสายชนิด Cross Over เชื่อมต่อให้อัตโนมัติ ที่เครื่องคอมพิวเตอร์จะปรากฏไฟสีเขียว แสดงว่าเชื่อมต่อสำเร็จ
5. ทดสอบการเชื่อมต่อโดยการเลือก Inspect (ในส่วน Common Tools Bar ด้านขวามือ) คลิกเลือกที่ PC0 และเลือก Port Status Summary Table ให้สังเกตุที่ Link จะมีสถานะเป็น up และ MAC Address จะปรากฏหมายเลขเป็นฐาน 16 เช่น 00E0.5C25.1EC1 (มีขนาด 48 บิต โดยตัวอักษร 1 ตัวแทนข้อมูล 4 บิต)

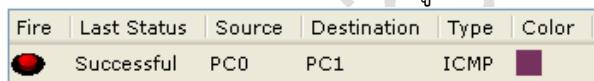
6. คลิกที่ PC0 เลือกแท็บ Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  Static  $\Rightarrow$  กำหนดค่าในช่อง IP Address เป็น 192.168.0.10 และ Subnet Mask เป็น 255.255.255.0
7. คลิกที่ PC1 เลือกแท็บ Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  Static  $\Rightarrow$  กำหนดค่าในช่อง IP Address เป็น 192.168.0.11 และ Subnet Mask เป็น 255.255.255.0
8. เสร็จสิ้นการเชื่อมต่อ

การทดสอบ :

1. เลือก Add Simple PDU  ในส่วน Common Tools Bar ด้านขวามือ
2. คลิกบนเครื่อง PC0 1 ครั้ง และคลิกที่ PC1 อีก 1 ครั้ง



3. สังเกต ในส่วน User Created Packet Window (ด้านล่างขวามือของโปรแกรม) ถ้า Last Status เป็น Successful แสดงว่าเชื่อมต่อสมบูรณ์แล้ว

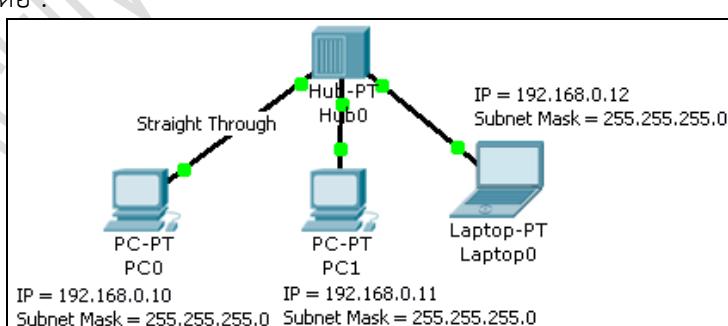


### Scenario 2: เชื่อมต่อคอมพิวเตอร์ PC0, PC1 และ Laptop0 กับ HUB

คำอธิบาย :

การเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์มากกว่า 2 เครื่องขึ้นไป จำเป็นต้องอาศัยอุปกรณ์เครือข่ายเพิ่มเติมเช่น สวิตซ์ หรือ อับ เพื่อร่วมอุปกรณ์เข้าด้วยกันเป็นเครือข่าย และใช้สายนำสัญญาณประเภทสายตรง (Straight Through) สำหรับเชื่อมอุปกรณ์เข้าด้วยกัน

แผนผังการเชื่อมต่อ :



รายการอุปกรณ์ :

1. เครื่อง PC 2 เครื่อง พร้อมการดเน็ตเวิร์คชนิด FastEthernet
2. เครื่อง Laptop 1 เครื่อง พร้อมการดเน็ตเวิร์คชนิด FastEthernet
3. สายนำสัญญาณชนิดตรง (Straight Through)

ขั้นตอนการเชื่อมต่อ :

1. เลือก End Devices  (ในส่วน Device-Type)

2. เลือก Generic  (ในส่วน Device-Specific) และลากมาวางใน workspace ให้ครบ 2 เครื่อง (โดยปกติจะมีชื่อเป็น PC0, PC1 ตามลำดับ)
3. เลือก Laptop-PT  (ในส่วน Device-Specific) และลากมาวางใน workspace
4. เลือก Connections  (ในส่วน Device-Type)
5. เลือก Copper Straight-Through  (ในส่วน Device-Specific) และคลิกที่เครื่อง PC0 ไปยัง HUB และ PC1, Laptop0 ไปยัง HUB ตามลำดับ ที่เครื่องคอมพิวเตอร์จะ ปรากฏไฟสีเขียว และง่ายๆ แสดงว่าเชื่อมต่อสำเร็จ
6. คลิกที่ PC0, PC1 และ Laptop0 ที่ลากมาไว้ในแต่ละเครื่องเลือกแท็บ Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  Static  $\Rightarrow$  กำหนดค่าหมายเลข IP Address และ Subnet Mask ดังตารางด้านล่าง

เครื่อง	IP Address	Subnet Mask
PC0	192.168.0.10	255.255.255.0
PC1	192.168.0.11	255.255.255.0
Laptop0	192.168.0.12	255.255.255.0

7. เสร็จสิ้นการเชื่อมต่อ

การทดสอบ :

1. ที่เครื่อง PC0 เลือก Desktop  $\Rightarrow$  Command Prompt
2. เมื่อปรากฏหน้าต่าง Command Prompt (หน้าต่างเป็นสีดำ) ให้ผู้ใช้ออกคำสั่งทดสอบ คือ ping ตามด้วยหมายเลข IP Address ที่ต้องการทดสอบ ในที่นี้ให้ใช้คำสั่งคือ

```
PC>ping 192.168.0.10 //ทดสอบเครื่องตัวเอง (PC0)
PC>ping 192.168.0.11 //ทดสอบเครื่อง PC1
PC>ping 192.168.0.12 //ทดสอบเครื่อง Laptop0
```

3. จากตัวอย่างการทดสอบข้างบน ถ้าเครื่องที่ถูก ping มีสถานะเป็นปกติ คือทำงานอยู่จะ ตอบกลับด้วย ICMP Reply (เช่น Reply from 192.168.0.12: bytes=32 time=109ms TTL=128) แต่ถ้า ping แล้วไม่มีเครื่องปลายทางที่ทำงานอยู่จริงจะแสดง Message คือ Request timed out

```

PC0
Physical Config Desktop

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.12

Pinging 192.168.0.12 with 32 bytes of data:

Reply from 192.168.0.12: bytes=32 time=109ms TTL=128
Reply from 192.168.0.12: bytes=32 time=47ms TTL=128
Reply from 192.168.0.12: bytes=32 time=47ms TTL=128
Reply from 192.168.0.12: bytes=32 time=31ms TTL=128

Ping statistics for 192.168.0.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 109ms, Average = 58ms

PC>

```

กราฟีฟดทดสอบ ping สำเร็จ

```

PC1
Physical Config Desktop

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.15

Pinging 192.168.0.15 with 32 bytes of data:

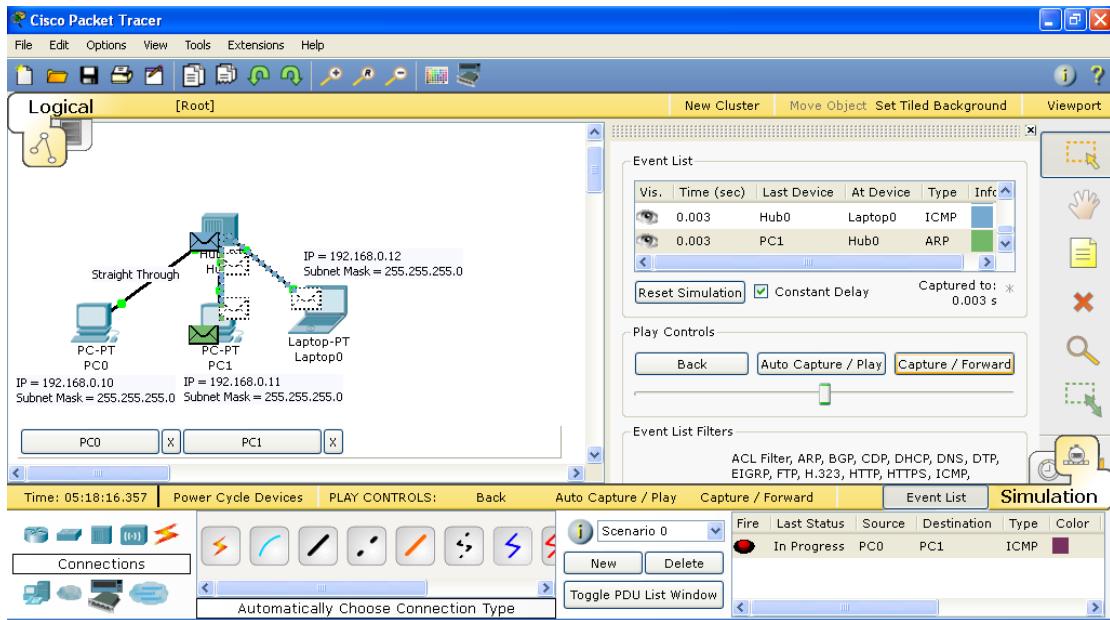
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>

```

กราฟีฟดทดสอบ ping ไม่สำเร็จ

4. ลองทดสอบด้วย ping อีกครั้ง ใน โหมด Simulation สังเกตพฤติกรรมการทำงานใน Even List (อ่านวิธีการใช้งานโหมด Simulation ในบทที่ 2)



การทดสอบด้วย ping ในโหมด Simulation

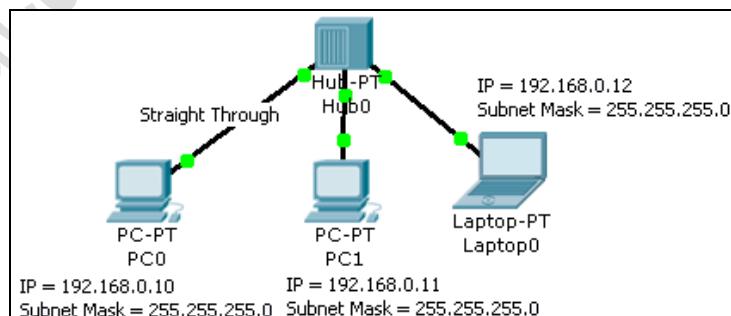
หมายเหตุ : MAC Address คือหมายเลขของการรับส่งข้อมูลที่ไม่ซ้ำกัน มีขนาด 48 บิต ใช้สำหรับติดต่อกันระหว่างอุปกรณ์ในระดับเลเยอร์ที่ 2 ของ OSI Model ซึ่งคุณสมบัติของอุปกรณ์ที่ทำงานในเลเยอร์ 2 จะติดต่อกับแบบ Hop ต่อ Hop เท่านั้น แต่เมื่อต้องการส่งข้อมูลให้ไกลออกไปจะต้องอาศัยคุณสมบัติของเลเยอร์ 3 คือ IP Address แทน

### Scenario 3: การวิเคราะห์แพ็คเก็ตอย่างละเอียด ตอนที่ 1

คำอธิบาย :

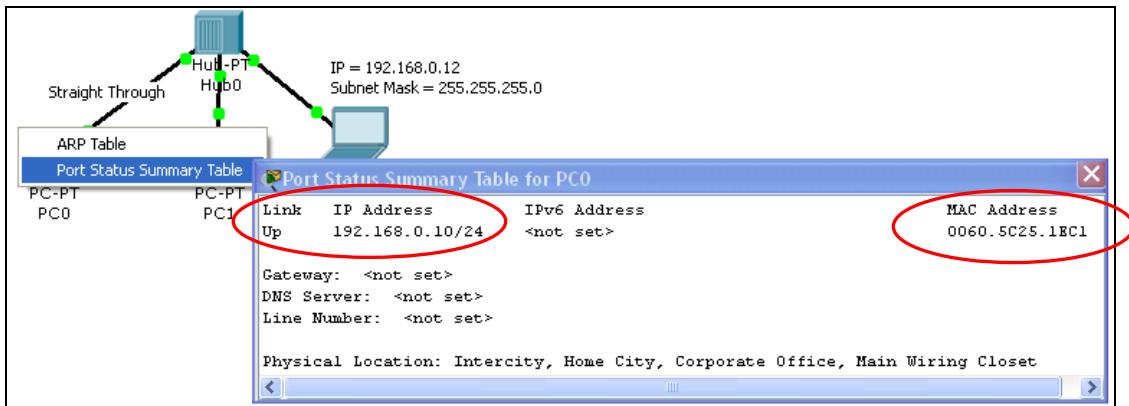
การวิเคราะห์แพ็คเก็ตอย่างละเอียดจะทำให้เราสามารถเข้าใจและค้นหาปัญหาที่เกิดขึ้นบนระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังนั้นในหัวข้อนี้ผู้เขียนจะแนะนำ เทคนิคการเฝ้ามองแพ็คเก็ตอย่างเป็นระบบ เพื่อให้ผู้อ่านเข้าใจกระบวนการทำงานของเครือข่ายอย่างเป็นรูปธรรม จากตัวอย่างเครือข่ายใน Scenario 2 ให้ปฏิบัติตามขั้นตอนดังนี้

แผนผังการเชื่อมต่อ :



ขั้นตอนการวิเคราะห์ :

1. ในเบื้องต้นให้ทำการตรวจสอบ Port Status ก่อนว่ามีสถานะเป็น up หรือไม่ กับทุกๆ เครื่องที่เชื่อมอยู่บนเครือข่ายโดยใช้ Inspect เมื่อแน่ใจว่าทุกๆ Port มีสถานะเป็น up แล้ว ให้ทำการต่อไป



#### การตรวจสอบสถานะการทำงานของ Port Status

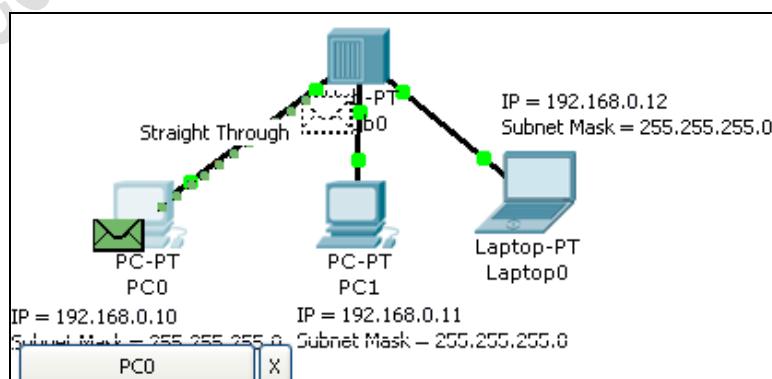
2. ตรวจสอบตาราง ARP ในเครื่องคอมพิวเตอร์ทุกๆ เครื่อง (ARP เป็นโปรโตคอลที่ทำหน้าที่สอบถามว่า หมายเลข IP Address ที่ต้องการติดต่อมีหมายเลข MAC ใด และ Reverse ARP เป็นการสอบถามกลับว่าหมายเลข MAC ที่ต้องการติดต่อตรงกับหมายเลข IP Address ใด) ซึ่งในเบื้องต้นเมื่อยังไม่มีการแลกเปลี่ยนข้อมูลกันระหว่างเครื่องผู้ใช้งาน จะยังไม่มีข้อมูลใดๆ ในตาราง ARP
3. ให้เลือกทำงานในโหมด Simulation เพื่อสังเกตุพฤติกรรมการทำงานของแพ็คเก็ต
4. ที่เครื่อง PC0 คลิกเลือก Desktop  $\Rightarrow$  Command Prompt
5. ใช้คำสั่ง ping ไปยัง IP Address ที่ต้องการทดสอบ ในที่นี้ให้ ping 192.168.0.12 (เครื่อง Laptop0)

```
PC>ping 192.168.0.12
```

6. ในโหมด Simulation แพ็คเก็ตจะหยุดรอให้ผู้ใช้งานเป็น step ได้ โดยการเลือก Capture/Forward
7. คลิก Capture/Forward 1 ครั้ง แพ็คเก็ต ICMP จะวิ่งไปยัง HUB (สังเกตุใน Even List จะเห็นว่ามีแพ็คเก็ต ICMP วิ่งจากเครื่อง PC0 ที่เวลา 0.000 วินาที)

Vis.	Time (sec)	Last Device	At Device	Type	Info
0.000	--	PC0	PC0	ICMP	

ข้อมูลที่เริ่มต้นส่งจาก PC0 คือ ICMP แพ็คเก็ต



#### ทดสอบโดยการ ping เริ่มต้นจาก PC0

8. เมื่อจากคำสั่ง ping นั้นใช้หมายเลข IP Address ในการทดสอบ ณ สถานะการณ์ปัจจุบันเครื่อง PC0 ไม่ทราบว่าเครื่องเป้าหมาย (192.168.0.12) คือใคร เพราะในตาราง

ARP Table ยังไม่มีข้อมูลใดๆ เลย ดังนั้นเครื่อง PC0 จึงส่งแพ็คเก็ต ARP กระจายออกไปยังทุกๆ พอร์ตยกเว้นตัวมันเอง (พอร์ต PC0)

Vis.	Time (sec)	Last Device	At Device	Type	Info
0.000	--	PC0		ICMP	
0.000	--	PC0		ARP	

เวลาที่ 0.000 PC0 ส่งแพ็คเก็ต ARP เพื่อถามว่าใครคือ IP เป้าหมาย (192.168.0.12)

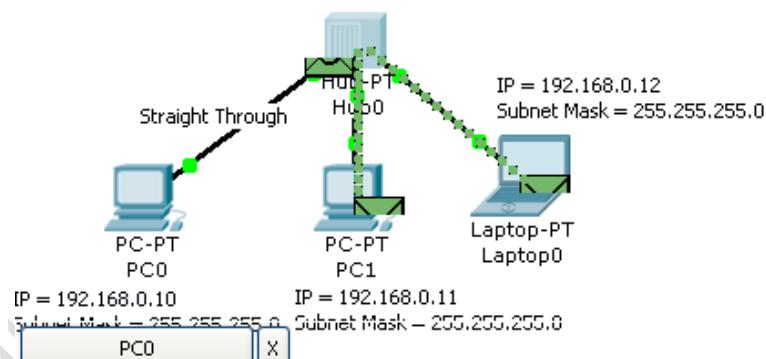
9. แพ็คเก็ต ARP จะส่งต่อไปยัง HUB (เวลา 0.001 ใน Even List )

Vis.	Time (sec)	Last Device	At Device	Type	Info
0.000	--	PC0		ARP	
0.001	--	PC0	Hub0	ARP	

10. HUB จะส่งแพ็คเก็ต ARP ต่อไปยัง PC1 และ Laptop0 พร้อมกัน (เวลา 0.002 ใน Even List)

Vis.	Time (sec)	Last Device	At Device	Type	Info
0.002	--	Hub0	PC1	ARP	
0.002	--	Hub0	Laptop0	ARP	

เวลา 0.002 HUB ส่ง ARP ไปยัง PC1 และ Laptop0 พร้อมกัน



การเดินทางของแพ็คเก็ต ARP

11. Laptop0 จะตอบกลับ ARP reply กลับมา เนื่องจากเป็นเครื่องที่มี IP Address เท่ากับ 192.168.0.12 แต่ เครื่อง PC1 จะไม่ตอบกลับ เพราะไม่ใช่ IP ของตนเอง

Vis.	Time (sec)	Last Device	At Device	Type	Info
0.002	--	Hub0	Laptop0	ARP	
0.003	--	Laptop0	Hub0	ARP	

เวลาที่ 0.003 Laptop0 ส่ง ARP Reply กลับไปให้กับ HUB

12. HUB จะกระจายแพ็คเก็ตที่ส่งมาจาก Laptop0 ไปยังทุกๆ เครื่องเนื่องจากคุณสมบัติของ HUB จะกระจายข้อมูลไปยังทุกๆ พอร์ตเสมอ

Vis.	Time (sec)	Last Device	At Device	Type	Info
0.004	--	Hub0	PC0	ARP	
0.004	--	Hub0	PC1	ARP	

เวลาที่ 0.004 HUB ส่ง ARP Reply ที่ได้รับจาก Laptop0 ไปยังทุกๆ พอร์ต

13. ในเวลาที่ 0.004 เครื่อง PC0 ก็จะทราบแล้วว่า IP 192.168.0.12 คือเครื่องทำการส่ง ICMP ออกไปยังเครื่องเป้าหมายทันที

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.004	Hub0	PC1	ARP	
	0.004	--	PC0	ICMP	

เครื่อง PC0 ทราบแล้วว่าเครื่องเป้าหมายคือเครื่องส่ง ICMP ออกไป เมื่อถึงขั้นตอนนี้ ARP Table ของเครื่อง PC0 และ Laptop0 ก็จะถูก Update ดังนี้

IP Address	Hardware Address (MAC)	Interface
192.168.0.10	0060.5C25.1EC1	FastEthernet

ตาราง ARP Table ของ PC1

IP Address	Hardware Address (MAC)	Interface
192.168.0.10	0060.5C25.1EC1	FastEthernet

ตาราง ARP Table ของ Laptop0

14. เวลาที่ 0.005 เครื่อง PC0 ส่ง ICMP อีกรอบไปยัง HUB

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.004	--	PC0	ICMP	
	0.005	PC0	Hub0	ICMP	

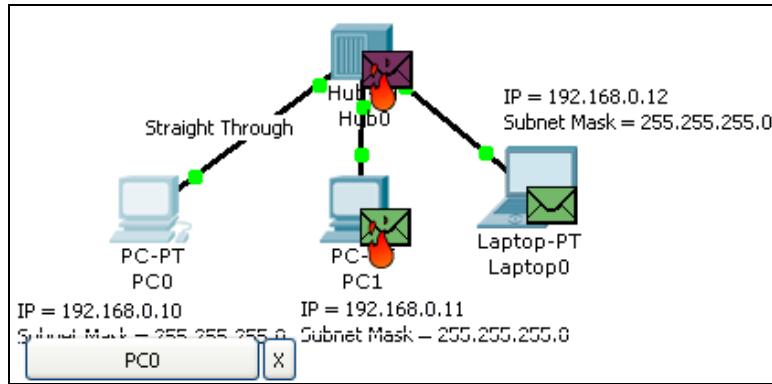
15. เวลาที่ 0.006 HUB จะกระจายแพ็คเก็ต ICMP ไปยังทุกๆ พอร์ต (คุณสมบัติของ HUB)

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.006	Hub0	PC1	ICMP	
	0.006	Hub0	Laptop0	ICMP	

16. เวลาที่ 0.007 Laptop0 ส่งแพ็คเก็ต ICMP reply กลับไปยัง HUB

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.006	Hub0	Laptop0	ICMP	
	0.007	Laptop0	Hub0	ICMP	

Laptop0 Reply ข้อมูลกลับ

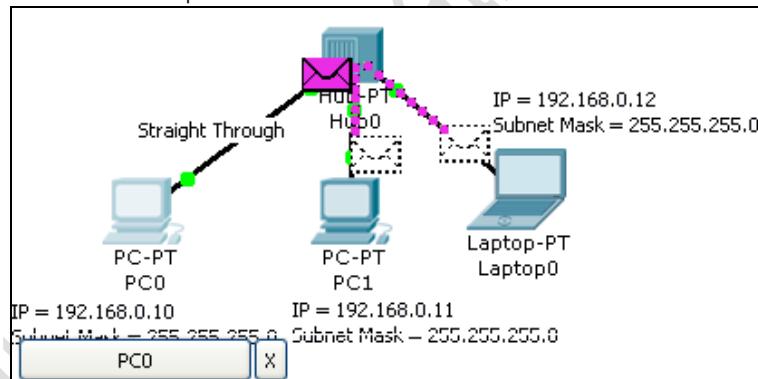


เครื่อง PC1 จะไม่ส่ง ICMP กลับเนื่องจากไม่ใช่เป้าหมาย

17. เวลาที่ 0.008 HUB จะกระจายแพ็คเก็ต ICMP ไปยังทุกๆ พอร์ต (คุณสมบัติของ HUB)

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.008	Hub0	PC0	ICMP	
	0.008	Hub0	PC1	ICMP	

18. การเชื่อมต่อ ก็จะสำเร็จลง เมื่อทำการ ping ครั้งที่ 2 แพ็คเก็ต ก็ยังคงเดินทางไปทางทุกเครื่องเหลือเดิม (ตอบกลับเฉพาะเครื่องที่เป็นเป้าหมายเท่านั้น) เพราะคุณสมบัติของ HUB นั้นจะส่งไปยังทุกๆ พอร์ต แต่จะไม่เกิดกระบวนการ ARP ครั้งที่ 2 จนกว่า จะถึงเวลาที่ ARP Cache expire ซึ่งจะใช้เวลาประมาณ 10 นาที (600 วินาที)



คุณสมบัติของ HUB จะกระจายแพ็คเก็ตไปยังทุกๆ เครื่องหมายเหตุ : ให้ทดลอง ping จากเครื่อง PC0 ไปยัง PC1 อีกครั้งแล้วสังเกตุพฤติกรรมการเปลี่ยนแปลง

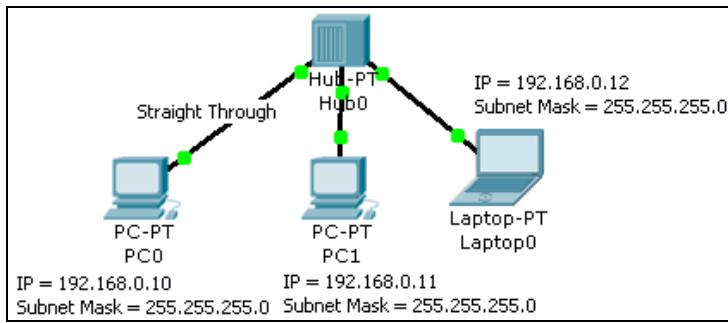


#### Scenario 4: การวิเคราะห์แพ็คเก็ตอย่างละเอียด ตอนที่ 2

คำอธิบาย :

การวิเคราะห์แพ็คเก็ตใน Scenario 3 ได้ทำการวิเคราะห์ทิศทางการส่งข้อมูล สำหรับใน Scenario 4 นี้ จะพิจารณาแพ็คเก็ตในระดับที่ลึกซึ้งลงไปถึงระดับบิตข้อมูล จากตัวอย่างเครือข่ายใน Scenario 2 ให้ปฏิบัติตามขั้นตอนดังนี้

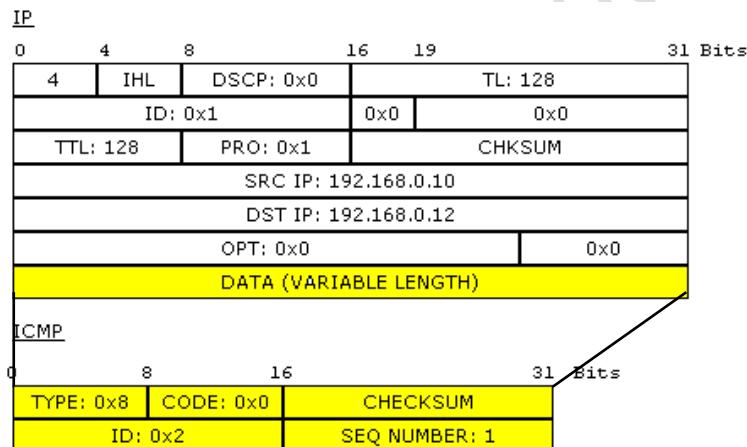
แผนผังการเชื่อมต่อ :



ขั้นตอนการวิเคราะห์ :

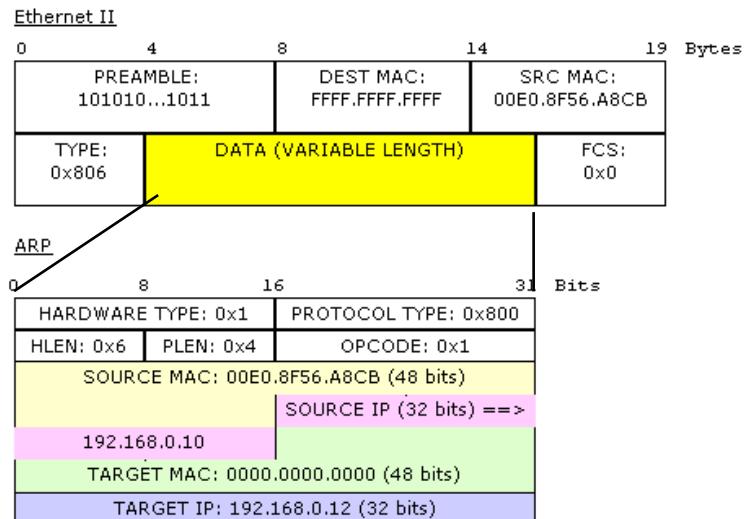
- เริ่มต้นที่เครื่อง PC0 โดยการใช้คำสั่ง ping จาก Command Prompt ไปยังเครื่อง Laptop0 อีกครั้ง
 

PC>ping 192.168.0.12
- ในโหมด Simulation เมื่อออกคำสั่ง ping แล้ว ให้ใช้ Inspect ตรวจสอบแพ็คเก็ต ที่มีรูปเป็นของจดหมาย (สีเขียวคือ ARP และสีเทาคือ ICMP ) โดยการคลิกที่ของจดหมายที่ต้องการ



ตัวอย่างแพ็คเก็ตของ ICMP ที่ซ่อนอยู่ใน IP

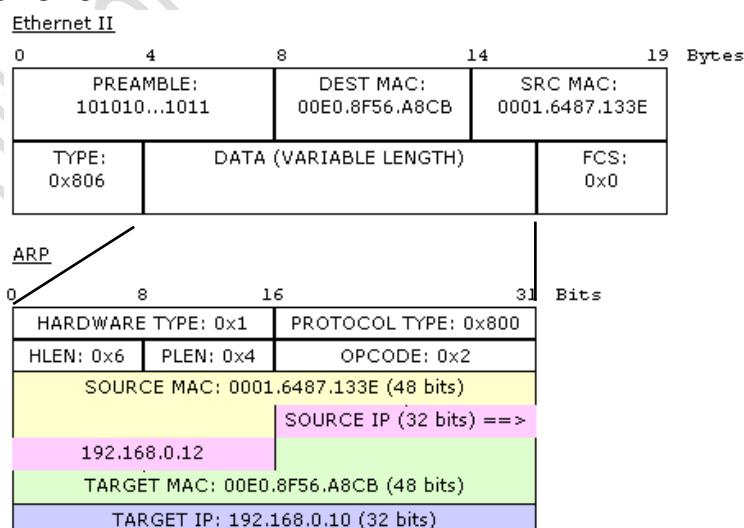
จากรูปข้างบน การสื่อสารข้อมูลในเน็ตเวิร์กจะแบ่งออกเป็นชั้นๆ ตามหลักการของ OSI Model (สามารถอ่านเพิ่มเติมได้ใน เรียนรู้เครือข่ายและอุปกรณ์ Cisco ด้วยโปรแกรม Simulation: ผู้เขียน สุชาติ คุ้มมะณี) จากในตัวอย่าง แพ็คเก็ตของ ICMP นั้นจะถูกซ่อนอยู่ใน IP (encapsulation) เพื่อให้แพ็คเก็ต IP นั้นเป็นผู้ส่งแพ็คเก็ต ICMP ไปให้ถึงปลายทาง ข้อมูลของ ICMP จะเป็นข้อมูลในส่วนของ DATA ใน IP แพ็คเก็ต โดย ICMP แพ็คเก็ตมีขนาดเท่ากับ 32 บิต  $\times$  2 คือ 64 บิต ประกอบไปด้วย Type มีขนาด 8 บิต เอาไว้บอกว่าเป็น โปรโตคอล ICMP ชนิด Echo Request, CODE มีค่าเท่ากับ 0, CHECKSUM เป็นค่าที่ใช้สำหรับตรวจสอบความผิดพลาดของข้อมูล, ID มีค่าเป็น 2, SEQ NUMBER คือลำดับของแพ็คเก็ต ซึ่งจะเปลี่ยนไปเรื่อยๆ ในที่นี้คือ 1



ตัวอย่างแพ็คเก็ต ARP ที่ซ่อนอยู่ในแพ็คเก็ต Ethernet II

จากรูปข้างบน แสดงข้อมูลของแพ็คเก็ต ARP ที่อาศัยพร็อโทคอล Ethernet (ทำงานในレイเยอร์ที่ 2) ส่งไปยังปลายทาง ข้อมูลที่อยู่ใน DATA ของ Ethernet frame จะเป็นแพ็คเก็ตของ ARP มีข้อมูลคือ HARDWARE TYPE=1, PROTOCOL TYPE=0x800, HLEN=ความยาวของ Header, PLEN=ความยาวของเนื้อข้อมูล, OPCODE=0x1, SOURCE MAX=48 บิต, SOURCE IP=32 บิต (192.168.0.10), TARGET MAC=48 บิต (เริ่มต้นจะต้องทำการกระจายข้อมูลไปทุกๆ เครื่อง โดยใช้ MAC=000.000.000), TARGET IP=32 บิต (192.168.0.12) สังเกตว่าใน Ethernet frame จะ DEST MAC= FFF.FFF.FFF แสดงว่าเป็นการ broadcast ข้อมูลไปทุกๆ เครื่อง

- เมื่อเครื่องปลายทางได้รับแพ็คเก็ตแล้วจะส่ง ARP Reply กลับไปยังเครื่องที่ส่งข้อมูลมาโดยการ update ค่า SOURCE MAC, SOURCE IP, TARGET MAC, TARGET IP ใน ARP frame คือ



ค่าของ SOURCE IP เป็น 192.168.0.10 และ TARGET IP เป็น 192.168.0.12 เมื่อตอบกลับ จะสลับค่าเป็น SOURCE IP เป็น 192.168.0.12 และ TARGET IP เป็น 192.168.0.10 เช่นเดียวกัน ค่าของ MAC ก็จะสลับตามหมายเลข IP สำหรับแพ็คเก็ตอื่นๆ ก็จะสามารถสังเกตได้ด้วยวิธีการเดียวกัน

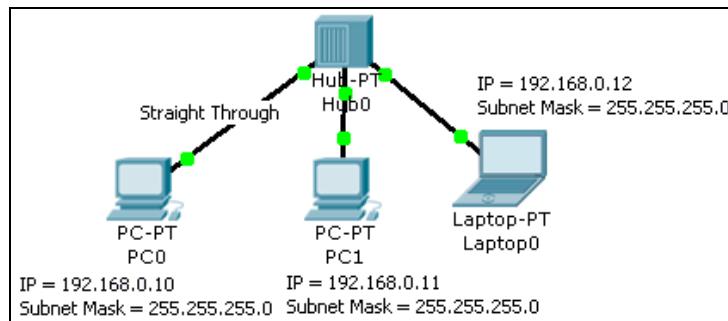


### Scenario 5: หลักการทำงานของ ARP โพรโทคอล

คำอธิบาย :

ARP เป็นโพรโทคอลที่มีความสำคัญมากในการสื่อสารข้อมูล และเป็นจุดอ่อนที่ Hacker นิยมใช้การดักจับข้อมูลด้วย ดังนั้นใน Scenario นี้จะมาทดลองวิเคราะห์แพ็คเก็ตของ ARP กันว่ามีหลักการทำงานเป็นอย่างไร

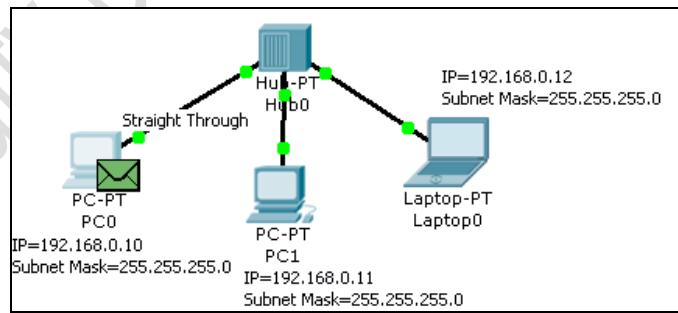
แผนผังการเชื่อมต่อ :



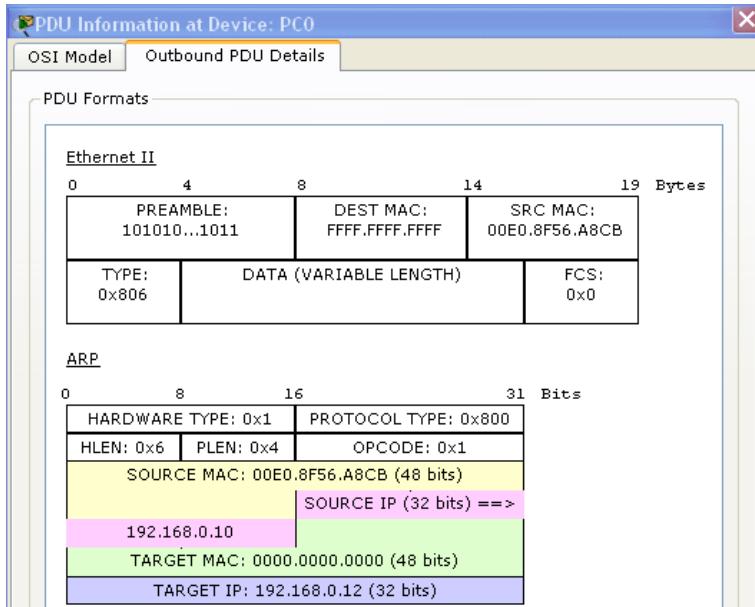
ขั้นตอนการวิเคราะห์ :

- เริ่มต้นให้เลือกที่โหมด Simulation ก่อน เครื่อง PC0 ให้ใช้คำสั่ง ping จาก Command Prompt ไปยังเครื่อง Laptop0 (จาก IP 192.168.0.10 ไปยัง 192.168.0.12)
 

```
PC>ping 192.168.0.12
```
- ในส่วน Event List Filters ให้เลือก Edit Filters  $\Rightarrow$  คลิกบล็อกช์ Show All/None ออก  $\Rightarrow$  คลิกบล็อกช์ ARP เพียงโพรโทคอลเดียวเท่านั้น เมื่อออค่าสั่ง ping แล้ว ให้ใช้ Inspect ตรวจสอบแพ็คเก็ต ที่มีรูปเป็นซอง สีเขียวคือ ARP █ โดยการคลิกที่ซองจะหมายที่ต้องการ

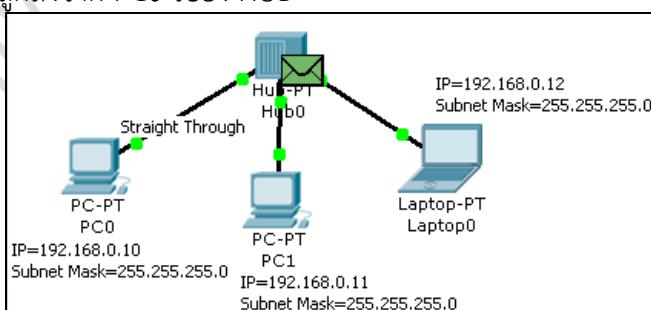


PC0 จะเริ่มส่ง ARP request ออกไปบนเน็ตเวิร์คเพื่อค้นหาว่าเครื่องใด คือ IP 192.168.0.12



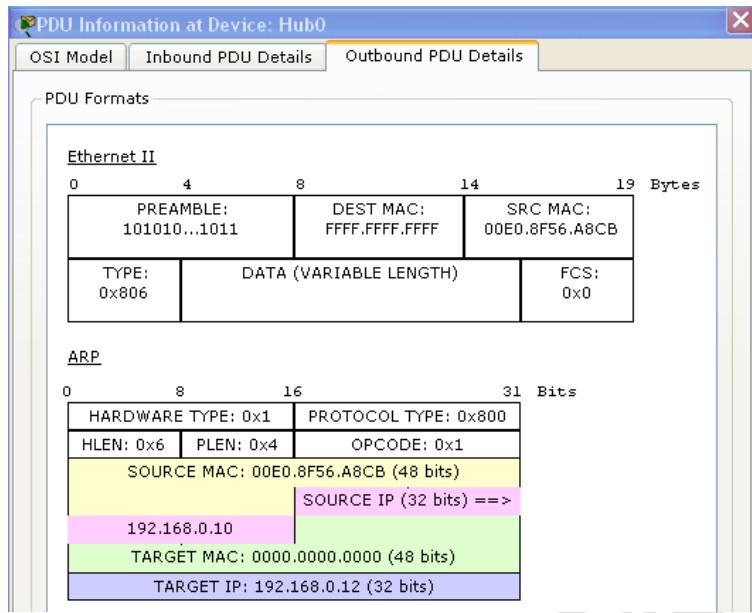
ข้อมูลของแพ็คเก็ตในเลเยอร์ที่ 2 ขาออก (Outbound PDU ของ การ์ดเน็ตเวิร์ค PC0) ประกอบไปด้วย Ethernet frame และ ARP frame ที่ซ่อนอยู่ใน DATA ของ Ethernet frame ข้อมูลใน Ethernet frame ที่สำคัญคือ DEST MAC มีค่าเป็น FFF.FFF.FFF คือการถ่ายไปยังทุกๆ เครื่องในเครือข่าย (broadcast frame) ว่าใครที่มีหมายเลข IP เป็น 192.168.0.12 (อยู่ใน TARGET IP ของ ARP frame) และ SRC MAC แสดงถึง MAC Address ของผู้ส่งข้อมูล (ในที่นี้คือ PC0=00E0.8F56.A8CB) สำหรับใน ARP frame เป็นต้นจะระบุเฉพาะค่า SOURCE MAC=00E0.8F56.A8CB, SOURCE IP=192.168.0.10 ซึ่งเป็นเครื่อง PC0 ที่ส่งข้อมูลออกมา และรู้ว่าจะต้องส่งไปที่ IP 192.168.0.12 (TARGET IP) แต่ไม่รู้ว่าเป้าหมายเป็น MAC Address หมายเลขใด (TARGET MAC=000.000.000) จึงต้องอาศัยให้ Ethernet frame ส่งข้อมูลกระจายไปทั้งเครือข่าย เพื่อให้คนที่มีหมายเลข IP 192.168.0.12 ตอบกลับมา

### 3. แพ็คเก็ตจะถูกส่งจาก PC0 ไปยัง HUB

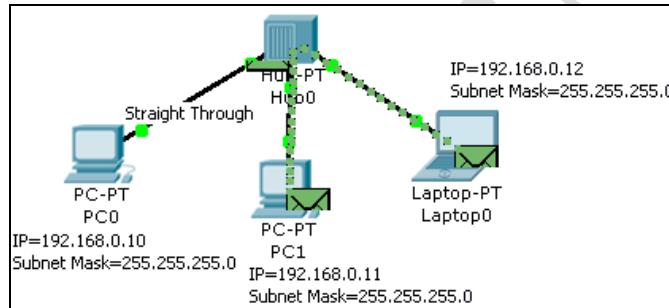


แพ็คเก็ต Ethernet และ ARP จะถูกส่งจาก PC0 ไปยัง HUB

ข้อมูลที่ HUB รับเข้ามาเรียกว่า Inbound PDU และ ส่งออกจาก HUB เรียกว่า Outbound PDU ซึ่งในสถานะตอนนี้จะมีความนิยมกันทุกประการ



4. แพ็คเก็ตจะถูกส่งออกจาก HUB ไปยังทุกๆ พอร์ตพร้อมกัน ยกเว้นพอร์ตที่รับแพ็คเก็ตเข้ามา เพื่อค้นหาว่า MAC Address ของ IP 192.168.0.12 คือเครื่องใด



ส่งเฟรมข้อมูลกระจายแบบ Broadcast

เครื่อง Laptop0 ซึ่งเป็นเจ้าของ IP ดังกล่าวตอบกลับด้วย ARP Reply พร้อมกับ update ข้อมูลใน frame Ethernet และ ARP ดังนี้  
เครื่อง Laptop0 แพ็คเก็ตขาเข้า

#### Inbound PDU

##### Ethernet frame

SRC MAC=00E0.8F56.A8CB (เครื่อง PC0)

DEST MAC=FFFF.FFFF.FFFF (ทุกๆ เครื่อง)

##### ARP frame

SOURCE MAC: 00E0.8F56.A8CB (เครื่อง PC0)

TARGET MAC: 0000.0000.0000 (ยังไม่ทราบว่าเครื่องใด)

OPCODE: 0x1 (ARP Request)

SOURCE IP=192.168.0.10 (IP เครื่อง PC0)

TARGET IP: 192.168.0.12 (IP เครื่อง Laptop0)

เครื่อง Laptop0 แพ็คเก็ตขาออก

#### Outbound PDU

## Ethernet frame

SRC MAC= 0001.6487.133E (เครื่อง Laptop0)

DEST MAC=00E0.8F56.A8CB (เครื่อง PC0)

## ARP frame

SOURCE MAC: 0001.6487.133E (เครื่อง Laptop0)

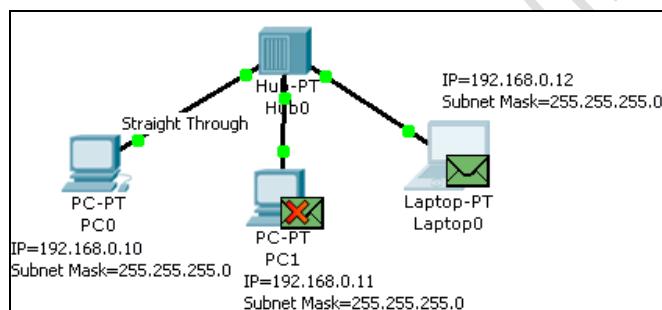
TARGET MAC: 00E0.8F56.A8CB (เครื่อง PC0)

OPCODE: 0x2 (ARP Reply)

SOURCE IP=192.168.0.10 (IP เครื่อง PC0)

TARGET IP: 192.168.0.12 (IP เครื่อง Laptop0)

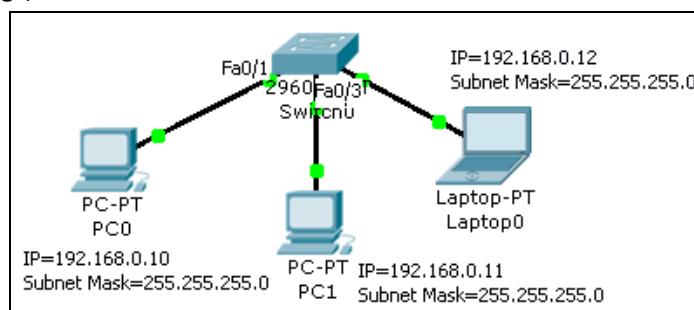
5. เมื่อแพ็คเก็ตเดินทางจาก Laptop0 กลับไปยัง HUB เพื่อกลับไปให้เครื่องที่เรียกมา คือ PC1, HUB จะทำการกระจายข้อมูลที่รับมาจาก Laptop0 ไปยังทุกๆ พอร์ตตามหน้าที่ของมัน แต่เครื่อง PC1 จะไม่รับแพ็คเก็ตดังกล่าว เนื่องจากไม่ใช่ IP ที่แพ็คเก็ตต้องการ ส่งให้ แต่สำหรับเครื่อง PC1 จะรับแพ็คเก็ตดังกล่าวไว้ เป็นอันจบกระบวนการของ ARP

**Scenario 6:** เชื่อมต่อคอมพิวเตอร์ PC, Laptop กับ Switch L2 (เลเยอร์ 2)

คำอธิบาย :

การเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์มากกว่า 2 เครื่องขึ้นไป โดยใช้อุปกรณ์ HUB นั้นไม่มีความปลอดภัย เนื่องจาก HUB จะกระจายข้อมูลที่รับเข้ามาออกไปยังทุกๆ พอร์ต ดังนั้นจึงเป็นเครื่องมือที่ Hacker นิยมใช้ในการดักจับข้อมูล ซึ่งแตกต่างจากอุปกรณ์ประเภทสวิตช์ที่ไม่มีการกระจายข้อมูลไปยังเครื่องลูกข่าย ซึ่งจะช่วยลดปัญหาการดักจับข้อมูลได้ระดับหนึ่ง

แผนผังการเชื่อมต่อ :



รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask	Interface Type	Cable Type
---------	------------	-------------	----------------	------------

PC0	192.168.0.10	255.255.255.0	FastEthernet	Straight-Through
PC1	192.168.0.11	255.255.255.0	FastEthernet	Straight-Through
Laptop0	192.168.0.12	255.255.255.0	FastEthernet	Straight-Through
Switch0	-	-	FastEthernet0/1 to PC0 FastEthernet0/2 to PC1 FastEthernet0/3 to Laptop0	Straight-Through

ขั้นตอนการเชื่อมต่อ :

8. เลือก End Devices  (ในส่วน Device-Type)
9. เลือก Generic  (ในส่วน Device-Specific) และลากมาวางใน workspace ให้ครบ 2 เครื่อง (โดยปกติจะมีชื่อเป็น PC0, PC1 ตามลำดับ)
10. เลือก Laptop-PT  (ในส่วน Device-Specific) และลากมาวางใน workspace
11. เลือก Connections  (ในส่วน Device-Type)
12. เลือก Copper Straight-Through  (ในส่วน Device-Specific) และคลิกที่เครื่อง PC0 ไปยัง HUB และ PC1, Laptop0 ไปยัง Switch0 ตามลำดับ ที่เครื่องคอมพิวเตอร์ จะปรากฏไฟสีเขียว (ถ้าไฟเป็นสีน้ำเงินแสดงว่ายังอยู่ในช่วงการเชื่อมต่ออยู่ รอประมาณ 30 วินาที) แสดงว่าเชื่อมต่อสำเร็จ
13. คลิกที่ PC0, PC1 และ Laptop0 ที่ลักษณะในแต่ละเครื่องเลือกแท็บ Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  Static  $\Rightarrow$  กำหนดค่าหมายเลข IP Address และ Subnet Mask ดังตารางด้านล่าง

เครื่อง	IP Address	Subnet Mask
PC0	192.168.0.10	255.255.255.0
PC1	192.168.0.11	255.255.255.0
Laptop0	192.168.0.12	255.255.255.0

14. เสร็จสิ้นการเชื่อมต่อ

การทดสอบ :

1. ที่เครื่อง PC0 เลือก Desktop  $\Rightarrow$  Command Prompt
2. เมื่อปรากฏหน้าต่าง Command Prompt ให้ผู้ใช้ออกคำสั่งทดสอบคือ ping หมายเลข IP Address 192.168.0.12
 

PC>ping 192.168.0.12
3. เครื่องที่ถูก ping จะตอบกลับด้วย ICMP Reply เมื่อเครื่องปลายทางทำงานปกติ แต่ถ้า ping แล้ว ผลที่ได้รับคือ Request timed out แสดงว่าเครื่องปลายทางไม่ได้ทำงาน

```

Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.12

Pinging 192.168.0.12 with 32 bytes of data:

Reply from 192.168.0.12: bytes=32 time=109ms TTL=128
Reply from 192.168.0.12: bytes=32 time=47ms TTL=128
Reply from 192.168.0.12: bytes=32 time=47ms TTL=128
Reply from 192.168.0.12: bytes=32 time=31ms TTL=128

Ping statistics for 192.168.0.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 109ms, Average = 58ms

PC>

```

กราฟีฟดทดสอบ ping สำเร็จ

```

Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.13

Pinging 192.168.0.13 with 32 bytes of data:

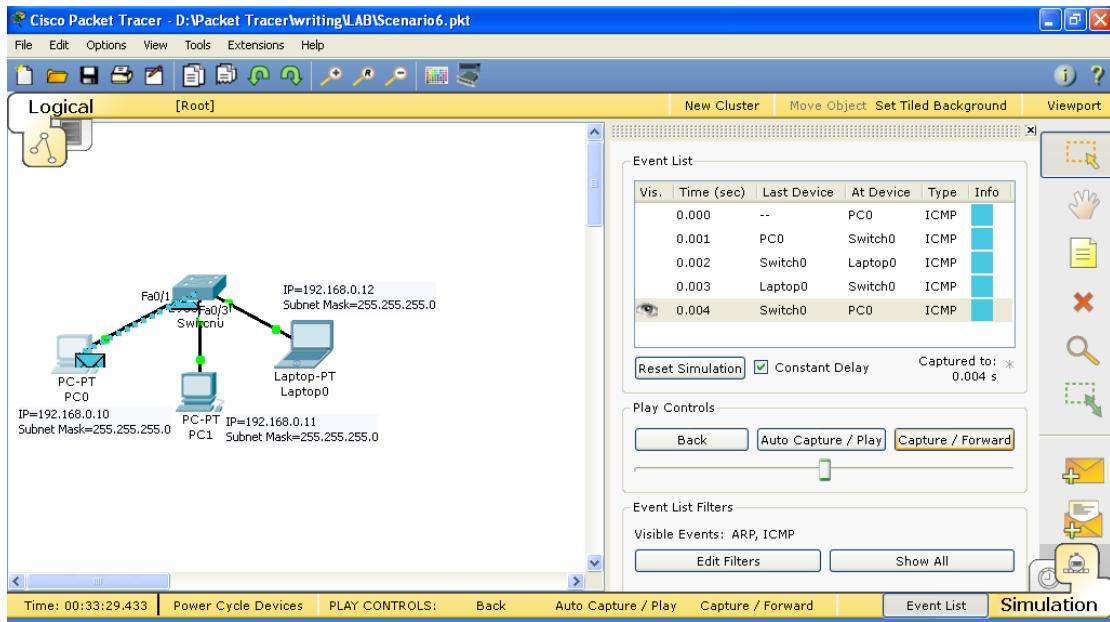
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>

```

กราฟีฟดทดสอบ ping ไม่สำเร็จ

4. ลองทดสอบด้วย ping อีกครั้ง ในโหมด Simulation สังเกตุพฤติกรรมการทำงานใน Even List ปรากฏว่าแพ็คเก็ตจะไม่กระจายไปยังทุกๆ พортเมื่อൺกราฟีของ HUB ทำให้ข้อมูลที่ส่งและรับมีความปลดภัยเพิ่มขึ้น



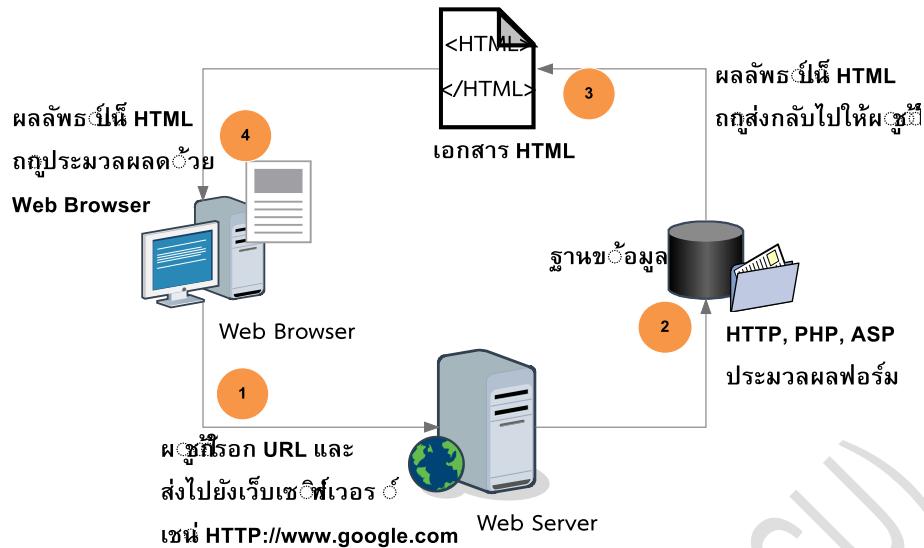
การทดสอบด้วย ping ในโหมด Simulation

### Scenario 7: การติดตั้งเว็บเซิร์ฟเวอร์ (Web Server : HTTP)

คำอธิบาย :

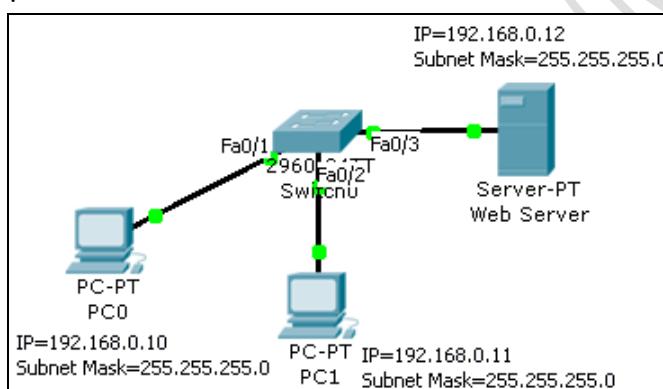


เว็บเซิร์ฟเวอร์ (Web Server) คือ เครื่องคอมพิวเตอร์ที่ทำหน้าที่ให้บริการเว็บ เพื่อให้แก่ผู้ร้องขอ ด้วยโปรแกรมประเภทเว็บบราวเซอร์ (Web Browser เช่น Internet Explorer, FireFox เป็นต้น) โดยร้องขอข้อมูลผ่านโปรโตคอลเอชทีพี (HTTP = Hyper Text Transfer Protocol) เครื่องผู้ให้บริการจะส่งข้อมูลให้กับผู้ร้องขอในรูปของข้อความ ภาพ เสียง หรือสื่อผสม (Multimedia) เครื่องให้บริการเว็บจะเปิดพอร์ต 80 (เป็นพอร์ตที่นิยม แต่ผู้ให้บริการก็สามารถเปลี่ยนเป็นพอร์ตอื่นๆ ก็ได้ เช่น 8080 เป็นต้น) เครื่องผู้ใช้ริมการเข้ามายังต่อโดยการระบุที่อยู่เว็บเพจที่ร้องขอ (Web Address หรือ URL = Uniform Resource Locator) เช่น <http://www.google.co.th> เป็นต้น สำหรับโปรแกรมที่นิยมใช้เป็นเครื่องให้บริการเว็บ เช่น Apache Web Server, IIS (Internet Information Server) เป็นต้น หลักการทำงานดังแสดงในภาพด้านล่าง



ขั้นตอนการทำงานของเว็บเซิร์ฟเวอร์

แผนผังการเชื่อมต่อ :



รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask	Interface Type	Cable Type
PC0	192.168.0.10	255.255.255.0	FastEthernet	Straight-Through
PC1	192.168.0.11	255.255.255.0	FastEthernet	Straight-Through
Server-PT	192.168.0.12	255.255.255.0	FastEthernet	Straight-Through
Switch0	-	-	FastEthernet0/1 to PC0 FastEthernet0/2 to PC1 FastEthernet0/3 to Server-PT	Straight-Through

ขั้นตอนการเชื่อมต่อ :

1. เลือก End Devices (ในส่วน Device-Type)
2. เลือก Generic (ในส่วน Device-Specific) และลากมาวางใน workspace ให้ครบ 2 เครื่อง (โดยปกติจะมีชื่อเป็น PC0, PC1 ตามลำดับ)
3. เลือก Server-PT (ในส่วน Device-Specific) และลากมาวางใน workspace
4. เลือก Connections (ในส่วน Device-Type)

5. เลือก Copper Straight-Through  (ในส่วน Device-Specific) แล้วคลิกที่เครื่อง PC0 ไปยัง HUB และ PC1, Server-PT ไปยัง Switch0 ตามลำดับ ที่เครื่องคอมพิวเตอร์ จะปรากฏไฟสีเขียว (ถ้าไฟเป็นสีส้มแสดงว่ายังอยู่ในช่วงการเชื่อมต่ออยู่ รอประมาณ 30 วินาที) แสดงว่าเชื่อมต่อสำเร็จ

6. คลิกที่ PC0, PC1 ที่จะเครื่อง ในแต่ละเครื่องเลือกแท็บ Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  Static  $\Rightarrow$  กำหนดค่าหมายเลข IP Address และ Subnet Mask ดังตารางด้านล่าง

เครื่อง	IP Address	Subnet Mask
PC0	192.168.0.10	255.255.255.0
PC1	192.168.0.11	255.255.255.0

7. ทำการ Enable Web Server โดยเลือกที่ Desktop  $\Rightarrow$  Config  $\Rightarrow$  เลือกแท็บ HTTP  $\Rightarrow$  ตรวจสอบ HTTP และ HTTPS อยู่ในสถานะ On หรือยัง ถ้ายังให้เลือกเป็น On
8. เครื่อง HTTP จะมีไฟล์ 3 ไฟล์ให้ผู้ใช้งานสามารถปรับแต่งได้ ซึ่งเขียนภาษา HTML คือไฟล์ index.html, helloworld.html, image.html ผู้ใช้งานสามารถแก้ไขได้ เช่น ในไฟล์ index.html จาก HTML <center><font size='+2' color='blue'>Cisco Packet Tracer</font></center> ทดสอบแก้ไขเป็น <center><font size='+2' color='blue'>Hello Network Simulation 2</font></center> เป็นต้น
9. ในแท็บ Desktop เลือก IP Configuration กำหนดค่าดังต่อไปนี้

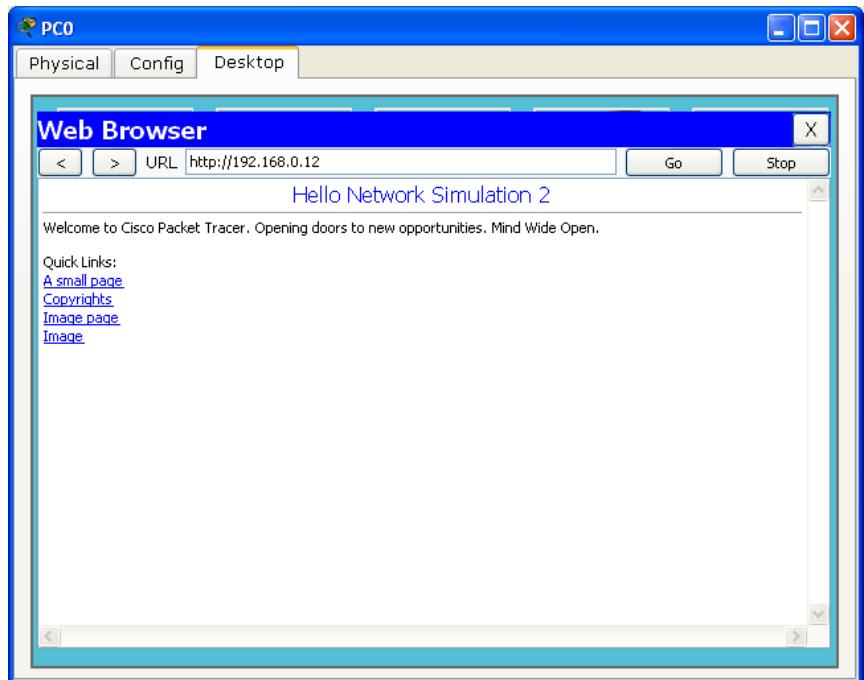
IP Address = 192.168.0.12

Subnet Mask = 255.255.255.0

10. เสร็จสิ้นการเชื่อมต่อ

การทดสอบ :

1. ให้ทำการทดสอบเว็บเซิร์ฟเวอร์ โดยการคลิกที่ PC0  $\Rightarrow$  Desktop  $\Rightarrow$  Web Browser  $\Rightarrow$  ให้กรอกในช่อง URL เป็น http://192.168.0.12 (ยังไม่สามารถเรียกแบบชื่อได้ เช่น [www.google.co.th](http://www.google.co.th) เนื่องจากยังไม่มีการติดตั้ง DNS) แล้วกดปุ่ม Go ดังรูปด้านล่าง



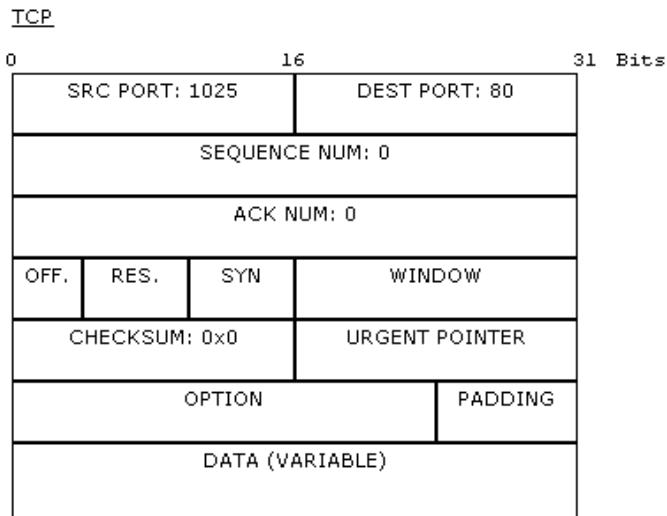
เมื่อทุกอย่างค่อนข้างถูกต้อง โปรแกรม Browser ของเครื่อง PC0 จะแสดงผลที่ส่งมาจาก Web Server ได้ถูกต้อง

การวิเคราะห์แพ็คเก็ต HTTP:

1. เลือกการทำงานเป็นโหมด Simulation
2. สำรวจตาราง ARP Table ของ PC0, PC1, Server-PT และ Switch0 โดยใช้ Inspect (ในเบื้องต้นจะต้องไม่มีการเก็บข้อมูลใดๆ ในตารางดังกล่าว) สำหรับ Port Status ต้องมีสถานะเป็น up
3. คลิกเลือก PC0  $\Rightarrow$  Desktop  $\Rightarrow$  Web Browser  $\Rightarrow$  ป้อน URL เป็น <http://192.168.0.12> แล้วกดปุ่ม Go
4. แพ็คเก็ตจะหยุดรอให้ผู้ใช้ควบคุมการทำงานของแพ็คเก็ต โดยผู้ใช้เลือกเป็น Capture/Forward เป็นการเลือกการทำงานแบบ Step by Step
5. ข้อมูลใน Even List จะเห็นว่าแพ็คเก็ตจะถูกส่งออกมาร่วมกัน 2 ประเภทคือ TCP/IP (แพ็คเก็ตของ HTTP ซึ่งใช้ port 80) และแพ็คเก็ตที่ 2 คือ ARP โปรโทคอล

IP										31 Bits	
0	4	8	16	19							
4	IHL	DSCP: 0x0		TL: 44							
			ID: 0x1	0x2		0x0					
TTL: 128		PRO: 0x6		CHKSUM							
		SRC IP: 192.168.0.10									
		DST IP: 192.168.0.12									
		OPT: 0x0			0x0						
		DATA (VARIABLE LENGTH)									

แพ็คเก็ต IP ทำหน้าที่ส่งข้อมูลไปในเส้นทางที่ดีที่สุดบนเครือข่าย พิลด์ที่สำคัญประกอบไปด้วย SRC IP คือ IP ต้นทางที่ต้องการร้องขอจากเว็บเซิร์ฟเวอร์ (192.168.0.10), DST IP คือ IP ของเครื่องเว็บเซิร์ฟเวอร์ (192.168.0.12) ข้อมูลที่อยู่ใน DATA คือ แพ็คเก็ตของ TCP



สำหรับแพ็คเก็ต TCP ทำหน้าที่ส่งข้อมูลให้ครบและถูกต้อง ฟิลด์ที่สำคัญได้แก่ SRC PORT เป็นหมายเลขพอร์ตต้นทางของเครื่องผู้ใช้ (PC0), DEST PORT เป็นหมายเลขพอร์ตที่ต้องการ เชื่อมต่อบนเครื่องเว็บเซิร์ฟเวอร์ (พอร์ต 80), SEQUENCE NUM คือลำดับการส่งข้อมูลของแพ็คเก็ต, ACK NUM หมายถึง สถานะการทำงาน, WINDOW คือ จำนวนขนาดของหน้าต่างที่ใช้รับส่งข้อมูล, DATA เป็นส่วนที่ใช้เก็บข้อมูลของแพ็คเก็ตของโพรโทคอล HTTP (เว็บ)

6. สำหรับใน Switch0 นั้นเริ่มต้นค่าในตารางต่างๆ เช่น ARP, MAC, QoS Queues จะ ว่างเปล่า แต่ Port Status จะมีสถานะเป็น up ทั้งหมด 3 ports คือ FastEthernet 0/1 (ต่อ กับ PC0), FastEthernet 0/2 (PC1) และ FastEthernet 0/3 (Web Server)

7. กดปุ่ม Capture/Forward อีกครั้ง พร้อมสังเกตุแพ็คเก็ตที่ปรากฏในแท็บ Event List ข้อสังเกตุ : แพ็คเก็ตของ HTTP จะยังไม่สามารถทำงานได้ในทันที จำเป็นต้องให้กระบวนการของ ARP เสร็จสิ้นก่อน (อ่านเพิ่มเติมในหัวข้อ หลักการทำงานของ ARP)

8. สำหรับข้อมูลในฟิลด์ของ DATA ในแพ็คเก็ต TCP นั้นคือ ข้อมูลของแพ็คเก็ต HTTP ซึ่ง ประกอบไปด้วย วิธีการเชื่อมต่อ เช่น Get หรือ Post, ชื่อไฟล์ที่ต้องการแสดงผล (index.html), เวอร์ชันของ HTTP (1.1), ภาษาที่ใช้สื่อสาร (Accept-Language: us-en), สถานะการเชื่อมต่อ (Connection: close), หมายเลข IP ที่ต้องการเชื่อมต่อ (Host: 192.168.0.12) เป็นต้น

```
HTTP
Get /index.html HTTP/1.1
Accept-Language: us-en
Accept: /*
Connection: close
Host: 192.168.0.12
```

HTTP
<pre>HTTP/1.1 200 OK Connection: close Content-Length: 364 Content-Type: text/html Server: PT-Server/5.2 HTTP DATA..</pre>

ตัวอย่างข้อมูลในแพ็คเก็ต HTTP

9. เมื่อการร้องขอบริการเว็บทำงานสำเร็จลง ข้อมูลต่างๆ ในอุปกรณ์จะมีสถานะดังนี้

PC0 (Web Browser)

ARP Table			
IP Address	MAC Address	Interface	Comment
192.168.0.12	0030.A398.4866	FastEthernet	เครื่อง Web Server

Server-PT (Web Server)

ARP Table			
IP Address	MAC Address	Interface	Comment
192.168.0.10	000A.4193.A5E1	FastEthernet	เครื่อง PC0

Switch0

ARP Table			
VLAN	MAC Address	Port	Comment
1	000A.4193.A5E1	FastEthernet0/1	เครื่อง PC0
1	0030.A398.4866	FastEthernet0/3	เครื่อง Web Server



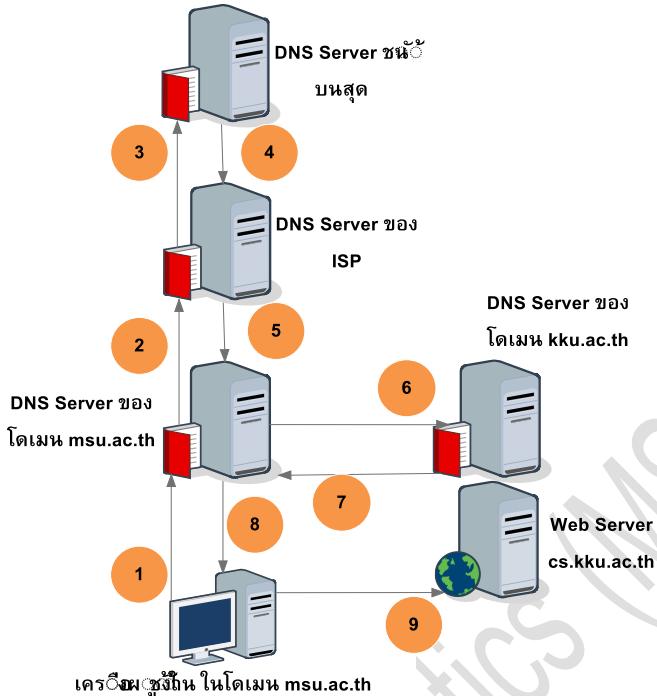
### Scenario 8: การติดตั้งโดเมนเนมเซิร์ฟเวอร์ (DNS)

คำอธิบาย :



DNS ย่อมาจาก Domain Name System หมายถึง ระบบใช้สำหรับอ้างถึงหมายเลขอร่อง หรือหมายเลขอาร์ที่ IP Address เข้ากับชื่อของเว็บไซต์ เพื่อให้ง่ายต่อการจดจำ DNS จะทำหน้าที่คล้ายกับสมุดโทรศัพท์ คือเมื่อมีผู้ใช้ต้องการจะโทรศัพท์หาบุคคลใด บุคคลหนึ่ง จะต้องเปิดสมุดโทรศัพท์เพื่อค้นหาเบอร์โทรศัพท์ของบุคคลที่ต้องการจะติดต่อด้วย คอมพิวเตอร์ก็เช่นกัน เมื่อต้องการจะสื่อสารกับคอมพิวเตอร์เครื่องอื่น เครื่องนั้นก็จะทำการสอบถามหมายเลขอาร์ที่ IP ของเครื่องที่ต้องการจะสื่อสาร กับ DNS server ซึ่งจะทำการค้นหาหมายเลขอาร์ทก่อน การเชื่อมต่อสื่อสารระหว่างคอมพิวเตอร์ในระบบ internet นั้นใช้มาตรฐาน TCP/ IP ที่เครื่องคอมพิวเตอร์นั้นต้องมีหมายเลขอาร์ทที่ไม่ซ้ำกัน โดยปกติเครื่อง Web Server จำเป็นต้องมี IP Address เสมอ จึงเกิดปัญหานี้ในการจำ เพราะว่า IP Address มีตัวเลขถึง 12 ตัว จำกัดนี้จึงได้มีการคิดที่จะแปลง IP Address ให้เป็นชื่อที่จำได้ง่าย เช่น IP Address "64.233.181.106" เรียกเป็น

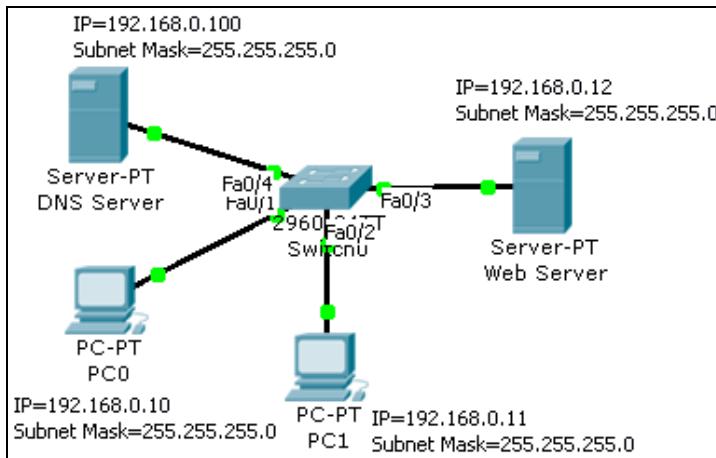
HTTP://www.google.co.th" (กูเกิล) เป็นต้น สำหรับลำดับการทำงานของ DNS มีขั้นตอนดังรูปด้านล่าง



#### ขั้นตอนการทำงานของ DNS เซิร์ฟเวอร์

1. เครื่องผู้ใช้หรือ client อยู่ในโดเมน msu.ac.th ร้องขอบริการเว็บชื่อว่า cs.kku.ac.th ซึ่งจะค้นหาในเครื่องของตนเองก่อน (local DNS ในวินโดวส์จะเก็บใน \system32\drivers\etc\hosts, linux อยู่ใน /etc/resolv.conf) เมื่อค้นหามา不及จะสอบถามไปที่ DNS ของหน่วยงานของตนเองก่อน
2. เมื่อค้นหานอกจาก local DNS แล้ว ไม่พบ DNS ของ ISP ที่เชื่อมต่ออยู่ในระดับที่สูงขึ้น
3. สมมุติว่าค้นหาที่ ISP ก็ไม่เจอ จะส่งการร้องขอไปยัง Root DNS ซึ่งให้บริการอยู่ทั่วโลก โดยปกติจะต้องเจอ ถ้าไม่เจอแสดงว่าชื่อที่ค้นหามาไม่มีในโดเมนนี้
4. Root DNS จะส่งที่อยู่ของ DNS ที่ ISP บริหารโดเมน kku.ac.th อยู่กลับมา
5. DNS ของ msu.ac.th ทราบว่า kku.ac.th อยู่ที่ไหน
6. DNS ของ msu.ac.th ส่งคำร้องขอไปยัง kku.ac.th
7. kku.ac.th จะตอบกลับเป็นหมายเลข IP ของ cs.kku.ac.th กลับมาให้
8. ได้รับหมายเลข IP ของ cs.kku.ac.th
9. เชื่อมต่อไปยัง Web Server ดังกล่าวด้วยหมายเลข IP ที่ได้รับมา

แผนผังการเชื่อมต่อ :

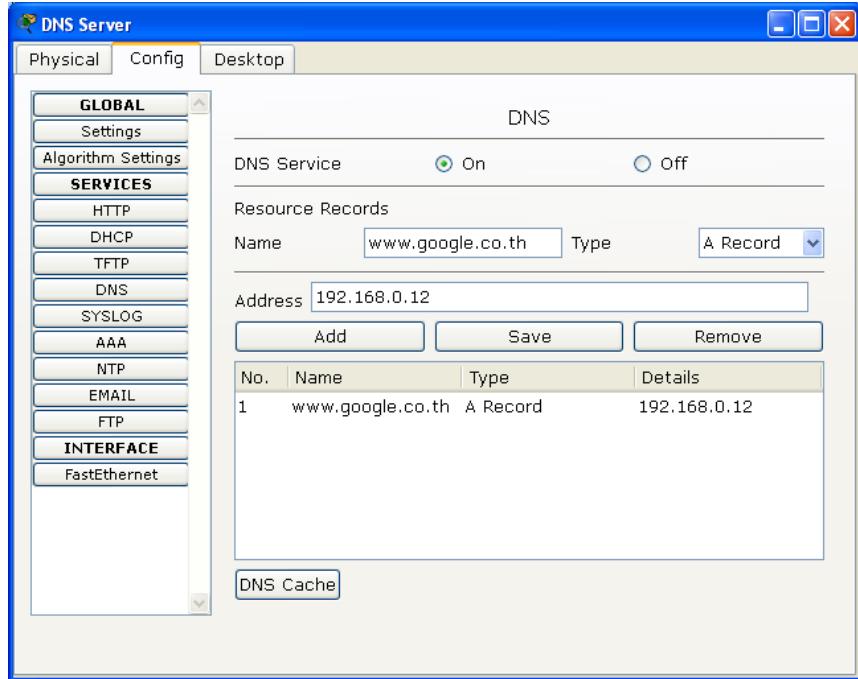


รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask	Interface Type
PC0	192.168.0.10	255.255.255.0	FastEthernet
PC1	192.168.0.11	255.255.255.0	FastEthernet
Web Server	192.168.0.12	255.255.255.0	FastEthernet
DNS Server	192.168.0.100	255.255.255.0	FastEthernet
Switch0	-	-	FastEthernet0/1 to PC0 FastEthernet0/2 to PC1 FastEthernet0/3 to Web Server FastEthernet0/4 to DNS Server

ขั้นตอนการเชื่อมต่อ :

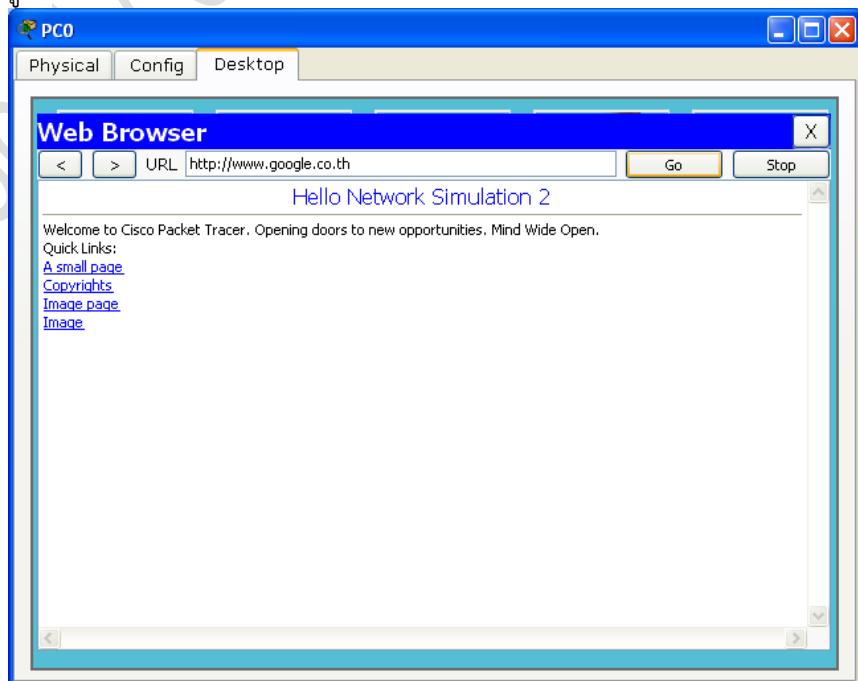
- ให้ทำการเชื่อมต่อ PC0, PC1, Web Server เมื่อ้อนกับ Scenario 7
- สำหรับเครื่อง DNS Server ให้ทำการคุณพิก IP Address โดยเลือกที่ Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนด IP ดังนี้
  - IP Address = 192.168.0.100
  - Subnet Mask = 255.255.255.0
- ทำการ Enable DNS Server โดยเลือกที่ Desktop  $\Rightarrow$  Config  $\Rightarrow$  เลือกแท็บ DNS  $\Rightarrow$  ตรวจสอบ DNS Service อยู่ในสถานะ On หรือยัง ถ้ายัง ให้เลือกเป็น On
- ในส่วน Resource Records ฟิลด์ Name ให้ใส่ชื่อของเว็บไซต์ฟาร์ม ในที่นี้ทดลองใช้ เป็น [www.google.co.th](http://www.google.co.th), ฟิลด์ Type ให้เลือกเป็น A Record (A Record=ระบุว่าเป็น Host, CNAME=ชื่อที่ใช้เรียกแทน คล้ายชื่อเล่น, SOA=นำเสนอแหล่งที่มาหลักข้อมูล เกี่ยวกับชื่อของ zone server, admin's email, flags และ Timeout, NS Record= ทำการระบุ Name Server)
- ในฟิลด์ Address ให้ใส่หมายเลข IP Address ที่ต้องการใช้งาน ในที่นี้ใช้ IP 192.168.0.12 แปลงเป็นชื่อ [www.google.co.th](http://www.google.co.th) และคลิกปุ่ม Add ดังรูป



6. ทำการกำหนดค่า DNS Server ในเครื่อง PC0 เพื่อทดสอบ DNS Server ว่าใช้งานได้ หรือไม่ โดยเลือกที่ Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  พิล์ด DNS Server ให้ใส่ IP Address ของ DNS Server ในที่นี่คือ 192.168.0.100
7. ให้ทดสอบเว็บเซิร์ฟเวอร์อีกรอบว่าทำงานอยู่หรือไม่ (IP 192.168.0.12) ทดสอบโดยการ ping หรือใช้ <http://192.168.0.12>
8. เสร็จกระบวนการเชื่อมต่อและถอนไฟล์เครื่อข่าย

การทดสอบ :

1. ให้ทำการทดสอบ DNS และเว็บเซิร์ฟเวอร์ โดยการคลิกที่ PC0  $\Rightarrow$  Desktop  $\Rightarrow$  Web Browser  $\Rightarrow$  ให้กรอกในช่อง URL เป็น <http://www.google.co.th> และกดปุ่ม Go ดังรูปด้านล่าง



เมื่อทุกอย่างคอนฟิกถูกต้อง โปรแกรม Browser ของเครื่อง PC0 จะแสดงผลที่ส่งมาจาก Web Server ได้ถูกต้องคือ โดเมนเนมชื่อ [www.google.co.th](http://www.google.co.th) จะมี IP คือ 192.168.0.12 การวิเคราะห์แพ็คเก็ต HTTP:

1. เลือกการทำงานเป็นโหมด Simulation
2. ในส่วนนี้จะข้ามขั้นตอนการทำงานของ ARP (สามารถอ่านได้ใน Scenario 5) เพื่อให้เนื้อหากระชับขึ้น โดยเริ่มจาก PC0 ร้องขอผ่านทาง URL คือ [www.google.co.th](http://www.google.co.th)
3. PC0 จะร้องขอไปยัง DNS Server (IP 192.168.0.100) ที่เวลา 0.000 ใน Event List

Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.000	--	PC0	DNS	

4. แพ็คเก็ตของ DNS จะถูกส่งจาก PC0 ไปยัง Switch0 เพื่อส่งต่อไปยังเครื่อง DNS Server ในเวลาที่ 0.001

Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.000	--	PC0	DNS	
	0.001	PC0	Switch0	DNS	

5. ในเวลาที่ 0.002 Switch0 ทำการรับส่งแพ็คเก็ตต่อไปยังเครื่อง DNS Sever เนื่องจาก Switch0 เรียนรู้แล้วว่า DNS Server อยู่ที่ใด (รู้ด้วยการໂປຣໂຫຍດ ARP)

Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.001	PC0	Switch0	DNS	
	0.002	Switch0	DNS Server	DNS	

6. เวลาที่ 0.003 DNS Server ตอบกลับว่าจาก [www.google.co.th](http://www.google.co.th) เป็น 192.168.0.12 ส่งกลับไปให้ Switch0

Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.002	Switch0	DNS Server	DNS	
	0.003	DNS Server	Switch0	DNS	

7. เวลาที่ 0.004 Switch0 ส่งแพ็คเก็ตที่ DNS ส่งให้ถึง PC0 เมื่อ PC0 ได้รับก็จะนำหมายเลข IP ดังกล่าวที่ได้รับ ร้องขอไปยังเว็บเซิร์ฟเวอร์ อีกครั้ง

Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.004	Switch0	PC0	DNS	
	0.004	--	PC0	TCP	

8. เวลาที่ 0.005 แพ็คเก็ตจาก PC0 ไปถึง Switch0 (TCP) เพื่อไปยังเว็บเซิร์ฟเวอร์เพื่อขอเปิดพอร์ต 80 (พอร์ตที่ให้บริการเว็บ)

Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.004	--	PC0	TCP	
	0.005	PC0	Switch0	TCP	

9. เวลาที่ 0.006 แพ็คเก็ตจาก Switch0 ไปถึงเครื่อง Web Server

Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.005	PC0	Switch0	TCP	
Eye	0.006	Switch0	Web Server	TCP	

10. เวลาที่ 0.007 Web Server ตอบกลับ โดยยอมให้ทำการเปิดพอร์ต 80 ตามที่ร้องขอมาโดยส่งกับไปยัง Switch0

Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.006	Switch0	Web Server	TCP	
Eye	0.007	Web Server	Switch0	TCP	

11. เวลาที่ 0.008 PC0 ได้รับตอบรับว่าเปิดพอร์ตแล้ว จึงร้องขอไปอีกครั้ง ด้วยprotoคือ HTTP

Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.008	Switch0	PC0	TCP	
Eye	0.008	--	PC0	HTTP	

12. เวลาที่ 0.010 Switch0 ส่งแพ็คเก็ต HTTP ต่อไปยัง Web Server

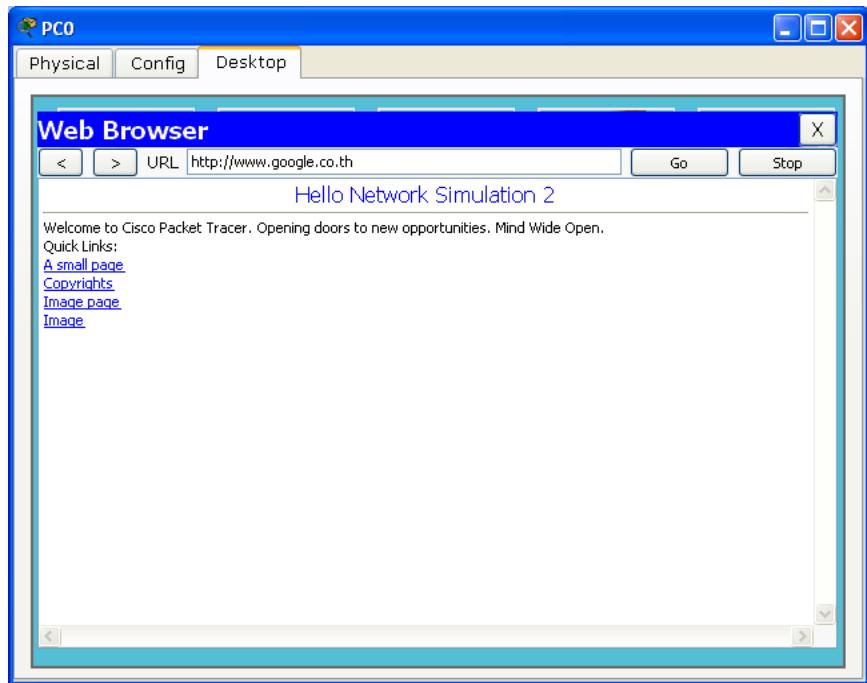
Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.010	PC0	Switch0	HTTP	
Eye	0.010	Switch0	Web Server	TCP	

13. เวลาที่ 0.012 Web Server นำข้อมูล HTML ส่งกลับไปให้ Switch0

Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.011	Switch0	Web Server	HTTP	
Eye	0.012	Web Server	Switch0	HTTP	

14. เวลาที่ 0.013 Switch0 ส่งข้อมูล HTML ให้กับ PC0 เมื่อ PC0 ได้รับก็จะทำการแสดงผลด้วย Web Browser ดังรูปด้านล่าง

Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.013	--	PC0	TCP	
Eye	0.013	Switch0	PC0	HTTP	



กระบวนการทำงานของ DNS, Web Server และ Web Browser เสร็จสิ้น



### Scenario 9: การติดตั้งอีเอชซีพีเซอร์ฟเวอร์ (DHCP)

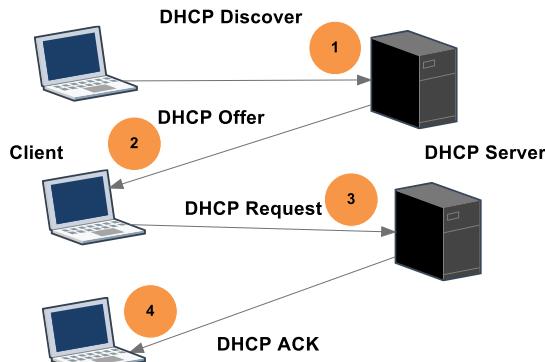
คำอธิบาย :



DHCP หรือ Dynamic Host Configuration Protocol คือ โพรโทคอลที่ใช้ในการกำหนดเลขหมาย IP Address อัตโนมัติแก่เครื่องลูกข่ายบนระบบเครือข่ายที่ติดตั้งโพรโทคอล TCP/IP, สำหรับ DHCP server มีหน้าที่แจก IP ในเครือข่ายโดยไม่ซ้ำกัน เนื่องจากองค์กรหรือหน่วยงานที่มีเครื่องลูกข่ายมากๆ จะประสบปัญหาในการจัดสรรหมายเลข IP แบบกำหนดตายตัว (fix IP) โดยการทำงานนั้นจะเริ่มต้นเมื่อเครื่องลูกข่ายเริ่มเปิดเครื่องก็จะขอ IP address, Subnet mask, หมายเลข DNS และ Default gateway จาก DHCP Server อัตโนมัติ

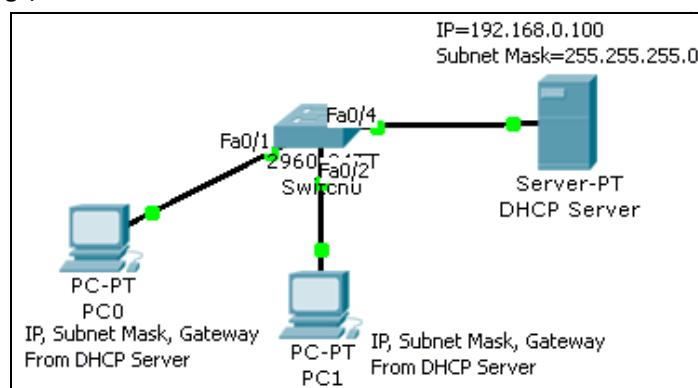
ขั้นตอนการเชื่อมต่อของเครื่องลูกข่ายกับ DHCP server มีดังนี้

1. เครื่องลูกข่ายค้นหาเครื่อง DHCP server ในเครือข่าย โดยส่ง DHCP discover เพื่อร้องขอ IP address
2. DHCP server จะค้นหา IP ที่ว่างอยู่ในฐานข้อมูล แล้วส่ง DHCP offer กลับไปให้เครื่องลูกข่าย
3. เมื่อเครื่องลูกข่ายได้รับ IP ก็จะส่งสัญญาณตอบกลับคือ DHCP Request ให้เครื่องแม่ทรานส์ฟอร์ม
4. DHCP server ส่งสัญญาณ DHCP ACK กลับไปให้เครื่องลูกข่าย เพื่อแจ้งว่าเริ่มใช้งานได้ ดังรูปด้านล่าง



ขั้นตอนการทำงานของ DHCP เซิร์ฟเวอร์

แผนผังการเชื่อมต่อ :



รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask	Interface Type
PC0	จาก DHCP	จาก DHCP	FastEthernet
PC1	จาก DHCP	จาก DHCP	FastEthernet
DNS Server	192.168.0.100	255.255.255.0	FastEthernet
Switch0	-	-	FastEthernet0/1 to PC0 FastEthernet0/2 to PC1 FastEthernet0/4 to DNS Server

ขั้นตอนการเชื่อมต่อ :

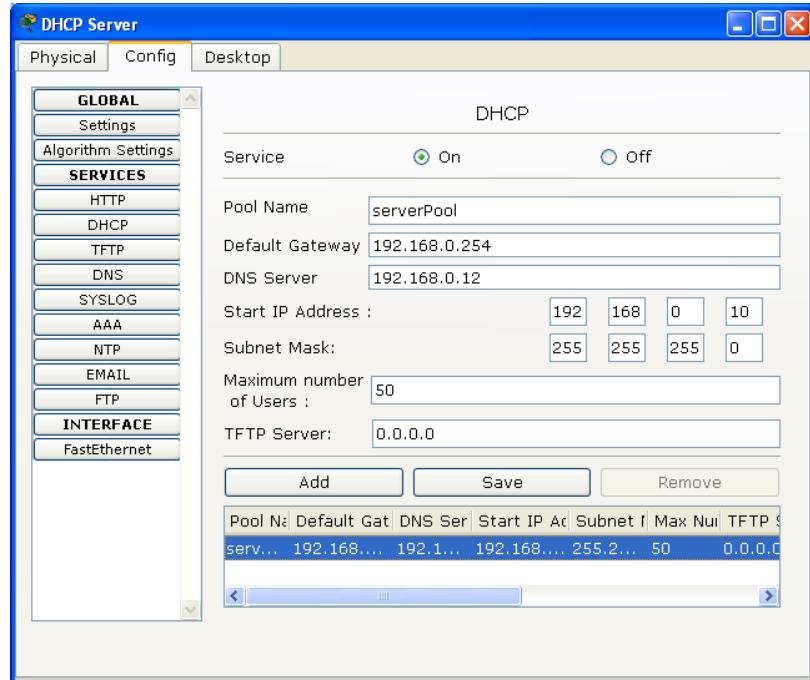
1. ทำการเชื่อมต่อ PC0, PC1 หรือบนกับ Scenario 7 โดยไม่ต้องกำหนดหมายเลข IP
2. สำหรับเครื่อง DHCP Server ให้ทำการคุณพิก IP Address โดยเลือกที่ Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนด IP ดังนี้

IP Address = 192.168.0.100

Subnet Mask = 255.255.255.0

3. ทำการ Enable DHCP Server โดยเลือกที่ Desktop  $\Rightarrow$  Config  $\Rightarrow$  เลือกแท็บ DHCP  $\Rightarrow$  ตรวจสอบ DHCP Service อยู่ในสถานะ On หรือยัง ถ้ายัง ให้เลือกเป็น On
4. ฟิลด์ Pool Name ให้ใส่ชื่อที่ต้องการ (ชื่อที่ตั้งควรสอดคล้องกับสถานที่ที่แจก IP แต่สำหรับ Packet Tracer ควรใช้ชื่อเดิมคือ ServerPool) เช่น Building A Floor Lab1, ฟิลด์ Default Gateway ใส่หมายเลข IP เกตเวย์ของเน็ตเวิร์คที่ต้องการแจกให้เครื่อง

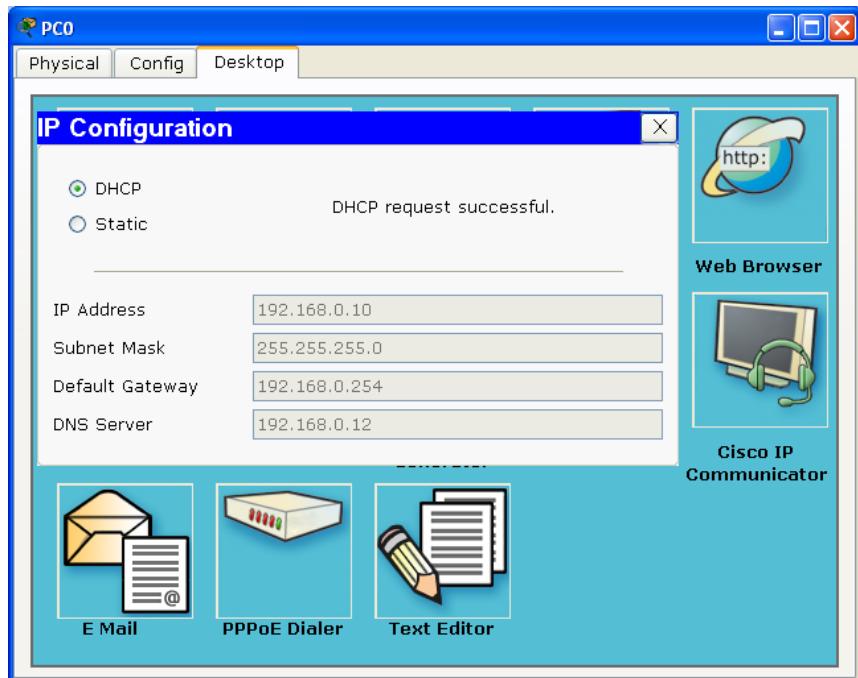
ลูกข่าย เช่น 192.168.0.254, DNS Server ใส่หมายเลข IP ของ DNS Server, Start IP Address ใส่ IP Address เริ่มต้นที่ต้องการแจกให้เครื่องลูกข่าย (ยกเว้น Network IP, Gateway IP, Broadcast IP) เช่น 192.168.0.10, Subnet Mask กำหนดหมายเลข Subnet Mask เช่น 255.255.255.0, Maximum Number of Users กำหนดจำนวน IP ที่ต้องการแจกให้กับเครื่องลูกข่าย เช่น 50 ต่อจากนั้นให้กดปุ่ม Add หรือ Save (ควรแก้ไขจาก ServerPool และเลือก Save)



### 5. เสร็จขั้นตอนการเชื่อมต่อ

การทดสอบ :

- ให้ทำการทดสอบ DHCP เซิร์ฟเวอร์ โดยการคอนฟิกให้เครื่องลูกข่ายรับหมายเลข IP Address จากเครื่อง DHCP Server โดยการคลิกที่ PC0  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  เลือก DHCP และสังเกตการเปลี่ยนแปลงในช่อง IP Address, Subnet Mask, Default Gateway เป็นต้น ดังรูปด้านล่าง (ถ้ายังไม่มีการเปลี่ยนแปลงให้กดสลับกันระหว่าง DHCP กับ Static)



เมื่อทุกอย่างค่อนพิกถูกต้อง เครื่อง PC0 จะแสดงค่า IP Address, Subnet Mask, Default Gateway, DNS Server อย่างถูกต้อง

#### การวิเคราะห์แพ็คเก็ต DHCP:

- เลือกการทำงานเป็นโหมด Simulation
- ในแท็บ Event List Filters ให้เลือกปุ่ม Edit Filters  $\Rightarrow$  Show All/None แล้วเลือกแสดงผลเฉพาะ DHCP เท่านั้น
- คลิกเลือก PC0  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  เลือก DHCP แล้วกลับไปพิจารณาในแท็บ Event List อีกครั้ง
- เริ่มต้น PC0 ทำการร้องขอไปยัง DHCP Server (IP 192.168.0.100)

#### DHCP Discovery

Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.000	--	PC0	DHCP	
	0.000	--	PC0	DHCP	

ข้อมูลใน Ethernet เฟรม

DEST MAC=FFF.FFF.FFF.FFF (กระจายไปทุกๆ เครื่อง)

SRC MAC=000A.4193.A5E1 (เครื่อง PC0)

#### Ethernet II

0	4	8	14	19 Byte
PREAMBLE: 101010...1011	DEST MAC: FFFF.FFFF.FFFF	SRC MAC: 000A.4193.A5E1		
TYPE: 0x800	DATA (VARIABLE LENGTH)		FCS: 0x0	

ข้อมูลใน IP แพ็คเก็ต

SRC IP: 0.0.0.0

DST IP: 255.255.255.255

IP				31 Bits		
0	4	8	16	19		
4	IHL	DSCP: 0x0		TL: 62		
			ID: 0x18	0x0	0x0	
TTL: 128		PRO: 0x11		CHKSUM		
		SRC IP: 192.168.0.12				
		DST IP: 255.255.255.255				
		OPT: 0x0		0x0		
		DATA (VARIABLE LENGTH)				

ข้อมูลใน UDP แพ็คเก็ต

SRC PORT: 68

DEST PORT: 67

UDP

16		31 Bits	
SRC PORT: 68	DEST PORT: 67		
LENGTH: 0x2a	CHECKSUM: 0x0		
DATA (VARIABLE)			

ข้อมูลใน DCHP แพ็คเก็ต

OP: 0x1

"YOUR" CLIENT ADDRESS: 0.0.0.0

SERVER ADDRESS: 0.0.0.0

CLIENT HARDWARE ADDRESS: 000A.4193.A5E1

DHCP

31 Bits			
0	8	16	31 Bits
OP: 0x7	HW TYPE	HW LEN	HOPS
TRANSACTION ID (4 BYTES)			
SECS	FLAGS		
CLIENT ADDRESS: 0.0.0.0			
"YOUR" CLIENT ADDRESS: 0.0.0.0			
SERVER ADDRESS: 0.0.0.0			
RELAY AGENT ADDRESS			
CLIENT HARDWARE ADDRESS: 000A.4193.A5E1			
SERVER HOSTNAME (64 BYTES)			
FILE (128 BYTES)			
OPTIONS (312 BYTES)			

ในขั้นตอนของ DHCP Discovery โปรโตคอล DHCP จะใช้ UDP ในการส่งข้อมูล ใช้หมายเลขพอร์ตต้นทางคือ 68, พอร์ตปลายทางคือ 67, IP ต้นทาง (SRC=0.0.0.0) เพราะยังไม่ได้รับจดสรร IP มาให้ เริ่มต้นจีบค่าเป็น 0.0.0.0 ก่อนเสมอ, IP ปลายทาง คือเครื่อง DHCP Server จะเป็น 255.255.255.255 ซึ่งเป็นการ Broadcast ซึ่งกระจายไปทั่วเครือข่าย และ Option จะถูกกำหนดเป็น 0x1

5. ขั้นตอนของ DHCP Offer แพ็คเก็ตของ DHCP จะถูกส่งจาก DHCP Server กลับไปยังเครื่อง PC0 ผ่าน Switch0

#### DHCP Offer

ข้อมูลใน Ethernet เฟรม

DEST MAC=FFF.FFF.FFF.FFF (กระจายไปทุกๆ เครื่อง)

SRC MAC= 00E0.F978.6CE3 (เครื่อง DHCP Server)

ข้อมูลใน IP แพ็คเก็ต

SRC IP: 192.168.0.100

DST IP: 255.255.255.255

ข้อมูลใน UDP แพ็คเก็ต

SRC PORT: 67

DEST PORT: 68

ข้อมูลใน DCHP แพ็คเก็ต

OP: 0x2 (DHCP Offer)

"YOUR" CLIENT ADDRESS: 192.168.0.12 (DHCP จะให้ client)

SERVER ADDRESS: 192.168.0.100 (เครื่อง DHCP Server)

CLIENT HARDWARE ADDRESS: 000A.4193.A5E1

ในขั้นตอนของ DHCP Offer โปรโตคอล DHCP จะใช้หมายเลขพอร์ตต้นทางคือ 67, พор์ตปลายทางคือ 68, IP ต้นทาง SRC=192.168.0.100, IP ปลายทางคือ 255.255.255.255 และ Option จะถูกกำหนดเป็น 0x2

6. ขั้นตอนของ DHCP Request แพ็คเก็ตของ DHCP จะถูกส่งจาก PC0 กลับไปยังเครื่อง DHCP Server อีกครั้ง ผ่าน Switch0

#### **DHCP Request**

ข้อมูลใน Ethernet เฟรม

DEST MAC=FFF.FFF.FFF.FFF

SRC MAC= 00A.4193.A5E1

ข้อมูลใน IP แพ็คเก็ต

SRC IP: 0.0.0.0

DST IP: 255.255.255.255

ข้อมูลใน UDP แพ็คเก็ต

SRC PORT: 68

DEST PORT: 67

ข้อมูลใน DCHP แพ็คเก็ต

OP: 0x3

"YOUR" CLIENT ADDRESS: 192.168.0.12

SERVER ADDRESS: 192.168.0.100

CLIENT HARDWARE ADDRESS: 000A.4193.A5E1

7. ขั้นตอนสุดท้ายคือ DHCP ACK แพ็คเก็ตของ DHCP จะถูกส่งจาก DHCP Server กลับไปยังเครื่อง PC0 อีกครั้ง ผ่าน Switch0

#### **DHCP ACK**

ข้อมูลใน Ethernet เฟรม

DEST MAC=FFF.FFF.FFF.FFF

SRC MAC= 00E0.F978.6CE3

ข้อมูลใน IP แพ็คเก็ต

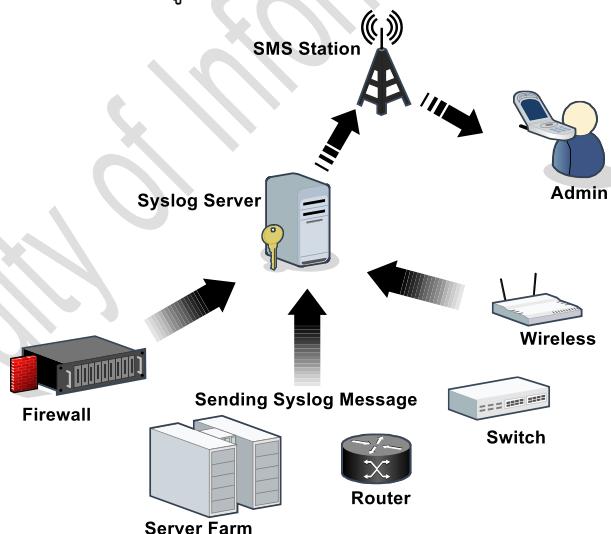
SRC IP: 192.168.0.100  
 DST IP: 255.255.255.255  
 ข้อมูลใน UDP แพ็คเก็ต  
 SRC PORT: 67  
 DEST PORT: 68  
 ข้อมูลใน DCHP แพ็คเก็ต  
 OP: 0x5  
 "YOUR" CLIENT ADDRESS: 192.168.0.12  
 SERVER ADDRESS: 192.168.0.100  
 CLIENT HARDWARE ADDRESS: 000A.4193.A5E1



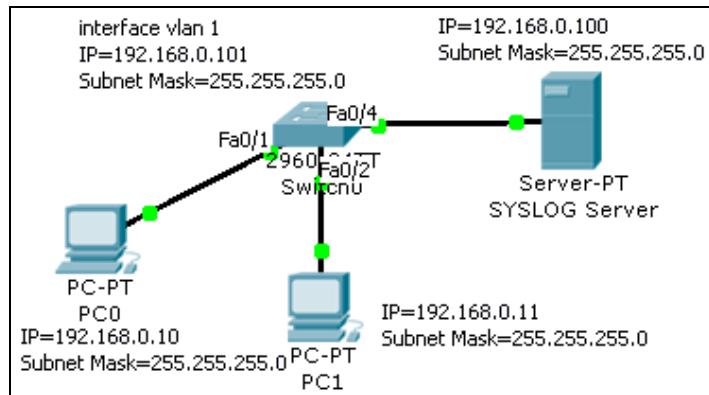
### Scenario 10: การติดตั้ง SYSLOG เครื่องเซิร์ฟเวอร์

คำอธิบาย :

SYSLOG หรืออาจจะเรียกเป็น Syslog Daemon เป็นซอฟต์แวร์ที่ทำหน้าที่รับ, บันทึกไฟล์ logs, แสดงผลไฟล์ logs และส่งข้อมูลการทำงาน เรียกว่า Syslog message จากเครื่องให้บริการ เช่น เรอาเตอร์, สวิตซ์, เซิร์ฟเวอร์, ไฮสตัต์ และอุปกรณ์อื่นๆ ที่มีการ enable โปรแกรม Syslog ไว้ Syslog ยังมีความสามารถอื่นๆ อีก เช่น ส่งเสียงเตือน, ส่ง email message เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น เป็นต้น ดังรูปด้านล่าง



แผนผังการเชื่อมต่อ :



รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask	Interface Type
PC0	192.168.0.10	255.255.255.0	FastEthernet
PC1	192.168.0.11	255.255.255.0	FastEthernet
SYSLOG Server	192.168.0.100	255.255.255.0	FastEthernet
Switch0	192.168.0.101	255.255.255.0	FastEthernet0/1 to PC0 FastEthernet0/2 to PC1 FastEthernet0/4 to SYSLOG Server

ขั้นตอนการเชื่อมต่อ :

- ให้ทำการเชื่อมต่อ PC0, PC1 ตามรูป พร้อมกำหนด IP ตามตารางด้านบน
- สำหรับเครื่อง SYSLOG Server ให้ทำการค้นฟิก IP Address โดยเลือกที่ Desktop  
 ⇒ IP Configuration ⇒ กำหนด IP ดังนี้  
 IP Address = 192.168.0.100  
 Subnet Mask = 255.255.255.0
- ทำการ Enable SYSLOG Server โดยเลือกที่ Desktop ⇒ Config ⇒ เลือกแท็บ SYSLOG ⇒ ตรวจสอบ SYSLOG Service อยู่ในสถานะ On หรือยัง ถ้ายัง ให้เลือก เป็น On
- กำหนด IP Address ให้กับ Switch0 เนื่องจากการใช้ SYSLOG จำเป็นต้องระบุ IP ใน การเชื่อมต่อ สามารถทำได้ดังนี้ คลิกที่ Switch0 ⇒ CLI ⇒ ให้กด Enter 1-2 ครั้ง เพื่อให้เข้าสู่โหมดผู้ใช้ทั่วไป โดยแสดงเป็น prompt คือ Switch> ⇒ ให้คีย์คำสั่ง enable และกดปุ่ม Enter

```

Switch>
Switch>enable <ENTER>
Switch#configuration terminal <ENTER>
Switch(config)#interface vlan 1 <ENTER>
Switch(config-if)#ip address 192.168.0.101 255.255.255.0 <ENTER>
Switch(config-if)#^Z (กดปุ่ม CTRL พร้อมกับอักษร z)
Switch#
  
```

- เสร็จขั้นตอนการเชื่อมต่อ

### การทดสอบ :

- ให้ทำการทดสอบ SYSLOG เซิร์ฟเวอร์ โดยการส่งบันทึก log จาก Switch0 ไปเก็บไว้ใน SYSLOG Server โดยใช้คำสั่ง ดังนี้

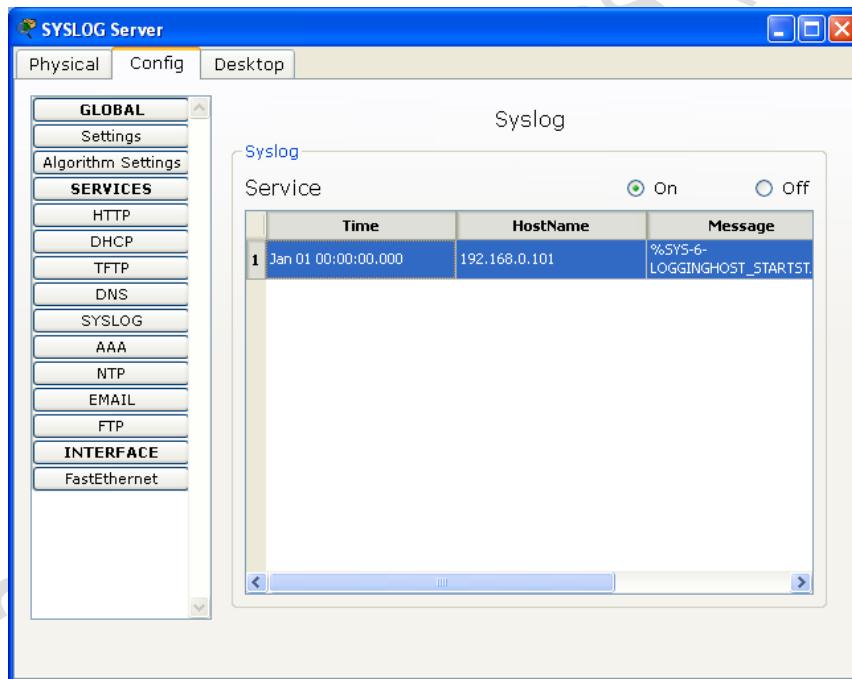
```

Switch>
Switch>enable <ENTER> ①
Switch#configure terminal <ENTER> ②
Switch(config)#logging 192.168.0.100 <ENTER> ③
Switch(config)#%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
192.168.0.100 port 514 started - CLI initiated

```

ขั้นตอนการทำงานของ SYSLOG ส่งข้อมูล log จาก Switch0 ไปเก็บยัง SYSLOG Server

- ① เข้าสู่โหมดผู้ดูแลระบบ
- ② เข้าสู่โหมดการคอนฟิกอุปกรณ์
- ③ สั่งให้บันทึกข้อมูล log ไฟล์การทำงานของ Switch0 ไปเก็บยังเครื่อง SYSLOG Server (SYSLOG คือ IP 192.168.0.100)



บนเครื่อง SYSLOG Server จะเริ่มทำการบันทึก log การทำงานของ Switch0



### Scenario 11: การติดตั้ง AAA/TACACS เซิร์ฟเวอร์

คำอธิบาย :

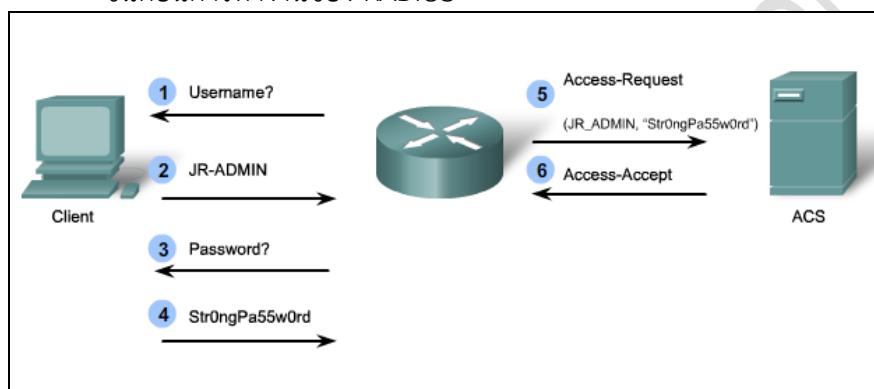
AAA เป็นมาตรฐานของการรักษาความปลอดภัยของข้อมูล (IEEE 802.1X) เช่น การจัดการ Account, การตรวจสอบสิทธิ เป็นต้น

AAA Server ย่อมาจาก 3 คำ คือ Authenticate, Authorization และ Accounting server เป็นการเพิ่มความปลอดภัยในการใช้งานแบบ Remote-Access ซึ่งเมื่อมีการเชื่อมต่อเข้ามา จะต้องถูกตรวจสอบด้วย AAA Server ก่อน ซึ่งจะตรวจสอบข้อมูลดังนี้ คือ

1. คุณเป็นใคร Who you are (authentication การยืนยัน, ระบุตัวตน - เป็นใคร?)
2. คุณได้รับอนุญาตให้ทำอะไรบ้าง What you are allowed to do (authorization การมอบสิทธิ์ใช้งาน - คนนี้ มีสิทธิ์แค่หน อ่าน/เขียน/ประมวลผล)
3. คุณทำอะไรไปบ้าง What you actually do (accounting การทำงานชีวิตประจำวัน - คนนี้ เข้ามายังไง)

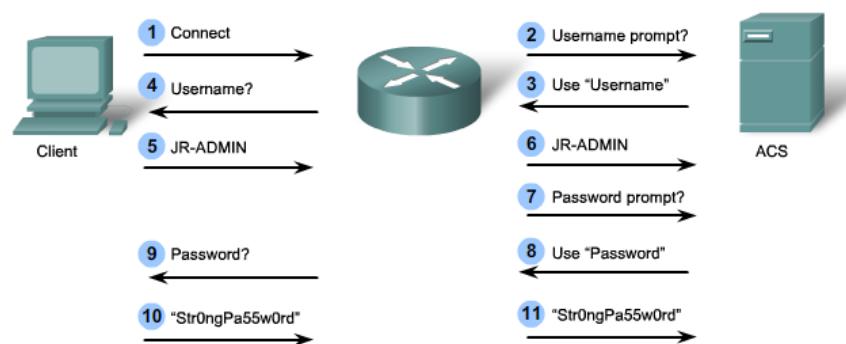
เทคนิคที่นิยมใช้งานมี 2 แบบคือ RADIUS และ TACACS+ (Terminal Access Controller Access Control System) ซึ่งแต่ละวิธีมีขั้นตอนการทำงานที่แตกต่างกันดังรูป

#### ขั้นตอนการทำงานของ RADIUS



- ❶ เมื่อผู้ใช้เชื่อมต่อผ่าน Remote-Access จะถูกสอบถาม User Name
- ❷ ผู้ใช้กรอก User Name
- ❸ ถามรหัสผ่าน
- ❹ ใส่รหัสผ่านของผู้ใช้
- ❺ อุปกรณ์ทำการส่งข้อมูล User Name และรหัสผ่านไปสอบ تمامยัง Access Control System (ACS) เพื่อตรวจสอบว่าข้อมูลถูกต้องหรือไม่
- ❻ อนุญาต เมื่อ User Name และรหัสผ่านถูกต้อง

#### ขั้นตอนการทำงานของ TACACS+



- ❶ ผู้ใช้ร้องขอการเชื่อมต่อ
- ❷ ตรวจสอบกับ ACS ว่ามีการเปิดใช้ User Name ?

- ③ เมื่อระบบเปิดใช้งาน จะส่งกลับว่าเปิดใช้งาน User Name
- ④ ส่งข้อมูลกลับให้ผู้ใช้งานว่าใช้งานแบบ User Name
- ⑤ ส่ง User Name
- ⑥ User Name ส่งให้ ACS ตรวจสอบความถูกต้อง
- ⑦ เมื่อ User Name ถูกต้อง ตรวจสอบว่าระบบเปิดใช้ Password?
- ⑧ เมื่อระบบเปิดการใช้งาน Password จะส่งข้อมูลกลับไปให้ผู้ใช้ວ่าต้องไปเปลี่ยนรหัสผ่าน

รหัสผ่าน

- ⑨ ส่งข้อมูลกลับไปให้ผู้ใช้ต่อไปเปลี่ยนรหัสผ่าน
- ⑩ ใส่รหัสผ่าน

⑪ ตรวจสอบรหัสผ่าน เมื่อถูกต้องจะอนุญาตให้ใช้งาน

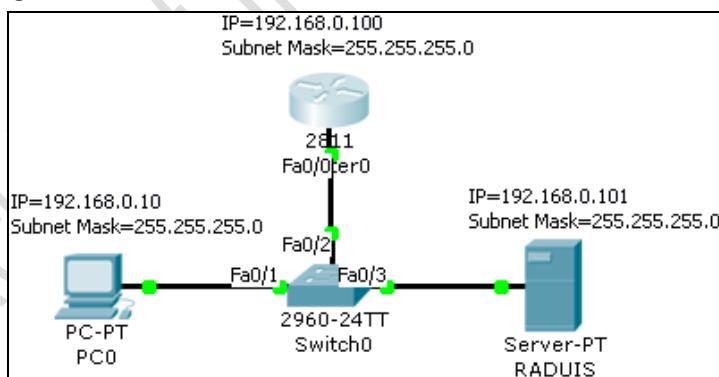
จากสองรูปด้านบน จะเห็นได้ว่า RADIUS มีการทำงานที่ซับซ้อนน้อยกว่า แต่ TACACS+ ยึดหยุ่นกว่า เพราะ TACACS+ แยกแต่ละขั้นตอนออกจากกัน ทำให้สามารถนำไปใช้กับการ Authentication ชนิดอื่นได้สะดวกกว่า แต่ต้องยังไงก็ตามการใช้งาน ขึ้นอยู่กับความเหมาะสม หรือสิ่งที่จะประยุกต์ใช้

สำหรับการใช้งาน AAA บนอุปกรณ์ของ Cisco แบ่งออกได้เป็นสองรูปแบบใหญ่ๆ คือ

1. Local AAA
2. Server-Based AAA

ในหัวข้อนี้จะทดสอบเฉพาะ Server-Based AAA (RADIUS) ซึ่งเป็นการนำ Server มาช่วยในเรื่องของการควบคุมและจัดการรหัสผ่านต่างๆ ของผู้ใช้ในเครือข่าย เครื่องลูกข่ายจะทำการ Authentication กับ Server โดยอาจจะมีเราเตอร์, สวิตช์ หรือไฟล์วอลล์ เป็นอุปกรณ์ที่ต้องการเข้าถึง

แผนผังการเชื่อมต่อ :

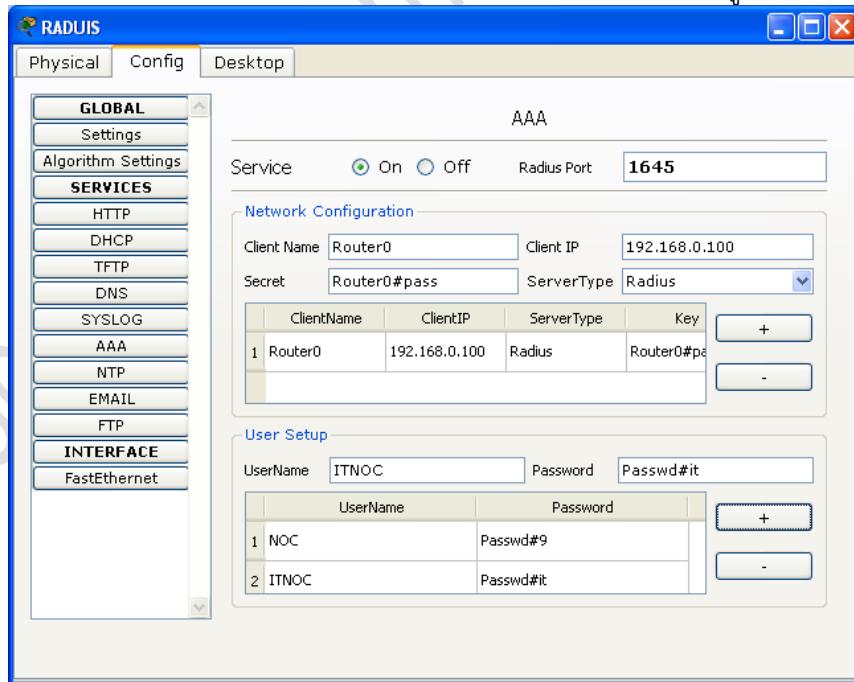


รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask	Interface Type
PC0	192.168.0.10	255.255.255.0	FastEthernet
Router0	192.168.0.100	255.255.255.0	FastEthernet 0/0
RADIUS Server	192.168.0.101	255.255.255.0	FastEthernet
Switch0	-	-	FastEthernet0/1 to PC0 FastEthernet0/2 to Router0 FastEthernet0/3 to RADIUS Server

ขั้นตอนการเชื่อมต่อ :

1. ให้ทำการเชื่อมต่อ PC0 ตามรูป พร้อมกำหนด IP ตามตารางด้านบน
2. สำหรับเครื่อง RADIUS Server ให้ทำการคอนฟิก IP Address โดยเลือกที่ Desktop  
⇒ IP Configuration ⇒ กำหนด IP ดังนี้  
IP Address = 192.168.0.101  
Subnet Mask = 255.255.255.0
3. ทำการ Enable RADIUS Server โดยเลือกที่ Desktop ⇒ Config ⇒ เลือกแท็บ RADIUS ⇒ ตรวจสอบ RADIUS Service อยู่ในสถานะ On หรือยัง ถ้ายัง ให้เลือกเป็น On
4. ในส่วน Network Configuration ฟิลด์ Client Name ให้ใส่ชื่ออุปกรณ์ที่ต้องการ Authentication เช่น Router0, Client IP ให้ใส่ IP อุปกรณ์ที่ต้องการ Authen ให้กำหนดเป็น 192.168.0.100, Secret ให้ใส่รหัสผ่าน กำหนดเป็น Router0#pass, ServerType เลือกเป็น RADIUS และคลิกเลือก + เพื่อเพิ่มข้อมูลที่ป้อนเข้าไปเก็บลงฐานข้อมูลของ RADIUS สำหรับข้อมูลในส่วน Network Configuration เป็นเหมือน Key ที่ใช้สำหรับผู้คนความสัมพันธ์ระหว่างชื่อผู้ใช้ เข้ากับอุปกรณ์เท่านั้น
5. ในส่วน User Setup ให้ทำการกำหนด User Name และรหัสผ่านที่ใช้ในการ Login จริงๆ ในฟิลด์ UserName ใส่ชื่อที่ต้องการ login ในที่นี่ใส่ NOC, Password ใส่ Passwd#9 และคลิก + เพื่อเพิ่มรายชื่อ ในส่วนนี้สามารถเพิ่มรายชื่อผู้ใช้กี่คนก็ได้ ดังรูป



6. บนเครื่อง Router0 ให้ดับเบิลคลิกที่ตัว Router0 ⇒ แท็บ CLI ⇒ ถ้าขึ้นข้อความ --- System Configuration Dialog --- ให้เลือก No และกด Enter ⇒ จะเข้าสู่โหมดผู้ใช้ที่ไปจากนั้นให้ทำการสั่งต่อไปนี้ เพื่อคอนฟิกอินเตอร์เฟส และ Enable AAA บน Router0

การคอนฟิก AAA และ Telnet

```

Router>
Router>enable <ENTER> ①
Router#configure terminal <ENTER> ②
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#aaa new-model <ENTER> ③
Router(config)#radius-server host 192.168.0.101 key Router0#pass
<ENTER> ④
Router(config)#aaa authentication login default group radius local
<ENTER> ⑤
Router(config)#line vty 0 4 <ENTER> ⑥
Router(config-line)#login authentication default <ENTER> ⑦
Router(config-line)#exit <ENTER> ⑧
Router(config)#exit <ENTER>
Router#write memory <ENTER> ⑨

```

- ① เข้าสู่โหมดผู้ดูแลระบบ
- ② เข้าสู่โหมดการคอนฟิก
- ③ enable AAA authentication
- ④ กำหนด IP ของเครื่อง Radius และ Key (shared secret) ที่ต้องการใช้จับคู่กับ User Name
- ⑤ เลือกวิธีการ authentication ในที่นี้เลือก Radius โดย login โดยใช้ค่า default
- ⑥ enable การ login ให้สามารถใช้ telnet ได้
- ⑦ เลือกวิธี login ด้วย Radius
- ⑧ ออกจากโหมดการคอนฟิก
- ⑨ บันทึกการเปลี่ยนแปลงบนเครื่องเราเตอร์

การคอนฟิก IP Address ที่อินเทอร์เฟส FastEthernet 0/0

```

Router>
Router>enable <ENTER> ①
Router#configure terminal <ENTER> ②
Router(config)#interface fastEthernet 0/0 <ENTER> ③
Router(config-if)#ip address 192.168.0.100 255.255.255.0 <ENTER> ④
Router(config-if)#no shutdown <ENTER> ⑤
Router#write memory <ENTER> ⑥

```

- ① เข้าสู่โหมดผู้ดูแลระบบ
- ② เข้าสู่โหมดการคอนฟิก
- ③ เข้าโหมดการคอนฟิกอินเทอร์เฟส FastEthernet 0/0
- ④ กำหนด IP Address ของอินเทอร์เฟส FastEthernet 0/0

⑤ เปิดการใช้งานอินเทอร์เฟส FastEthernet 0/0

⑥ บันทึกคอนฟิกุเรชันลงบนเครื่องเราเตอร์

การทดสอบ :

- ให้ทำการทดสอบ RADUIS เซิร์ฟเวอร์ โดยมีขั้นตอนดังนี้ เลือก PC0  $\Rightarrow$  Desktop  $\Rightarrow$  Command Prompt จากนั้นคีย์คำสั่งดังต่อไปนี้

PC>telnet 192.168.0.100 <ENTER> ①

Trying 192.168.0.100 ...Open

User Access Verification

Username: NOC <ENTER> ②

Password:##### <ENTER> ③

Router> ④

ขั้นตอนการทดสอบ RADIUS

① ใช้คำสั่ง telnet ทำการ remote login ไปยังเราเตอร์ (IP 192.168.0.100)

② เมื่อการเชื่อมต่อสำเร็จ ระบบจะให้ผู้ใช้ใส่ User Name

③ ใส่รหัสผ่าน

④ เมื่อ login สำเร็จ จะสามารถเข้าสู่โหมดผู้ใช้ทั่วไปได้



### Scenario 12: การติดตั้ง NTP เซิร์ฟเวอร์

คำอธิบาย :

Network Time Protocol (NTP) เป็นโปรโตคอลในระดับ Application Layer ที่หน้าที่ในการเทียบเวลาระหว่างอุปกรณ์คอมพิวเตอร์ การทำงานของโปรโตคอล NTP จะต้องอาศัยเครื่องให้บริการ (NTP Server) ที่เปิดบริการพอร์ตหมายเลข 123 ชนิด UDP สำหรับการร้องขอการเทียบเวลาจากเครื่องลูกข่าย จะอยู่ในรูปแบบลำดับชั้น ที่เรียกว่า “Clock Strata” โดยแบ่งลำดับชั้นของการเทียบเวลาดังนี้

Stratum 0 เป็นอุปกรณ์ของแหล่งกำเนิดเวลา เช่น Atomic clocks, GPS เป็นต้น

Stratum 1 เป็นเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับ Stratum 0 ได้รับค่าเวลามาจาก Stratum 0 โดยตรงผ่านการเชื่อมต่อในระบบคอมพิวเตอร์ เช่น RS-232 เป็นต้น

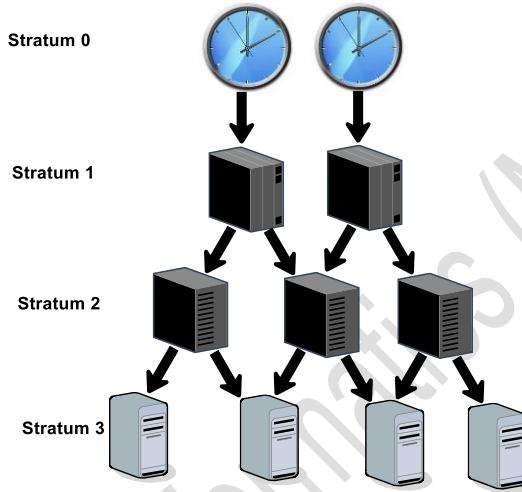
Stratum 2 เป็นเครื่องคอมพิวเตอร์ที่ร้องขอการเทียบเวลาจากเครื่องคอมพิวเตอร์แม่ข่าย Stratum 1 ผ่านระบบเครือข่าย TCP/IP ด้วยการใช้งาน NTP เครื่องคอมพิวเตอร์ในระดับนี้อาจจะร้องขอการเทียบเวลาจาก Stratum 1 ได้มากกว่า 1 แหล่งเพื่อรับการทำงานแบบทดแทนกันเมื่อไม่สามารถเข้าถึง Stratum 1 ตัวใดตัวหนึ่งก็จะสามารถร้องขอการเทียบเวลาจาก Stratum 1 ตัวอื่นได้ต่อไป

Stratum 3 เป็นเครื่องคอมพิวเตอร์ที่ร้องขอการเทียบเวลาจากเครื่องคอมพิวเตอร์แม่ข่าย Stratum 2 ผ่านระบบเครือข่าย TCP/IP ด้วยการใช้งาน NTP เครื่องคอมพิวเตอร์ในระดับนี้จะสามารถอ้างอิง Stratum 2 ได้มากกว่า 1 แหล่ง NTP นั้นสามารถรองรับระดับของการเทียบเวลาได้ถึง 16 ระดับ

หากอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์เครือข่ายในระบบสารสนเทศมีค่าเวลาที่แตกต่างกัน แล้วนั้นจะส่งผลให้เกิดปัญหาแก้ผู้ใช้งาน รวมทั้งผู้ดูแลระบบในการปฏิบัติงานต่างๆ เช่น

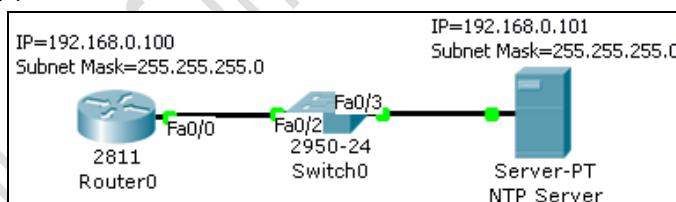
1. ความคาดเคลื่อนของเวลาในการการแจ้งปัญหาของระบบสารสนเทศ ระหว่างผู้ใช้งาน และผู้ดูแลระบบ
2. ความสับสนในการตรวจสอบ และวิเคราะห์เหตุการณ์ต่างๆ เช่น เหตุการณ์การบุกรุก เหตุการณ์ของปัญหาด้านเครือข่าย หรือระบบคอมพิวเตอร์
3. ผู้พัฒนาไม่สามารถสับสนในเวอร์ชันของโค้ดระหว่างการพัฒนา
4. มีการใช้งานไฟล์ข้อมูล หรือฐานข้อมูล ที่ซ้อนทับกัน

**หมายเหตุ:** ข้อมูล NTP อ้างอิงจาก <http://netco.ku.ac.th/law/ntp.htm>



ลำดับชั้นของการเทียบเวลาใน NTP

แผนผังการเชื่อมต่อ :



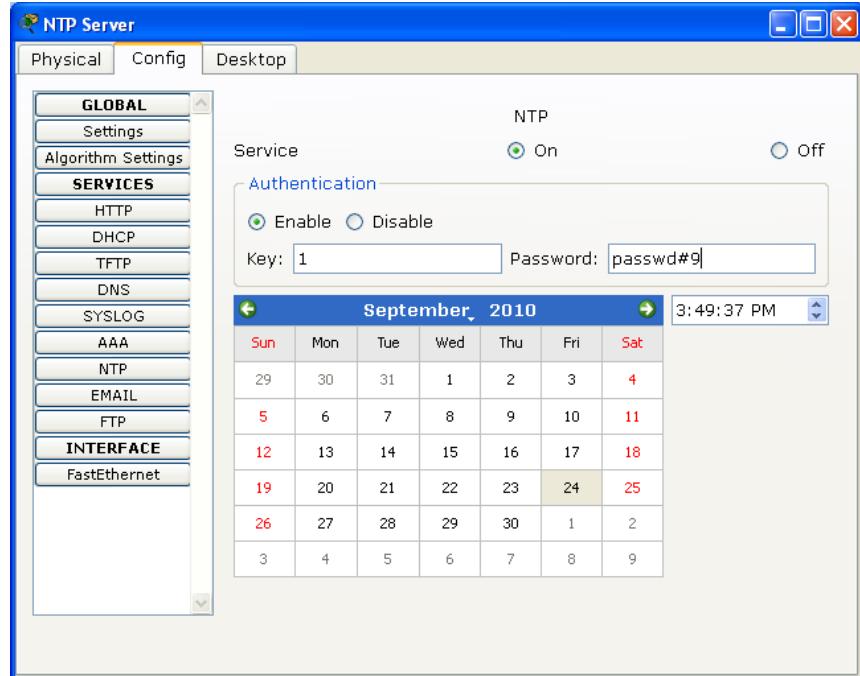
รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask	Interface Type
Router0	192.168.0.100	255.255.255.0	FastEthernet 0/0
NTP Server	192.168.0.101	255.255.255.0	FastEthernet
Switch0	-	-	FastEthernet0/2 to Router0 FastEthernet0/3 to NTP Server

ขั้นตอนการเชื่อมต่อ :

1. ให้ทำการเชื่อมต่อและกำหนด IP Address ของ Router0, NTP Server, Switch0 ตามรูป พร้อมกำหนด IP ตามตารางด้านบน
2. ทำการ Enable NTP Server โดยเลือกที่ Desktop  $\Rightarrow$  Config  $\Rightarrow$  เลือกแท็บ NTP  $\Rightarrow$  ตรวจสอบ NTP Service อยู่ในสถานะ On หรือยัง ถ้ายัง ให้เลือกเป็น On

3. ในส่วน Authentication ให้เลือกเป็น Enable ในฟิลด์ Key ให้ใส่ Key ที่ต้องการ Authentication, ในฟิลด์ Password ให้ใส่รหัสผ่านที่ต้องการ Authen, จากนั้นให้เลือกวันเวลาที่ต้องการให้อัปเกรดเข้ามาเทียบเวลา ซึ่งใน Packet Tracer จะดึงเวลาจากเครื่องที่ทำงานอยู่โดยอัตโนมัติ แต่ในการทำงานจริง NTP Server จะต้องเชื่อมต่อกับเวลาของ Stratum Server อีกที



แสดงการคอนฟิก NTP Server

4. ขั้นตอนต่อไปจะเป็นการคอนฟิกให้เราเตอร์หรือเชื่อมต่อกับ NTP Server เพื่อเทียบเวลา ในเบื้องต้นให้ตรวจสอบ Interface FastEthernet 0/0 ว่ามีหมายเลข IP Address และสามารถ ping เครื่อง NTP Server ได้หรือไม่ ถ้ายัง ให้กลับไปทำขั้นตอนการเชื่อมต่อก่อน ขั้นตอนนี้จะใช้คำสั่งต่อไปนี้บน Router0

```

Router>
Router>enable <ENTER> ①
Router#show clock <ENTER> ②
*3:59:22.756 UTC Mon Mar 1 1993
Router#configure terminal <ENTER> ③
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#ntp server 192.168.0.101 key 1 <ENTER> ④
Router(config)# ^Z <ENTER> ⑤
Router#sh clock <ENTER>
*16:3:23.469 UTC Fri Sep 24 2010

```

① เข้าสู่โหมดผู้ดูแลระบบ

② แสดงเวลาของ Router0 เดิม ในที่นี่คือ 3:59:22.756 UTC Mon Mar 1 1993

- ③ เข้าโหมดโภกออลคอนฟิก
- ④ เปิดการทำงานของ NTP บนเราเตอร์ ให้ทำการระบุเครื่อง NTP Server และ Key
- ⑤ กดปุ่ม CTRL + Z เพื่อออกไปสู่โหมดผู้ดูแลระบบ
- ⑥ ทดสอบเวลาของ Router0 อีกครั้ง ปรากฏว่าเวลาจะเปลี่ยนตาม NTP Server คือ 16:3:23.469 UTC Fri Sep 24 2010

การทดสอบ :

1. ให้ทำการทดสอบ NTP เชิร์ฟเวอร์ โดยใช้คำสั่ง show clock บนเราเตอร์ดังต่อไปนี้

```
Router#sh clock <ENTER>
```

```
*16:3:23.469 UTC Fri Sep 24 2010
```

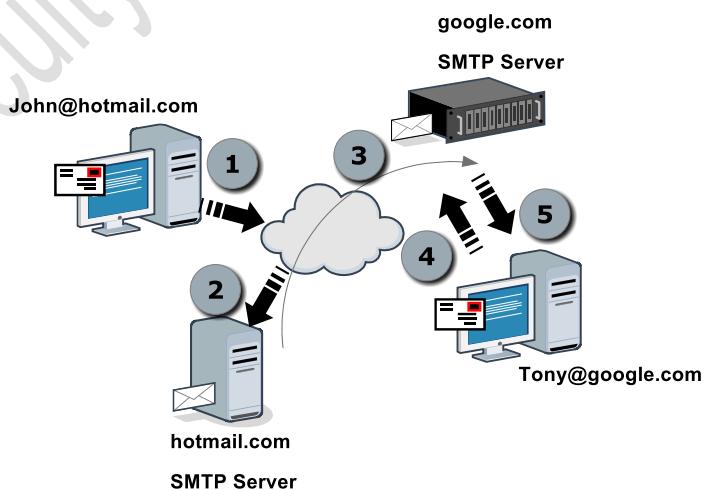


### Scenario 13: การติดตั้ง EMAIL เชิร์ฟเวอร์ (SMTP/POP3)

คำอธิบาย :

E-mail คือ จดหมายอิเล็กทรอนิกส์ หรือ ไปรษณีย์อิเล็กทรอนิกส์ (electronic mail, ย่อ e-mail หรือ email) เป็นการส่งข้อความจากบุคคลหนึ่งไปยังอีกบุคคลหนึ่ง ที่ใช้รับส่งกันโดยผ่านเครือข่ายคอมพิวเตอร์ E-mail จำเป็นต้องมีระบบการกำหนดชื่อที่อยู่ (e-mail address เช่น [suchart.k@msu.ac.th](mailto:suchart.k@msu.ac.th)) ซึ่งประกอบด้วยชื่อบัญชี (suchart.k) ตามด้วยเครื่องหมาย @ และปิดท้ายด้วยชื่ออีสต์ต์ ชื่องค์กร หรือ domain name ที่ลงทะเบียนไว้ การส่งจดหมายอิเล็กทรอนิกส์เป็นวิธีการส่งเหมือนจดหมายจริง โดยจะไปเก็บไว้ในเมล์บ็อกซ์ของผู้รับปลายทาง الرحمنกว่าผู้รับปลายทางจะมาเปิดเมล์บ็อกซ์นำจดหมายไป e-mail ประกอบไปด้วย 2 ส่วนคือ E-mail Server คือ

1. คอมพิวเตอร์ที่ทำหน้าที่ให้บริการด้านจดหมายอิเล็กทรอนิกส์ หรือ SMTP Server (Mail Server) และ protocols สำหรับการเข้าถึงจดหมายที่อยู่ใน SMTP Server เช่น POP และ IMAP
2. โปรแกรมที่ใช้สำหรับอ่านจดหมาย เขียนจดหมาย ส่งจดหมาย และรับจดหมาย (Mail Client) มีอยู่หลายตัวด้วยกันยกตัวอย่าง เช่น Pine, Netscape, Outlook, Webmail เป็นต้น



หลักการทำงานของ E-Mail Server

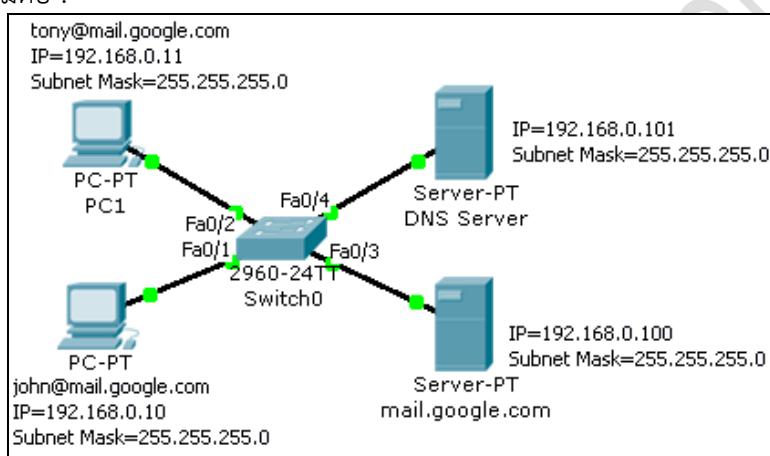
① ผู้ใช้ชื่อ John (ใช้ email ของ hotmail) ต้องการส่ง email ไปหา Tony (ใช้ email ของ google) โดย John จะเปิดโปรแกรม email client เช่น outlook หรือ web mail (ใช้งานอีเมลผ่านเว็บ) เช่น hotmail, yahoo เป็นต้น

② เมื่อผู้ใช้เขียนเมล์เสร็จ จะทำการส่งไปยัง Mail Server ของ hotmail เพื่อให้ทำการส่งเมล์ดังกล่าวไปยัง email ปลายทางซึ่งอยู่ที่ google.com  
 ③ Server hotmail ส่งจดหมายไปเก็บไว้ยัง Server google อยู่ในกล่องจดหมายของ Tony

④ Tony เข้ามาเปิดอ่านจดหมายในกล่องจดหมายของตนเอง

⑤ Tony อ่านจดหมาย ในทางกลับกันถ้า Tony ต้องการส่งจดหมายบ้าง ก็จะมีหลักการทำงานที่เหมือนกัน

แผนผังการเชื่อมต่อ :



รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask	Function
PC0 (john)	192.168.0.10	255.255.255.0	john@mail.google.com
PC1 (tony)	192.168.0.11	255.255.255.0	tony@mail.google.com
MAIL Server	192.168.0.100	255.255.255.0	mail.google.com
DNS Server	192.168.0.101	255.255.255.0	Domain Name Server
Switch0	-	-	-

ขั้นตอนการเชื่อมต่อ :

- ให้ทำการเชื่อมต่ออุปกรณ์ต่างๆ ดังผังเครือข่ายด้านบน และคอนฟิกค่าต่างๆ ตามตารางด้านบน ดังนี้

บนเครื่อง PC0 (john)

เลือก Desktop  $\Rightarrow$  IP Configuration

IP Address = 192.168.0.10

Subnet Mask = 255.255.255.0

DNS Server = 192.168.0.101

เลือก Desktop  $\Rightarrow$  E Mail  $\Rightarrow$  Configure Mail

Your Name = john

Email Address = [john@mail.google.com](mailto:john@mail.google.com)

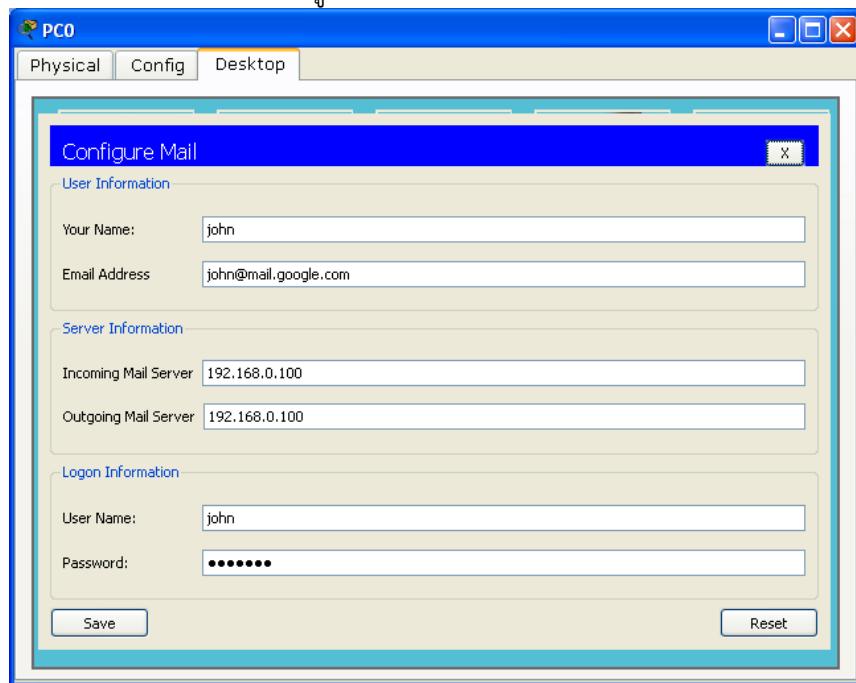
Incoming Mail Server = 192.168.0.100

Outgoing Mail Server = 192.168.0.200

User Name = john (ชื่อผู้ใช้ที่ใช้ติดต่อกับ Mail Server)

Password = john123 (รหัสผ่านผู้ใช้ที่ใช้ติดต่อกับ Mail Server)

เมื่อกรอกข้อมูลครบแล้วเลือก Save



แสดงการ Configure Mail

#### บนเครื่อง PC1 (tony)

เลือก Desktop  $\Rightarrow$  IP Configuration

IP Address = 192.168.0.11

Subnet Mask = 255.255.255.0

DNS Server = 192.168.0.101

เลือก Desktop  $\Rightarrow$  E Mail  $\Rightarrow$  Configure Mail

Your Name = tony

Email Address = [tony@mail.google.com](mailto:tony@mail.google.com)

Incoming Mail Server = 192.168.0.100

Outgoing Mail Server = 192.168.0.200

User Name = tony

Password = tony123

เมื่อกรอกข้อมูลครบแล้วเลือก Save

#### บนเครื่อง Mail Server

เลือก Desktop  $\Rightarrow$  IP Configuration

IP Address = 192.168.0.100

Subnet Mask = 255.255.255.0

เลือก Config  $\Rightarrow$  MAIL  $\Rightarrow$  เพิ่มรายชื่อผู้ใช้งดังต่อไปนี้

Domain Name = mail.google.com กรอกเสร็จแล้วเลือก Set  
เพิ่มผู้ใช้ชื่อ john

User = john

Password = john123

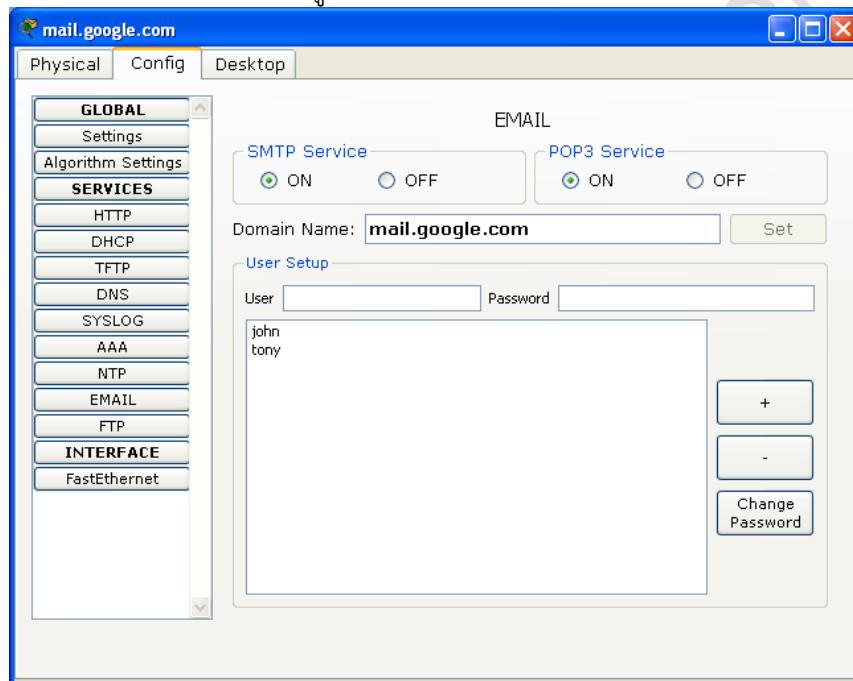
เมื่อกรอกข้อมูลครบแล้วเลือก + เพื่อเพิ่มรายชื่อ (เป็นการลงทะเบียนขอใช้ email  
บน Mail Server ของ google.com)

เพิ่มผู้ใช้ tony

User = tony

Password = tony123

เมื่อกรอกข้อมูลครบแล้วเลือก + เพื่อเพิ่มรายชื่อ



ตอนพิก Mail Server ชื่อ mail.google.com

บนเครื่อง DNS Server

เลือก Desktop  $\Rightarrow$  IP Configuration

IP Address = 192.168.0.101

Subnet Mask = 255.255.255.0

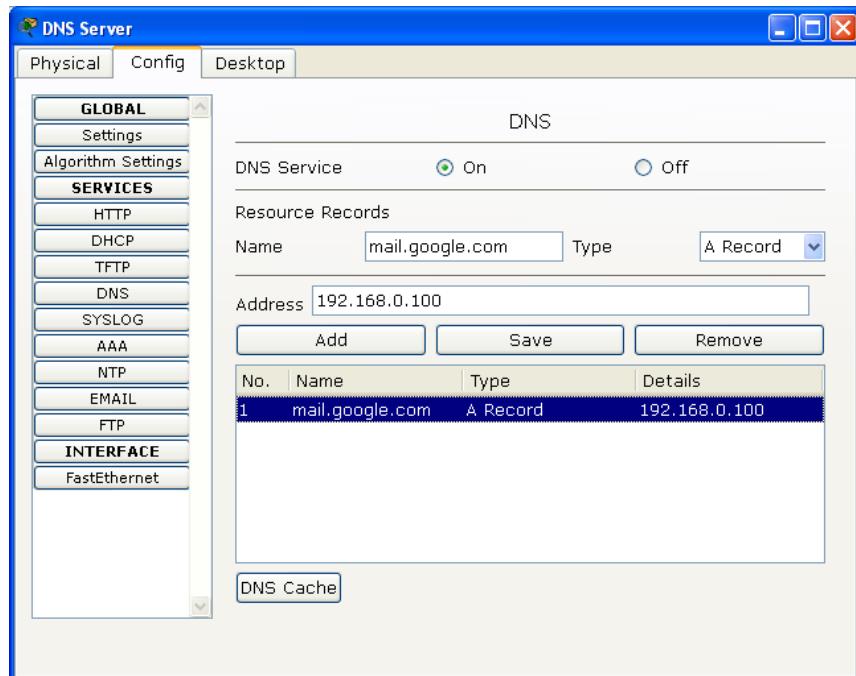
เลือก Config  $\Rightarrow$  DNS  $\Rightarrow$  เพิ่มโดเมนเนมดังต่อไปนี้

Name = mail.google.com

Type = A Record

Address = 192.168.0.100

เมื่อกรอกข้อมูลครบแล้วเลือก Save



ค่อนพิก DNS Server

## การทดสอบ :

- ให้ทำการทดสอบ MAIL เซิร์ฟเวอร์ โดยการส่ง email จากผู้ใช้ชื่อ john ไปหา tony โดยมีขั้นตอนดังนี้

เลือก PC0  $\Rightarrow$  Desktop  $\Rightarrow$  E Mail ทำการเขียนจดหมาย เพื่อส่งไปยัง tony  $\Rightarrow$  เลือก Compose Mail กรอกข้อมูลดังต่อไปนี้

To: = [tony@mail.google.com](mailto:tony@mail.google.com)

Subject: = Hi tony.

ในช่องเขียนจดหมายให้ผู้ใช้เขียนจดหมาย เช่น

Dear Mr. Tony

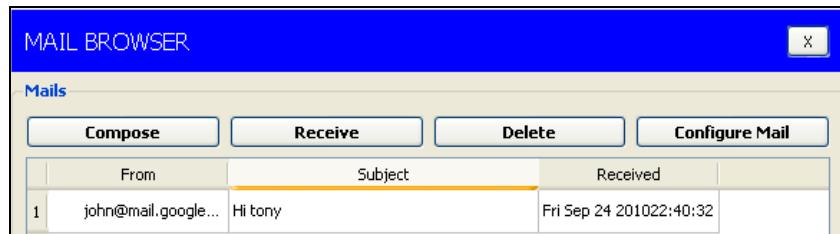
We wish to thank you once again for inviting us to your anniversary party, where good time was had by all. It was a successful event, and we really enjoyed ourselves.

Thank you again for being such wonderful hosts. We look forward to seeing you soon.

John.

เมื่อเขียนจดหมายเสร็จแล้วให้กดปุ่ม Send จดหมายจะส่งไปยัง Mail Box ของ tony

- ที่เครื่องของ tony ให้เลือก  $\Rightarrow$  Desktop  $\Rightarrow$  E Mail เพื่อทำการอ่านเมลที่ส่งมาจาก john  $\Rightarrow$  ที่ Mail Browser ให้เลือก Receive จะปรากฏจดหมายของ john อยู่ใน Mail Box ให้ดับเบิลคลิกเมล์ดังกล่าวเพื่ออ่านเมล



เมจดหมายจาก john อยู่ใน Mail Box ของ Tony



Tony เปิดจากหมายที่ส่งมาจาก John

3. ให้ทดลองส่งเมล์จาก tony ไปยัง john เพื่อทดสอบการทำงานของ Mail Server ว่า ทำงานถูกต้อง



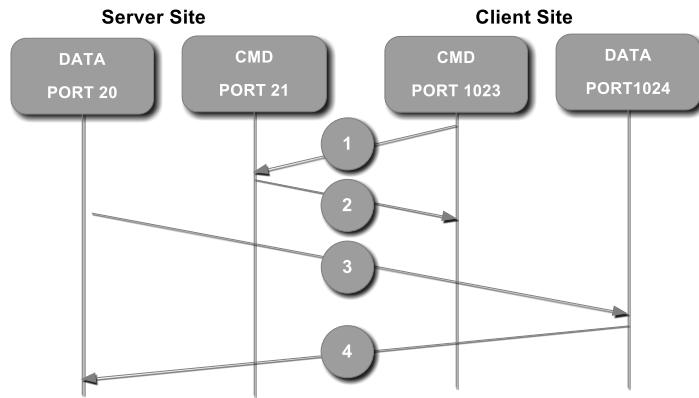
#### Scenario 14: การติดตั้งเอฟทีพีเซอร์ฟเวอร์ (FTP)

คำอธิบาย :

เอฟทีพี (FTP = File Transfer Protocol) คือ โปรแกรมที่ใช้สำหรับส่งแฟ้ม (Send) หรือรับแฟ้ม (Receive) ระหว่างเครื่องคอมพิวเตอร์ของผู้ใช้ (Client Computer) กับเครื่องให้บริการ (FTP Server) ผู้ให้บริการจะสร้างรหัสผู้ใช้(User Name) และรหัสผ่าน>Password) ให้ผู้ใช้แต่ละคนได้เป็นเจ้าของพื้นที่แต่ละห้อง (User Folder), FTP มีการทำงานโดยใช้พอร์ตสองพอร์ตคือ data port และ command port (หรือ control port) ซึ่งโดยทั่วไปจะใช้พอร์ตที่ 21 เป็น command port และใช้พอร์ต 20 สำหรับ data port แต่จะมีความสับสนเกิดขึ้นเมื่อ data port ไม่เป็นพอร์ต 20 ซึ่งจะขึ้นอยู่กับโหมดการทำงาน แบ่งได้เป็น 2 โหมดคือ Active FTP, Passive FTP

#### โหมด Active FTP

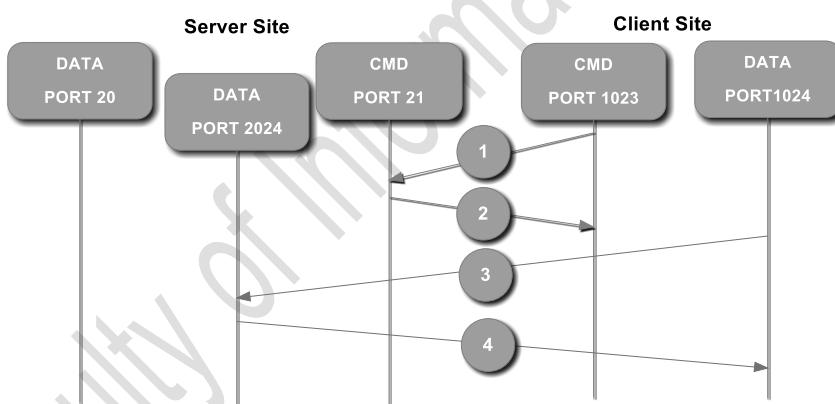
โหมดการทำงานที่เป็น Active FTP เครื่อง client จะเขื่อมต่อจากพอร์ตที่ไม่มีสิทธิเช่น (unprivileged port) แบบสูงที่มีค่าพอร์ตมากกว่า 1024 ( $N > 1024$ ) ไปยัง command port (21) ของ FTP Server จากนั้นเครื่อง client ก็จะเริ่มค่อยฟัง (listening) พอร์ต  $N+1$  และส่ง FTP command port  $N+1$  ไปยัง FTP Server และเครื่อง FTP Server ก็จะเขื่อมตอกลับมายังเครื่อง client ตาม data port ที่ได้กำหนดไว้ โดยที่ FTP Server จะเป็น Data Port 21 ซึ่งสามารถแสดงรูปการเชื่อมต่อของ Active FTP ดังรูปต่อไปนี้



- ❶ Command port ของเครื่อง client ติดต่อ command port ของเครื่อง Server และ ส่ง command PORT 1023
- ❷ Server ส่ง ACK กลับไปยัง command port ของเครื่อง client
- ❸ Server เริ่มต้นการเชื่อมต่อ (initiate) โดยใช้ data port ของตัวเองคือ 20 ไปยัง data port ของเครื่อง client ที่ถูกกำหนดไว้
- ❹ เครื่อง client ส่ง ACK กลับไปยัง Server

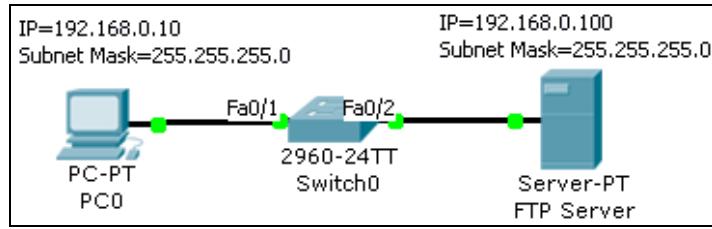
### โหมด Passive FTP

รูปการเชื่อมต่อของ Passive FTP ดังรูปด้านล่าง



- ❶ client ติดต่อ Server บน command port และส่ง PASV command
- ❷ Server ตอบกลับด้วยพอร์ต 2024 เพื่อบอก client ว่าพอร์ตไหนที่ Server กำลัง listening เพื่อการเชื่อมต่อ data
- ❸ client เริ่มต้นการเชื่อมต่อ data จาก data port ของตัวเองไปยัง data port ของ server ที่ถูกระบุ
- ❹ Server ส่ง ACK กลับไปยัง data port ของ client

หมายเหตุ: ข้อมูล FTP ข้างต้นจาก <http://www.tkc.ac.th/osunun/>  
แผนผังการเชื่อมต่อ :



รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask
PC0	192.168.0.10	255.255.255.0
FTP Server	192.168.0.100	255.255.255.0
Switch0	-	-

ขั้นตอนการเชื่อมต่อ :

- ให้ทำการเชื่อมต่ออุปกรณ์ต่างๆ ดังผังเครือข่ายด้านบน และคอนฟิกค่าต่างๆ ตามตารางด้านบน ดังนี้

#### บนเครื่อง PC0

เลือก Desktop  $\Rightarrow$  IP Configuration

IP Address = 192.168.0.10

Subnet Mask = 255.255.255.0

#### บนเครื่อง FTP Server

เลือก Desktop  $\Rightarrow$  IP Configuration

IP Address = 192.168.0.100

Subnet Mask = 255.255.255.0

เลือก Config  $\Rightarrow$  FTP  $\Rightarrow$  ตรวจสอบข้อมูลดังต่อไปนี้

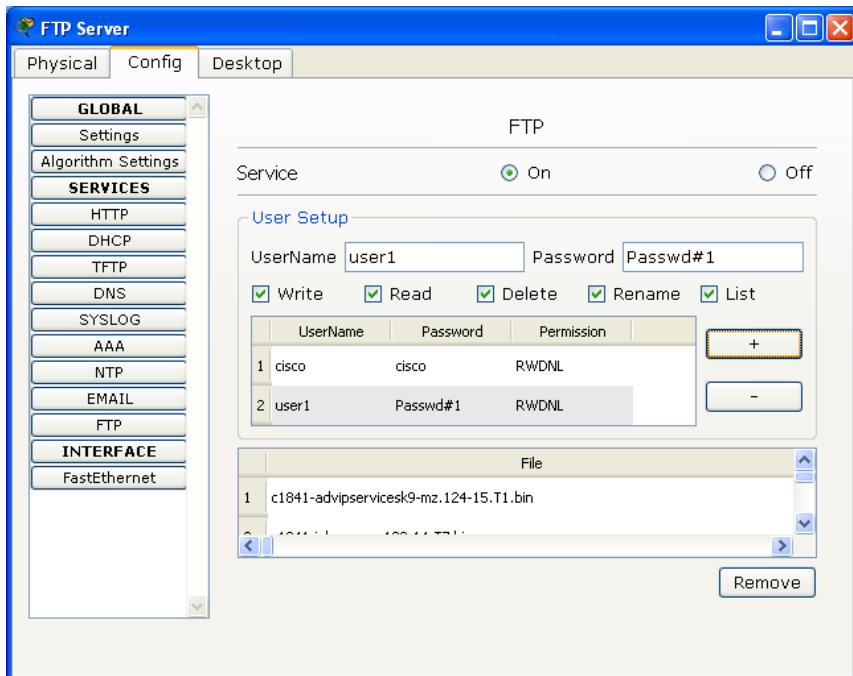
Service = on

User Name = user1 (กำหนดรายชื่อผู้ใช้งานบน FTP Server)

Password = Passwd#1 (กำหนดรหัสผ่านผู้ใช้งานสำหรับ user1)

คลิกเลือกสิทธิการใช้งานบน FTP Server โดยมีคุณสมบัติให้เลือกดังนี้

Write(เขียนได้), Read(อ่านได้), Delete(ลบได้), Rename(เปลี่ยนชื่อได้), List(แสดงรายชื่อในไดเรคทอรีได้) เมื่อเลือกคุณสมบัติเสร็จแล้ว ให้เลือก +



กำหนดคุณสมบัติของ FTP Server

การทดสอบ :

- ให้ทำการทดสอบ FTP เซิร์ฟเวอร์ โดยการลองโอนย้ายไฟล์จากเครื่องผู้ใช้ไปยัง FTP Server โดยมีขั้นตอนดังนี้  
เลือก PC0  $\Rightarrow$  Desktop  $\Rightarrow$  Command Prompt ใช้คำสั่งดังต่อไปนี้

```

PC>
PC>? <ENTER> (แสดงคำสั่งทั้งหมดที่ Packet Tracer สนับสนุน)
Available Commands:
?           Display the list of available commands
arp         Display the arp table
delete     Deletes the specified file from C: directory.
dir         Displays the list of files in C: directory.
ftp         Transfers files to and from a computer running an FTP server.
help        Display the list of available commands
ipconfig    Display network configuration for each network adapter
ipv6config  Display network configuration for each network adapter
netstat     Displays protocol statistics and current TCP/IP network
            connections
nslookup   DNS Lookup
ping       Send echo messages
snmpget    SNMP GET
snmpgetbulk SNMP GET BULK
snmpset    SNMP SET
ssh        ssh client

```

```

telnet      Telnet client
tracert     Trace route to destination
PC>dir <ENTER> (แสดงข้อมูลในไดเรคทรีปัจจุบัน สำหรับใน Packet Tracer ได้
เตรียมไฟล์ไว้ให้ 1 ไฟล์คือ sampleFile.txt)
Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\

2/7/2106  13:28 PM    26          sampleFile.txt
                           26 bytes      1 File(s)

PC>ftp 192.168.0.100 <ENTER> (เชื่อมต่อไปยัง FTP Server)
Trying to connect...192.168.0.100
Connected to 192.168.0.100
220- Welcome to PT Ftp server
Username:user1 <ENTER> (ป้อนรายชื่อผู้ใช้ที่ลงทะเบียนไว้บน FTP Server)
331- Username ok, need password
Password:Passwd#1 <ENTER> (ป้อนรหัสผ่านที่ลงทะเบียนไว้บน FTP Server)
230- Logged in
(passive mode On) (การ login สำเร็จ และเป็นโหมด Passive )

ftp>put sampleFile.txt <ENTER> (โอนข้อมูลจากเครื่องผู้ใช้ชื่อ sampleFile.txt
ไปเก็บไว้บนเครื่อง FTP Server)
Writing file sampleFile.txt from 192.168.0.100:
File transfer in progress...

[Transfer complete - 26 bytes]
26 bytes copied in 0.141 secs (184 bytes/sec) (การโอนข้อมูลสำเร็จ)

ftp>dir <ENTER> (ตรวจสอบรายการไฟล์ข้อมูลที่อยู่บน FTP Server)
Listing /ftp directory from 192.168.0.100:

0 : c1841-advipsericesk9-mz.124-15.T1.bin           33591768
1 : c1841-ipbase-mz.123-14.T7.bin                  13832032
2 : c1841-ipbasek9-mz.124-12.bin                 16599160
3 : c2600-advipsericesk9-mz.124-15.T1.bin           33591768
4 : c2600-i-mz.122-28.bin                          5571584
5 : c2600-ipbasek9-mz.124-8.bin                   13169700
6 : c2800nm-advipsericesk9-mz.124-15.T1.bin       50938004
7 : c2800nm-ipbase-mz.123-14.T7.bin                5571584
8 : c2800nm-ipbasek9-mz.124-8.bin                15522644

```

9 : c2950-i6q4l2-mz.121-22.EA4.bin	3058048
10 : c2950-i6q4l2-mz.121-22.EA8.bin	3117390
11 : c2960-lanbase-mz.122-25.FX.bin	4414921
12 : c2960-lanbase-mz.122-25.SEE1.bin	4670455
13 : c3560-advipservicesk9-mz.122-37.SE1.bin	8662192
14 : pt1000-i-mz.122-28.bin	5571584
15 : pt3000-i6q4l2-mz.121-22.EA4.bin	3117390
16 : sampleFile.txt	26

ftp>**get sampleFile.txt <ENTER>** (ทดสอบการโอนย้ายข้อมูลกลับจาก FTP Server  
มายังเครื่องผู้ใช้)

Reading file sampleFile.txt from 192.168.0.100:  
File transfer in progress...

[Transfer complete - 26 bytes]

26 bytes copied in 0.109 secs (238 bytes/sec) (การโอนย้ายสำเร็จ)



### Scenario 15: การติดตั้งทีโอพทีพีเซิร์ฟเวอร์ (TFTP)

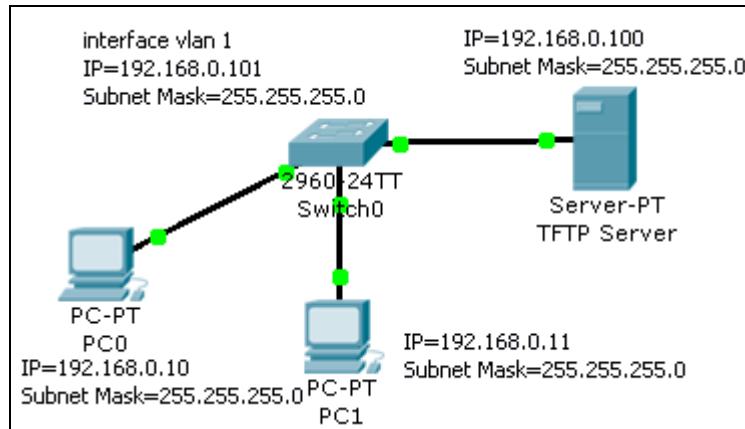
คำอธิบาย :

TFTP เป็นกระบวนการรับส่งไฟล์ที่เรียบง่ายกว่า FTP โดยใช้กลไกการสื่อสารแบบ UDP (User Datagram Protocol) ซึ่งเป็นโปรโตคอลที่ทำงานแบบ Connectionless ผู้ใช้ไม่จำเป็นต้องใส่รหัสผ่าน (Password) แต่จะต้องจัดเตรียมข้อมูลที่จะโอนย้ายไว้ก่อนเสมอ TFTP จะมีคุณสมบัติเพิ่มเติมอี่นๆ ให้ผู้ใช้ปรับแต่งได้เล็กน้อย เช่น การแสดงรายชื่อไฟล์, การเปลี่ยนໄดเร็คทอรี เป็นต้น

กลไกการทำงานของ TFTP จะกำหนดขนาดของบล็อกข้อมูลที่โอนย้ายไว้ 512 ไบต์คงที่ และมีขนาดของการรับส่งข้อมูลที่ต้องเป็น 512 ไบต์เข่นกัน การรับส่งข้อมูลในแต่ละบล็อก ผู้ส่งจะต้องรอให้ผู้รับยืนยันความถูกต้องของข้อมูลบล็อกที่ได้รับก่อน จึงจะสามารถส่งข้อมูลบล็อกต่อไปได้ กรณีที่ไม่มีการยืนยันความถูกต้องของข้อมูลในเวลาที่กำหนด (timeout) จะถือว่าไม่มีผู้รับข้อมูลดังกล่าว และจะต้องส่งข้อมูลหรือยืนยันความถูกต้องใหม่อีกครั้งหนึ่ง (retransmit) แต่ถ้าหากเกิดปัญหาขึ้นในระหว่างการรับส่งข้อมูลการทำงานจะถูกยกเลิกและ TFTP ก็ไม่สามารถจะรับส่งข้อมูลต่อจากส่วนเดิมได้ ใน TFTP ได้รับการพัฒนาประสิทธิภาพต่อมา ให้ผู้รับและผู้ส่งสามารถกำหนดขนาดของบล็อกได้ตั้งแต่ 8 – 64 ไบต์ กำหนดระยะเวลา Timeout ได้ตั้งแต่ 1 ถึง 255 วินาที รวมทั้งกำหนดขนาดของไฟล์ที่จะรับส่งกัน การทำงานของ TFTP จะไม่เซ็บช้อน ดังนั้นโปรแกรมที่ใช้งานจะมีขนาดเล็ก ใช้เนื้อที่ในหน่วยความจำน้อย สามารถบรรจุโปรแกรมลงในชิปประเภทที่เป็น Programmable Read-Only Memory (PROM) เพื่อนำไปใช้งานในเครื่องที่ใช้พกพาหรือเครื่องขนาดเล็กได้ง่ายกว่าการใช้โปรแกรมประเภท FTP ใน Scenario นี้จะใช้ TFTP เพื่อสำรองไฟล์คอนฟิกและระบบปฏิบัติการของอุปกรณ์เครือข่าย เช่น สวิชต์, เร��เตอร์ เป็นต้น

หมายเหตุ: ข้อมูล TFTP อ้างอิงจาก <http://wich246.tripod.com/tftp.htm>

แผนผังการเชื่อมต่อ :



ขั้นตอนการเชื่อมต่อ :

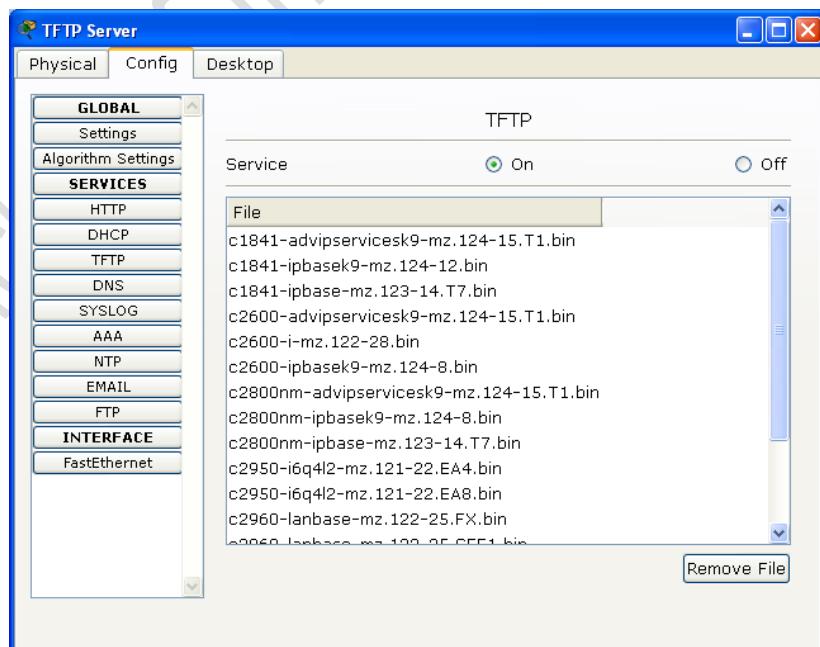
- ให้ทำการเชื่อมต่ออุปกรณ์ต่างๆ ดังผังเครือข่ายด้านบน และค่อนพิกค่าต่างๆ ดังนี้  
บนเครื่อง PC0, PC1

PC0: IP Address = 192.168.0.10, Subnet Mask = 255.255.255.0

PC2: IP Address = 192.168.0.11, Subnet Mask = 255.255.255.0

#### บนเครื่อง TFTP Server (แท็บ Config)

IP Address = 192.168.0.100, Subnet Mask = 255.255.255.0 และตรวจสอบว่า TFTP อยู่ในสถานะ on หรือไม่ ถ้าไม่ให้เลือกเป็น on โดยปกติบนเครื่อง TFTP จะมีรายชื่อของไฟล์ที่เคยสำรองไว้แล้ว



กำหนดคุณสมบัติของ TFTP Server

- บนอุปกรณ์สวิตช์ L2 (Switch 0) ให้ทำการกำหนดหมายเลขไอพีให้กับ vlan 1 เนื่องจาก ในทางทฤษฎีอุปกรณ์ที่ทำงานอยู่ในระดับแลเยอร์ 2 จะไม่จำเป็นต้องใช้

หมายเลขอ้อฟี แต่ปัจจุบันอุปกรณ์ L2 บางตัวจะต้องถูก monitoring เพื่อหาจุดบกพร่อง หรือประเมินประสิทธิภาพ จึงอนุญาตอุปกรณ์ดังกล่าวสามารถมีอ้อฟีเพื่อ monitor ได้ โดยที่ว่าจะกำหนดไว้บน vlan 1 เช่น

บน Switch 0: โหมด Configure

```
Switch(config)# interface vlan 1
Switch(config-if)#ip address 192.168.0.101 255.255.255.0 <ENTER>
(กำหนดให้ vlan 1 บนสวิชต์ L2 มีหมายเลขอ้อฟี)
Switch(config-if)#end <ENTER> ออกจากโหมดคอนฟิก ไปยังโหมด admin
Switch#ping 192.168.0.100 <ENTER> ทดสอบ ping เครื่อง TFTP server
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/28/32 ms
จากผลลัพธ์ข้างต้นแสดงว่า ping สำเร็จ
```

การทดสอบ :

- ให้ทำการทดสอบ TFTP เซิร์ฟเวอร์ โดยการสำรองไฟล์คอนฟิกและ IOS (Backup) จากสวิชต์ไปยัง TFTP Server โดยมีขั้นตอนดังนี้

Switch 0: โหมด admin

```
Switch#copy running-config tftp: <ENTER> สำรองไฟล์คอนฟิก (running-config)
จากเครื่องสวิชต์ไปยัง tftp server
Address or name of remote host []? 192.168.0.100 <ENTER> กำหนดอ้อฟีของ
tftp server ที่ต้องการส่งไฟล์ไปเก็บไว้
Destination filename [Switch-config]? Room2Floor2-281110 <ENTER> กำหนด
ชื่อของไฟล์ที่ต้องการสำรอง ควรจะตั้งชื่อให้สื่อถึงสถานที่ที่อุปกรณ์ดังกล่าวติดตั้งอยู่
```

Writing running-config...!!

[OK - 1024 bytes]

1024 bytes copied in 0.078 secs (13000 bytes/sec)

การโอนย้ายสำเร็จ จากนั้นให้เปิดดูที่ TFTP server จะมีไฟล์ดังกล่าวปรากฏอยู่

- ทดสอบการโอนย้ายไฟล์คอนฟิกกลับคืนมา (Restore)

```
Switch#copy tftp: running-config <ENTER> สำรองคืนไฟล์คอนฟิกจากเครื่อง tftp
กลับมายัง switch 0
Address or name of remote host []? 192.168.0.100 <ENTER> กำหนดอ้อฟีของ
tftp server ที่ต้องการโอนไฟล์กลับมา
Source filename []? Room2Floor2-281110 <ENTER> กำหนดชื่อของไฟล์ที่ต้องการ
```

### โอนย้ายกลับ

Destination filename [running-config]? <ENTER> กำหนดชื่อไฟล์ที่ต้องการเขียนทับในที่นี่ไม่ควรเปลี่ยนชื่อไฟล์ เพราะว่า ชื่อไฟล์คอนฟิกใน cisco เป็นค่า default คือ running-config สำหรับเก็บข้อมูลการคอนฟิกที่อยู่ในหน่วยความจำหลัก (สูญหายเมื่อปิดเครื่อง) และ startup-config เก็บคอนฟิกอยู่ในหน่วยความจำแบบไม่สูญหาย

Accessing tftp://192.168.0.100/Room2Floor2-281110...

Loading Room2Floor2-281110 from 192.168.0.100: !

[OK - 1024 bytes]

1024 bytes copied in 0.031 secs (33032 bytes/sec)

การ backup คอนฟิกสำเร็จ

### 3. ทำการสำรองและกู้คืนไฟล์ระบบปฏิบัติการหรือ IOS

Switch#**sh flash:** <ENTER> เพื่อตรวจสอบชื่อของ IOS ที่ต้องการสำรอง (สำหรับ Switch ตัวดังกล่าวจะมีชื่อว่า c2960-lanbase-mz.122-25.FX.bin สำหรับสวิตช์หรือเราเตอร์ตัวอื่นๆ จะมีชื่อที่แตกต่างกันไปตามรุ่น แต่ให้สังเกตว่าไฟล์ IOS จะมีส่วนขยายเป็น .bin เช่น)

Switch#**copy flash: tftp:** <ENTER> สั่งให้ทำการสำรอง IOS ไปยัง TFTP

Source filename []? **c2960-lanbase-mz.122-25.FX.bin** <ENTER> กำหนดชื่อไฟล์ IOS ที่ต้องการสำรอง

Address or name of remote host []? **192.168.0.100** <ENTER> ระบุอีพีของเครื่อง TFTP Server

Destination filename [**c2960-lanbase-mz.122-25.FX.bin**]? <ENTER> ตั้งชื่อ IOS (ควรใช้ค่า default)

Writing c2960-lanbase-mz.122-

**25.FX.bin...!!!!!!**

[OK - 4414921 bytes]

4414921 bytes copied in 2.594 secs (1701000 bytes/sec)

โอนย้าย IOS สำเร็จ

### ขั้นตอนการสำรอง IOS กลับจาก TFTP

Switch#**copy tftp: flash:** <ENTER> Backup IOS กลับคืนสู่สวิตช์

Address or name of remote host []? **192.168.0.100** <ENTER>

Source filename []? **c2960-lanbase-mz.122-25.FX.bin** <ENTER>

Destination filename [**c2960-lanbase-mz.122-25.FX.bin**]? <ENTER>

```
%Warning:There is a file already existing with this name  
Do you want to over write? [confirm] <ENTER>  
Erase flash: before copying? [confirm] <ENTER>  
Erasing the flash filesystem will remove all files! Continue? [confirm]  
<ENTER>  
Erasing device...  
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee...erased  
Erase of flash: complete  
Accessing tftp://192.168.0.100/c2960-lanbase-mz.122-25.FX.bin...  
Loading c2960-lanbase-mz.122-25.FX.bin from 192.168.0.100:  
!!!!!!!!!!!!!!  
[OK - 4414921 bytes]  
  
4414921 bytes copied in 2.594 secs (46242 bytes/sec)
```



## Scenario 16: การติดตั้ง Wireless Access Point

คำอธิบาย :

ระบบเครือข่ายไร้สาย (Wireless LAN: WLAN) หมายถึง เทคโนโลยีที่ช่วยให้การติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ 2 เครื่อง หรือกลุ่มของเครื่องคอมพิวเตอร์สามารถสื่อสารกันได้ ร่วมถึงการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่ายคอมพิวเตอร์ด้วยเช่นกัน โดยปราศจากการใช้สายสัญญาณในการเชื่อมต่อ แต่จะใช้คลื่นวิทยุเป็นช่องทางการสื่อสารแทน การรับส่งข้อมูลระหว่างกันจะผ่านอากาศ ทำให้ไม่ต้องเดินสายสัญญาณ และติดตั้งใช้งานได้สะดวกขึ้น

ระบบเครือข่ายไร้สายใช้แม่เหล็กไฟฟ้าผ่านอากาศ เพื่อรับส่งข้อมูลข่าวสารระหว่างเครื่องคอมพิวเตอร์ และระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่าย โดยคลื่นแม่เหล็กไฟฟ้านี้อาจเป็นคลื่นวิทยุ (Radio) หรืออินฟราเรด (Infrared) ที่ได้ การสื่อสารผ่านเครือข่ายไร้สายมีมาตรฐาน IEEE802.11 เป็นมาตรฐานกำหนดรูปแบบการสื่อสาร ซึ่งมาตรฐานแต่ละตัวจะบอกถึงความเร็ว และคลื่นความถี่สัญญาณที่แตกต่างกันใน การสื่อสารข้อมูล เช่น 802.11b และ 802.11g ที่ความเร็ว 11 Mbps และ 54 Mbps ตามลำดับ ขอบเขตของสัญญาณคลื่นบลูทูฟท์ประมาณ 100 เมตร ในพื้นที่โปร่ง และประมาณ 30 เมตร ในอาคาร ซึ่งระยะทางของสัญญาณมีผลกระทบจากสิ่งรอบข้าง หลายๆ อย่าง เช่น โทรศัพท์มือถือ ความหนาของกำแพง เครื่องใช้ไฟฟ้า อุปกรณ์อิเล็กทรอนิกส์ต่างๆ รวมถึงร่างกายมนุษย์ด้วยเช่นกัน สิ่งเหล่านี้มีผลกระทบต่อการใช้งานเครือข่ายไร้สายทั้งสิ้น

การเชื่อมต่อเครือข่ายไร้สายมี 2 รูปแบบ คือแบบ Ad-Hoc และ Infrastructure ทั้งสองรูปแบบมีการทำงานดังต่อไปนี้

### 1. การเชื่อมต่อแบบกลุ่มส่วนตัว(Ad-Hoc)

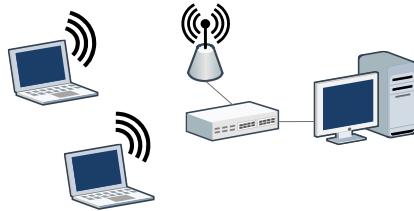
การเชื่อมต่อแบบ Ad-Hoc เป็นการเชื่อมต่อที่ประกอบด้วยเครื่องคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไปที่ติดตั้งการตัดแลนไว ทำการเชื่อมต่อสื่อสารกันโดยตรงไม่ต้องผ่านอุปกรณ์กระจายสัญญาณ (Access Point) โดยเครื่องคอมพิวเตอร์ที่เชื่อมต่อแบบนี้สามารถสื่อสารแลกเปลี่ยนข้อมูลได้ เช่น แชร์ไฟล์ เครื่องพิมพ์หรืออุปกรณ์ต่างๆ



การเชื่อมต่อแบบกลุ่มส่วนตัว(Ad-Hoc)

### 2. การเชื่อมต่อแบบกลุ่มโครงสร้าง (Infrastructure)

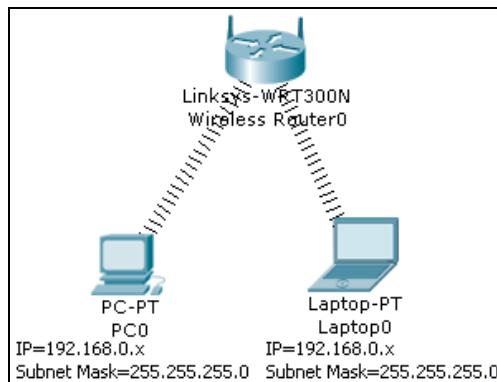
การเชื่อมต่อแบบ Infrastructure เป็นการเชื่อมต่อที่มีอุปกรณ์กระจายสัญญาณ (Access Point) เป็นตัวกลาง ทำหน้าที่รับส่งสัญญาณและข้อมูลจากเครื่องคอมพิวเตอร์ไร้สายของเครือข่ายไร้สายไปสู่เครือข่ายมีสาย หากสังเกตจะพบว่า Access Point มีการทำงานเหมือนอุปกรณ์ชี้บ (HUB) ในเครือข่ายคอมพิวเตอร์แบบมีสาย และที่สำคัญหากมีการเข้าใช้งานเครือข่ายไร้สายของเครื่องลูกข่ายในจำนวนมาก ต่อหนึ่ง Access Point จะมีผลทำให้ความเร็วของการสื่อสารเครือข่ายไร้สายช้าลงด้วยเช่นกัน



การเชื่อมต่อแบบกลุ่มโครงสร้าง (Infrastructure)

หมายเหตุ: WLAN อ้างอิงจาก <http://wise.swu.ac.th/>

แผนผังการเชื่อมต่อ :

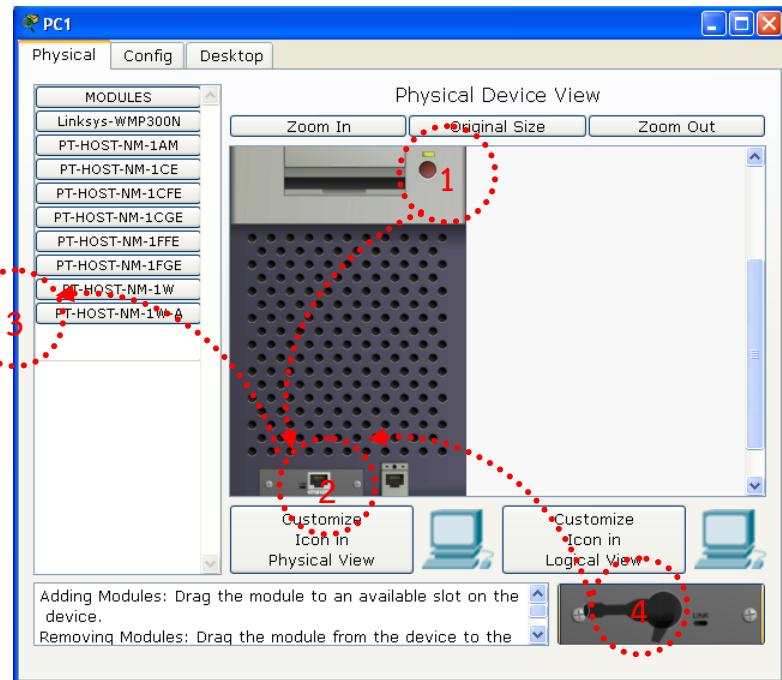


รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask
PC0	192.168.0.X	255.255.255.0
Laptop0	192.168.0.X	255.255.255.0
Wireless Router0	-	-

ขั้นตอนการเชื่อมต่อ :

- เลือก Wireless Devices  $\Rightarrow$  Linksys-WRT300N วางใน workspace
- เลือก End Devices  $\Rightarrow$  เลือก PC-PT และ Labtop-PT มาลงบน workspace
- คลิกเลือก PC0  $\Rightarrow$  แท็บ Physical  $\Rightarrow$  ปิดปุ่ม switch power ของเครื่อง PC0 แล้ว คลิกลากเน็ตเวิร์คการ์ดออกจากเครื่อง PC0 และเลือกการ์ด Wireless Lan มาใส่แทน



- ❶ ปิดปุ่ม power
- ❷ คลิกที่การ์ดเน็ตเวิร์ค
- ❸ ลาก FastEthernet ไปที่ใน MODULES (จะมีช่องว่างปรากฏ)
- ❹ คลิกลากเอาการ์ดไวเลสแลนเดิม มาวางในช่องว่างแทน FastEthernet

4. คลิกเลือก PC0  $\Rightarrow$  แท็บ Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  เลือก DHCP จะได้รับ IP Address เป็นหมายเลข 192.168.0.x (x หมายถึง IP ที่ได้รับจากการตั้งค่า DHCP จาก Wireless Access Point ซึ่งทำหน้าที่เป็น DHCP ในตัว)
5. คลิกเลือก Laptop0 ให้ทำงานขึ้นตอนเหมือน PC0 คือเปลี่ยนจาก FastEthernet ไปเป็นการ์ด Wireless แทน

#### การทดสอบ :

1. ให้ทำการทดสอบการเชื่อมต่อโดย คลิกที่ PC0  $\Rightarrow$  แท็บ Desktop  $\Rightarrow$  Command Prompt  $\Rightarrow$  แล้วทดสอบ ping ระหว่างเครื่อง PC0 กับ เครื่อง Laptop0 ว่ามีการตอบสนองหรือไม่  
บนเครื่อง PC0 (IP 192.168.0.100)

```
PC>
PC>ping 192.168.0.101 <ENTER> (ทดสอบโดยการ ping เครื่อง Laptop0)
Pinging 192.168.0.101 with 32 bytes of data:
```

```
Reply from 192.168.0.101: bytes=32 time=126ms TTL=128
Reply from 192.168.0.101: bytes=32 time=125ms TTL=128
Reply from 192.168.0.101: bytes=32 time=125ms TTL=128
Reply from 192.168.0.101: bytes=32 time=125ms TTL=128
```

```
Ping statistics for 192.168.0.101:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 125ms, Maximum = 126ms, Average = 125ms
```



### Scenario 17: การติดตั้ง Wireless Access Point (WEP Authentication)

คำอธิบาย :

เนื่องจากระบบ Wireless LAN ใช้คลื่นวิทยุในการส่ง ดังนั้นการที่ผู้ไม่ประสงค์ดีสามารถดักจับสัญญาณ และ Hack เอาข้อมูลที่มีการรับ-ส่งระหว่างเครื่องลูกข่าย (Client) กับ Access Point ใน การเข้มต่อแบบ Infrastructure หรือระหว่าง Client กับ Client ดังนั้นการใช้งาน Wireless LAN นั้น ควรที่จะต้องมีการกำหนดคุณสมบัติในด้านความปลอดภัยให้กับระบบด้วย ถ้าพูดถึงระบบ Security ของ Wireless LAN นั้น มืออยู่มากมายหลายวิธี โดยขึ้นอยู่กับอุปกรณ์แต่ละประเภท ในที่นี้ จะเป็นการกำหนด Security ที่ผู้ใช้จำเป็นต้องทำ 5 ข้อดังนี้

- เปลี่ยน SSID คือชื่อของ Network ที่เราตั้งขึ้นมาเอง โดยที่ทุกๆ เครื่องในระบบที่เข้มต่อ ด้วยต้องตั้งค่า SSID เป็นค่าเดียวกัน เมื่อซื้อ Wireless Access Point มาใหม่ๆ จะมีการตั้งค่า SSID ไว้แล้วเป็นค่า default แต่เราควรที่จะเปลี่ยนชื่อ SSID ในทันทีที่ติดตั้ง การตั้งชื่อ SSID นั้นต้องไม่เกิน 32 ตัวอักษร เช่น ITNetwork เป็นต้น

- เปลี่ยน Password สำหรับ Admin ซึ่งโดยปกติค่าเริ่มต้นจะเป็นค่าที่ง่ายๆ เช่น admin, password เป็นต้น เพราะฉะนั้นคุณจำเป็นต้องเปลี่ยน Default Password ของ Wireless Access Point ของคุณทันทีที่เริ่มติดตั้งระบบครับ

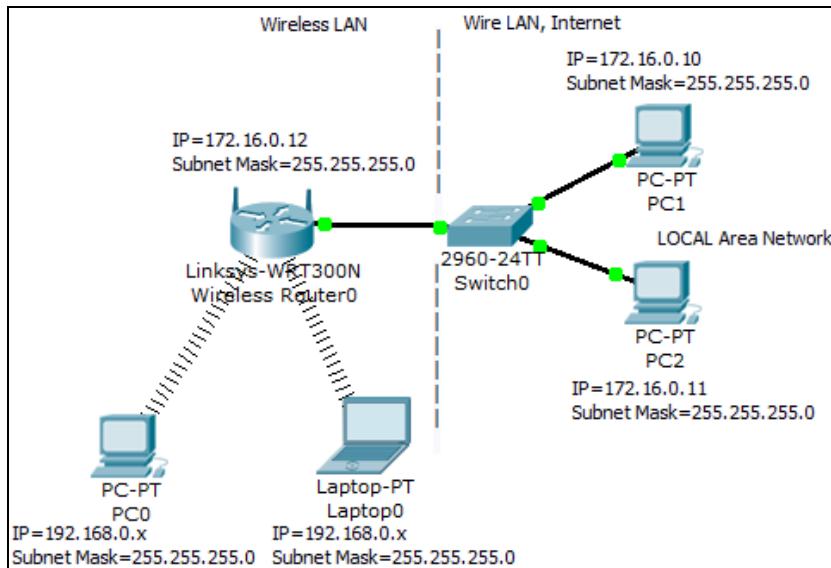
- กำหนดค่า SSID Broadcast = Disabled, SSID Broadcast คือการยอมให้เผยแพร่ SSID ให้ทุกๆ เครื่องที่อยู่ในระยะสั้งของ Wireless Access Point (AP) สามารถที่จะเห็น AP ของเรา ได้ ซึ่งเป็นสิ่งที่ดีในขณะที่เราทำการติดตั้งระบบในครั้งแรก เพราะจะทำให้ง่ายในการทดสอบระบบ และเซตเครื่องลูกข่าย แต่หลังจากที่เราติดตั้งระบบ Wireless Network เรียบร้อยแล้ว เราควรที่จะยกเลิก SSID Broadcast ในทันที เพราะการที่เราเปิดเผย SSID ของเรานั้น อาจทำให้ผู้ไม่ประสงค์ดี สามารถที่จะแอบเข้ามาในระบบ Network ของเราได้ง่ายขึ้น

- กำหนด WEP Encryption = Enabled, WEP ย่อมาจาก Wired Equivalent Privacy เป็นรูปแบบการเข้ารหัสของอุปกรณ์ Wireless LAN ที่แพร่หลายที่สุด ไม่ว่าจะเป็น Wireless Adapter รุ่นใดๆ ก็ใช้ WEP ได้, 在การเข้ารหัสแบบ WEP นั้น สามารถที่จะเลือกระดับของการเข้ารหัสได้ว่า จะใช้ 64-bit, 128-bit หรือ 256-bit โดยการใช้จำนวน Bit ที่มากขึ้นนั้น ทำให้ความเร็วในการเข้มต่อลดลง แต่ว่าจำนวน Bit ยิ่งมาก ก็ยิ่งทำให้มีความปลอดภัยมากขึ้น แต่ในปัจจุบัน WEP ถูก Hack ได้ง่ายแล้ว ส่วนการเข้ารหัสแบบใหม่ ซึ่งออกแบบ WEP นั้นมีชื่อว่า WPA ย่อมาจาก Wi-Fi Protected Access ซึ่งมีความปลอดภัยสูงมาก ปัจจุบันถึง WPA2 แล้ว

- MAC Address Filtering, MAC Address ทำหน้าที่เสมือนเลขประจำตัวของอุปกรณ์ Network ต่างๆ ซึ่งอุปกรณ์ Network ทุกชิ้นในโลกนี้ จะไม่มี MAC Address ที่ซ้ำกันเลยครับ ดังนั้น การที่เราสามารถที่จะกำหนดให้แค่เครื่องคอมพิวเตอร์ของเราเท่านั้น ที่สามารถเข้าสู่ Wireless

Network ของเราได้ ก็ย่อมที่จะเสริมความปลอดภัยให้กับระบบ Wireless LAN ของเราให้ดีขึ้นไปอีก  
ขั้นหนึ่ง

แผนผังการเชื่อมต่อ :



รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask
PC0	192.168.0.X	255.255.255.0
Laptop0	192.168.0.X	255.255.255.0
PC1	172.16.0.10	255.255.255.0
PC2	172.16.0.11	255.255.255.0
Wireless Router0	172.16.0.12	255.255.255.0

ขั้นตอนการเชื่อมต่อ :

1. เลือก Wireless Devices  $\Rightarrow$  Linksys-WRT300N วางใน workspace
2. เลือก End Devices  $\Rightarrow$  เลือก PC-PT และ Labtop-PT มาลงบน workspace
3. เครื่อง PC0 และ Labtop0 ให้เปลี่ยนการ์ดเน็ตเวิร์คจาก FastEthernet เป็น Wireless มาได้สั่น
4. เครื่อง PC1 และ PC2 ให้คอนฟิก IP Address และ Subnet Mask ตามตารางด้านบน
5. เครื่อง Wireless Router0 ให้เลือก Config  $\Rightarrow$  เมนูด้านซ้ายเลือก Internet  $\Rightarrow$  Internet Settings (เป็น IP ที่ใช้เชื่อมต่อเพื่อออกสู่อินเทอร์เน็ต)  $\Rightarrow$  ในส่วน Connection Type ให้เลือก Static และกำหนด หมายเลข IP เป็น 172.16.0.12, Subnet Mask เป็น 255.255.255.0
6. เครื่อง Wireless Router0 ให้เลือก Config  $\Rightarrow$  เมนูด้านซ้ายเลือก LAN  $\Rightarrow$  LAN Settings (เป็น IP ที่ใช้เพื่อเป็นทางออกให้กับเครื่องลูกข่ายใน Wireless LAN)  $\Rightarrow$  กำหนด หมายเลข IP เป็น 192.168.0.1, Subnet Mask เป็น 255.255.255.0

7. เครื่อง Wireless Router0 ให้เลือก Config  $\Rightarrow$  เมนูด้านซ้ายเลือก Wireless  $\Rightarrow$  Wireless Settings (กำหนดค่าการรักษาความปลอดภัยแบบ WEP)  $\Rightarrow$  ให้กำหนดค่าพารามิเตอร์ดังนี้

พารามิเตอร์	ค่าที่กำหนด	คำอธิบาย
SSID	IT01	กำหนดค่า SSID
Channel	6	กำหนดของสัญญาณในการสื่อสาร
Authentication	WEP	เลือกการเข้ารหัสการสื่อสารชนิด WEP
Key	1a2b3c4d5e	กำหนดคีย์ในการเข้ารหัส ต้องไม่น้อยกว่า 10 ตัวอักษร และเป็นเลขฐาน 16
Encryption Type	40/64 bits	เลือกขนาดของบิตในการเข้ารหัส ยิ่งมากยิ่งปลอดภัย

8. คลิกเลือก PC0  $\Rightarrow$  แท็บ Desktop  $\Rightarrow$  PC Wireless  $\Rightarrow$  เลือกแท็บ Connect ต่อจากนั้นให้กดปุ่ม Refresh 1-2 ครั้ง Wireless Access Name จะขึ้นชื่อเป็น IT01 ให้เลือก Connect  $\Rightarrow$  ในช่อง Security เลือก WEP, ในช่อง WEP เลือก 64 bit และช่อง Key 1 ให้ใส่คีย์มีค่าเป็น 1a2b3c4d5e เข้าไป  $\Rightarrow$  กดปุ่ม Connect
9. คลิกเลือก PC0  $\Rightarrow$  แท็บ Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  เลือก DHCP จะปรากฏ IP หมายเลข 192.168.0.x (x หมายถึง IP ที่ Wireless Router0 แจกให้อัตโนมัติ) จากนั้ทดสอบโดยการ ping ไปยัง IP Gateway ของตนเองคือ 192.168.0.1 และ ping ไปยังเครื่อง PC1 (IP 172.16.0.10), และ PC2 (IP 172.16.0.10) ตามลำดับ ต้องมีการตอบสนองกลับมาจากเครื่องทั้ง 3 จากนั้นให้ค่อนฟิกค่าของ Labtop0 เมื่อ้อนขั้นตอนที่กระทำกับเครื่อง PC0 ทุกประการ (เมื่อ้อนกับขั้นตอนที่ 8)

#### การทดสอบ :

1. ให้ทำการทดสอบการเชื่อมต่อโดย คลิกที่ PC0  $\Rightarrow$  แท็บ Desktop  $\Rightarrow$  Command Prompt  $\Rightarrow$  แล้วทดสอบ ping ระหว่างเครื่อง PC0 กับ เครื่อง Labtop0 ว่ามีการตอบสนองหรือไม่
- บนเครื่อง PC0 (IP 192.168.0.100)

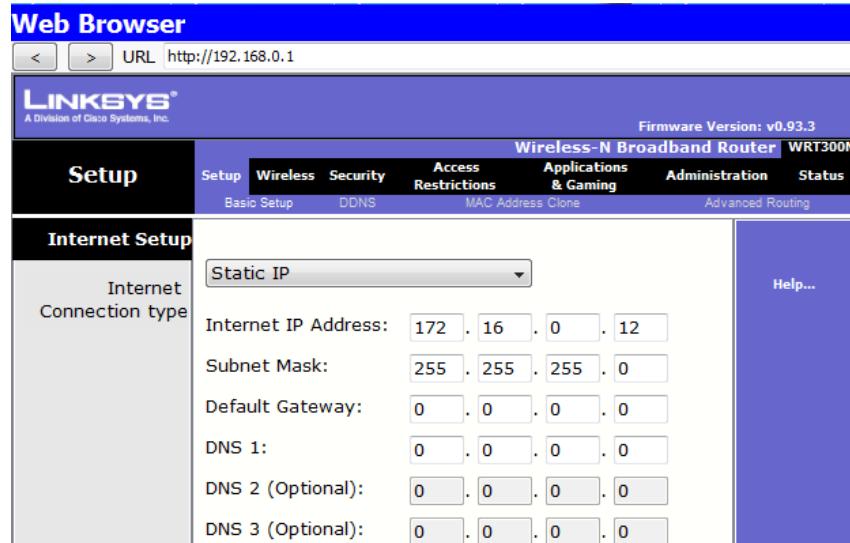
```

PC>
PC>ping 192.168.0.1 <ENTER> (ทดสอบโดยการ ping gateway)
PC>ping 192.168.0.101 <ENTER> (ทดสอบโดยการ ping เครื่อง Labtop0)
PC>ping 172.16.0.10 <ENTER> (ทดสอบโดยการ ping เครื่อง PC1)
PC>ping 172.16.0.11 <ENTER> (ทดสอบโดยการ ping เครื่อง PC2)

```

2. ทดสอบแบบที่ 2 โดยการเข้าไปจัดการค่อนฟิก Wireless Router0 โดยผ่านหน้าเว็บ เพจ (ต้องค่อนฟิกให้ Wireless Router0 เปิดการใช้งาน Web Management ก่อน โดยเข้าไปที่ Wireless Router0  $\Rightarrow$  GUI  $\Rightarrow$  Administration  $\Rightarrow$  กำหนดรหัสผ่าน (กำหนดเป็น 123)  $\Rightarrow$  เลือกลงมาด้านล่างคลิก Save Settings) ไปที่ PC0 เลือก Desktop  $\Rightarrow$  Web Browser  $\Rightarrow$  ช่อง URL ให้ใส่หมายเลข IP Gateway ของ Wireless ในที่นี่คือ 192.168.0.1 แล้วกด Go  $\Rightarrow$  จะปรากฏเมนูให้ใส่ Username และ

Password ให้ใส่ Username = admin, Password=123 แล้วกด Ok เครื่อง PC0 ก็จะสามารถคอนฟิก Wireless Router0 ผ่านเว็บเพจได้



แสดงการคอนฟิก Wireless Router0 ผ่านเว็บเพจ

สำหรับการเลือกวิธีเข้ารั้งแบบอื่นๆ จะมีหลักการคล้ายกับ WEP ซึ่งจะมีแทรกอยู่ใน Scenario อื่นๆ ต่อไป



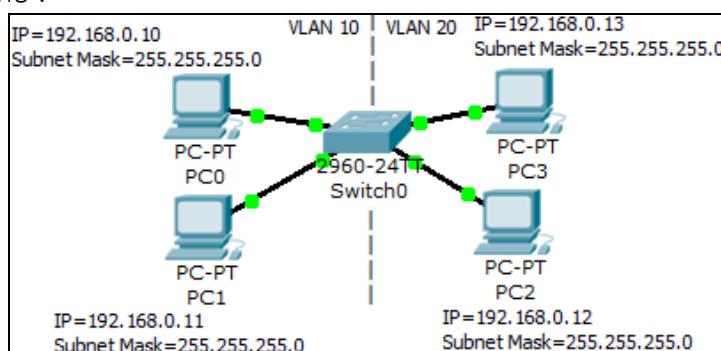
### Scenario 18: การคอนฟิก VLAN (บน switch 2900 series)

คำอธิบาย :

VLAN ย่อมาจาก Virtual LAN เป็นเทคโนโลยีที่ใช้ในการจำลองสร้างเครือข่าย LAN แต่ไม่ขึ้นอยู่กับการต่อทางกายภาพ เช่น สวิตช์หนึ่งตัวสามารถใช้จำลองเครือข่าย LAN ได้มากกว่า 1 เครือข่าย หรือสามารถใช้สวิตซ์หลายตัวจำลองเครือข่าย LAN เพียงหนึ่งเครือข่าย เป็นต้น

ในการสร้าง VLAN โดยใช้อุปกรณ์เครือข่ายหลายตัว จะมีพอร์ตที่ทำหน้าที่เชื่อมต่อระหว่างอุปกรณ์เครือข่ายแต่ละตัว เรียกว่า Trunk port ซึ่งเสมือนมีท่อเชื่อม เนื่องจาก VLAN เป็น LAN แบบจำลอง ถึงแม้ว่าจะต่อทางกายภาพอยู่บนอุปกรณ์เครือข่ายตัวเดียวกัน แต่การติดต่อกันนั้นจำเป็นต้องใช้อุปกรณ์ที่มีความสามารถในการค้นหาเส้นทาง เช่น เราเตอร์ หรือสวิตซ์แลเยอร์ 3 ในการเชื่อมต่อ VLAN ให้สามารถสื่อสารกันได้

แผนผังการเชื่อมต่อ :



รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask	VLAN
---------	------------	-------------	------

PC0	192.168.0.10	255.255.255.0	VLAN 10
PC1	192.168.0.11	255.255.255.0	VLAN 10
PC2	192.168.0.12	255.255.255.0	VLAN 20
PC3	192.168.0.13	255.255.255.0	VLAN 20
Switch0	-	-	-

ขั้นตอนการเขื่อมต่อ :

1. เลือก PC0  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.0.10, Subnet Mask=255.255.255.0
2. เลือก PC1  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.0.11, Subnet Mask=255.255.255.0
3. เลือก PC2  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.0.12, Subnet Mask=255.255.255.0
4. เลือก PC3  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.0.13, Subnet Mask=255.255.255.0
5. ทดสอบ ping จาก PC0 ไปยัง PC1, PC2, PC3 ซึ่งผลของการ ping จะมีการตอบสนองจากเครื่องปลายทางทุกๆ เครื่อง เนื่องจาก switch0 จะมี VLAN สร้างขึ้นอัตโนมัติคือ VLAN1 เสมอ ทำให้ทุกๆ เครื่องสามารถสื่อสารกันได้ทันทีเมื่อกำหนด IP Address เสร็จ การแสดงข้อมูล VLAN จะใช้คำสั่ง show vlan บนสวิตช์ โดยคลิกที่ switch0  $\Rightarrow$  CLI  $\Rightarrow$  <ENTER>

Switch>

Switch>enable <ENTER> เข้าสู่โหมดผู้ดูแลระบบ

Switch#show vlan <ENTER> แสดงรายการ VLAN

```

Switch#show vlan
Switch#show vlan

VLAN Name                               Status      Ports
---- --
1   default                             active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                         Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                         Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                         Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                         Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                         Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                         Gig1/1, Gig1/2

1002 fddi-default                       act/unsup
1003 token-ring-default                 act/unsup
1004 fdnet-default                      act/unsup
1005 trnet-default                      act/unsup

VLAN Type      SAID      MTU      Parent RingNo BridgeNo Stp      BrdgMode Trans1 Trans2
---- --
1   enet      100001    1500      -       -       -       -       0       0
1002 fddi     101002    1500      -       -       -       -       0       0
1003 tr       101003    1500      -       -       -       -       0       0
1004 fdnet    101004    1500      -       -       ieee    -       0       0
1005 trnet    101005    1500      -       -       ibm    -       0       0

```

Copy      Paste

- ① แสดง default VLAN คือ VLAN 1 จะสร้างมาพร้อมกับสวิตช์เสมอ  
 ② แสดงพอร์ตที่เป็นสมาชิกของ VLAN 1 ในเบื้องต้นทุกๆ พอร์ตจะเป็นสมาชิกของ VLAN 1 ทั้งหมด
6. เพื่อเป็นการทดสอบบุคลิสมบัติของ VLAN จะทดลองสร้าง VLAN 10 และ VLAN 20 จากนั้นกำหนดให้ เครื่อง PC0, PC1 เป็นสมาชิกของ VLAN 10 และ PC2, PC3 เป็นสมาชิกของ VLAN 20 โดยมีขั้นตอนดังนี้ คลิกที่ Switch0  $\Rightarrow$  CLI  $\Rightarrow$  <ENTER>

```
Switch>
```

```
Switch>enable <ENTER> เข้าสู่โหมดผู้ดูแลระบบ
```

```
Switch#configure terminal <ENTER> เข้าสู่โหมดการคอนฟิก
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)#interface fastEthernet 0/1 <ENTER> เข้าไปยังอินเทอร์เฟส Fa0/1
```

```
Switch(config-if)#switchport access vlan 10 <ENTER> เปลี่ยนสมาชิกจาก VLAN 1 เป็น VLAN 10 ของเครื่อง PC0
```

```
% Access VLAN does not exist. Creating vlan 10 กรณีไม่มี VLAN สวิตช์จะสร้างให้อัตโนมัติ
```

```
Switch(config-if)#exit <ENTER> ออกจาก การคอนฟิกอินเทอร์เฟส Fa0/1
```

```
Switch(config)#interface fastEthernet 0/2 <ENTER> เข้าไปยังอินเทอร์เฟส Fa0/2
```

```
Switch(config-if)#switchport access vlan 10 <ENTER> เปลี่ยนสมาชิกจาก VLAN 1 เป็น VLAN 10 ของเครื่อง PC1
```

```
Switch(config-if)#exit <ENTER> ออกจาก การคอนฟิกอินเทอร์เฟส Fa0/2
```

```
Switch(config)#interface fastEthernet 0/3 <ENTER> เข้าไปยังอินเทอร์เฟส Fa0/3
```

```
Switch(config-if)#switchport access vlan 20 <ENTER> > เปลี่ยนสมาชิกจาก VLAN 1 เป็น VLAN 20 ของเครื่อง PC2
```

```
% Access VLAN does not exist. Creating vlan 20
```

```
Switch(config-if)#exit <ENTER> ออกจาก การคอนฟิกอินเทอร์เฟส Fa0/3
```

```
Switch(config)#interface fastEthernet 0/4 <ENTER> เข้าไปยังอินเทอร์เฟส Fa0/4
```

```
Switch(config-if)#switchport access vlan 20 <ENTER> เปลี่ยนสมาชิกจาก VLAN 1 เป็น VLAN 20 ของเครื่อง PC3
```

7. แสดงการคอนฟิก VLAN อีกครั้ง โดยใช้คำสั่ง show vlan ผลที่ถูกต้องคือ จะมี VLAN ใหม่เกิดขึ้น 2 VLAN คือ VLAN 10 และ 20 ซึ่งใน VLAN 10 จะมีพอร์ตที่เป็นสมาชิกคือ Fa0/1 (PC0), Fa0/2 (PC1) และ VLAN 20 มีพอร์ตที่เป็นสมาชิกคือ Fa0/3 (PC2), Fa0/4 (PC3)

```
Switch#show vlan <ENTER>
```

VLAN Name	Status	Ports
10 VLAN0010	active	Fa0/1, Fa0/2
20 VLAN0020	active	Fa0/3, Fa0/4

8. ทดสอบ ping เมื่อนั้นข้อที่ 5 อีกครั้ง ผลที่ถูกต้องคือ เครื่อง PC0 และ PC1 จะสามารถ ping กันได้ (อยู่ใน VLAN เดียวกัน), PC2 และ PC3 สามารถ ping กันได้ แต่เครื่องที่อยู่ต่าง VLAN กันจะไม่สามารถ ping กันได้ ซึ่งเป็นไปตามคุณสมบัติของ VLAN

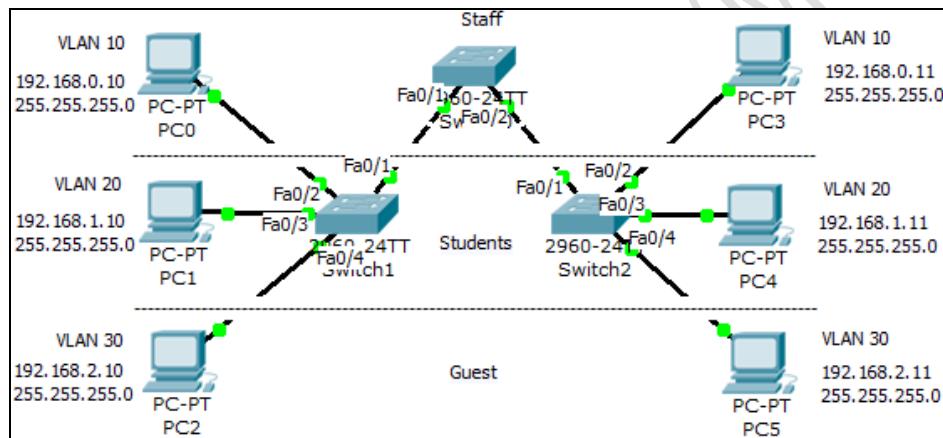


### Scenario 19: การคอนฟิก VLANs และ Trunks (บน switch 2900 series)

คำอธิบาย :

ในการสร้าง VLAN โดยใช้อุปกรณ์เครือข่ายหลายตัว จะมีพอร์ตที่ทำหน้าที่เชื่อมต่อระหว่าง อุปกรณ์เครือข่ายแต่ละตัว เรียกว่า Trunk port ซึ่งเมื่อมีท่อเชื่อม หรือ Trunk เป็นตัวเชื่อม VLAN ของแต่ละสวิตช์เข้าด้วยกัน ซึ่งเป็นการเชื่อมต่อของ VLAN ในแต่ละเครื่องที่เป็น VLAN ซึ่งเดียวกันเข้าด้วยกัน แต่ไม่สามารถเชื่อม VLAN ที่มีชื่อต่างกันเข้ากันได้ ถ้าต้องการให้ VLAN ที่แตกต่างกันสามารถสื่อสารกันได้ต้องอาศัยอุปกรณ์ที่ทำงานในレイเยอร์ที่ 3 เช่น สวิตช์เลเยอร์ 3 หรือเราเตอร์ เป็นต้น

แผนผังการเชื่อมต่อ :



รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask	VLAN
PC0	192.168.0.10	255.255.255.0	VLAN 10
PC3	192.168.0.11	255.255.255.0	VLAN 10
PC1	192.168.1.10	255.255.255.0	VLAN 20
PC4	192.168.1.11	255.255.255.0	VLAN 20
PC2	192.168.2.10	255.255.255.0	VLAN 30
PC5	192.168.2.11	255.255.255.0	VLAN 30
Switch0	-	-	Trunk Fa0/1, Fa0/2
Switch1	-	-	Trunk Fa0/1
Switch2	-	-	Trunk Fa0/1

ขั้นตอนการเชื่อมต่อ :

- เลือก PC0  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.0.10, Subnet Mask=255.255.255.0

2. เลือก PC3  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.0.11, Subnet Mask=255.255.255.0
3. เลือก PC1  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.1.10, Subnet Mask=255.255.255.0
4. เลือก PC4  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.1.11, Subnet Mask=255.255.255.0
5. เลือก PC2  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.2.10 Subnet Mask=255.255.255.0
6. เลือก PC5  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.2.11, Subnet Mask=255.255.255.0
7. เลือก Switch0  $\Rightarrow$  CLI  $\Rightarrow$  <ENTER>

บนเครื่อง Switch0

```
Switch>
Switch0>enable <ENTER> เข้าสู่โหมดผู้ดูแลระบบ
Switch0#configure terminal <ENTER> เข้าสู่โหมดการคอนฟิก
Switch0(config)#vlan 10 <ENTER> สร้าง vlan 10 บนเครื่อง Switch0
Switch0(config-vlan)#name Staff <ENTER> ตั้งชื่อให้ vlan 10 เป็นของ Staff
Switch0(config)#vlan 20 <ENTER> สร้าง vlan 20 บนเครื่อง Switch0
Switch0(config-vlan)#name Students <ENTER> ตั้งชื่อให้ vlan 20 เป็นของ Students
Switch0(config)#vlan 30 <ENTER> สร้าง vlan 30 บนเครื่อง Switch0
Switch0(config-vlan)#name Guest <ENTER> ตั้งชื่อให้ vlan 30 เป็นของ Guest
Switch0(config)#vlan 99 <ENTER> สร้าง vlan 99 บนเครื่อง Switch0 เพื่อเป็นพอร์ต manage
Switch0(config-vlan)#name Management <ENTER> ตั้งชื่อให้ vlan 99 เป็นของ Management
```

บนเครื่อง Switch0 สามารถแสดง vlan ด้วยคำสั่งดังต่อไปนี้

```
Switch0#show vlan <ENTER> แสดงรายการ vlan ทั้งหมดบน Switch0
```

VLAN Name	Status	Ports
10 Staff	active	
20 Students	active	
30 Guest	active	
99 Management	active	

8. บน Switch1, Switch2 ให้ทำการสร้าง vlan เมื่อกับ Switch0 ทุกประการ
9. ทำการเปลี่ยนสมาชิกของพอร์ตเข้าสู่ vlan ที่กำหนด บน Switch1 และ Switch2

บนเครื่อง Switch1 ให้ทำการเปลี่ยนพอร์ต Fa0/2 เข้า vlan 10, Fa0/3 เข้า vlan 20, Fa0/4 เข้า vlan 30

```
Switch1(config-if)#interface fastEthernet 0/2 <ENTER> เข้าสู่อินเทอร์เฟส Fa0/2
Switch1(config-if)#switchport mode access <ENTER>
Switch1(config-if)#switchport access vlan 10 <ENTER> ย้ายจาก vlan 1 เข้าสู่ vlan 10
```

```

Switch1(config-if)#interface fastEthernet 0/3 <ENTER> เข้าสู่อินเทอร์เฟส Fa0/3
Switch1(config-if)#switchport mode access <ENTER>
Switch1(config-if)#switchport access vlan 20 <ENTER> ย้ายจาก vlan 1 เข้าสู่ vlan 20
Switch1(config-if)#interface fastEthernet 0/4 <ENTER> เข้าสู่อินเทอร์เฟส Fa0/4
Switch1(config-if)#switchport mode access <ENTER>
Switch1(config-if)#switchport access vlan 30 <ENTER> ย้ายจาก vlan 1 เข้าสู่ vlan 30

```

10. บน Switch2 ให้ทำการย้ายพอร์ตเข้าสู่ vlan เมื่อตอนที่ 9 ทุกประการ

11. ทำการสร้าง Trunking ระหว่าง Switch0 กับ Switch1 และ Switch0 กับ Switch2

บน Switch0

```

Switch0(config)#interface fastEthernet 0/1 <ENTER> เข้าสู่อินเทอร์เฟส Fa0/1
Switch0(config-if)#switchport mode trunk <ENTER> เปลี่ยนเป็นโหมด Trunk
Switch0(config-if)#switchport trunk native vlan 99 <ENTER> กำหนด Fa0/1 ให้เข้าสู่
vlan 99 ซึ่งเป็น Trunk port
Switch(config)#interface fastEthernet 0/2 <ENTER> เข้าสู่อินเทอร์เฟส Fa0/2
Switch(config-if)#switchport mode trunk <ENTER> เปลี่ยนเป็นโหมด Trunk
Switch(config-if)#switchport trunk native vlan 99 <ENTER> กำหนด Fa0/2 ให้เข้าสู่ vlan
99 ซึ่งเป็น Trunk port

```

บน Switch1 ทำการสร้าง vlan trunk ดังนี้

```

Switch1(config)#interface fastEthernet 0/1 <ENTER> เข้าสู่อินเทอร์เฟส Fa0/1
Switch1(config-if)#switchport mode trunk <ENTER> เปลี่ยนเป็นโหมด trunk
Switch1(config-if)#switchport trunk native vlan 99 <ENTER> ย้ายจาก vlan 1 เข้าสู่ vlan
99 ซึ่งเป็นโหมด trunk

```

บน Switch2 ทำการสร้าง vlan trunk ดังนี้

```

Switch2(config)#interface fastEthernet 0/1 <ENTER> เข้าสู่อินเทอร์เฟส Fa0/1
Switch2(config-if)# switchport mode trunk <ENTER> เปลี่ยนเป็นโหมด trunk
Switch2(config-if)# switchport trunk native vlan 99 <ENTER> ย้ายจาก vlan 1 เข้าสู่
vlan 99 ซึ่งเป็นโหมด trunk

```

การทดสอบ :

- ให้ทำการทดสอบการเชื่อมต่อโดย การ ping ภายใน vlan โดยกัน คือ PC0 และ PC3, PC2 และ PC4, PC3 และ PC5 ต้องสามารถเชื่อมต่อกันได้ แต่ถ้า ping ข้าม vlan จะไม่สามารถ ping กันได้



#### Scenario 20: การคอนฟิก VTP (บน switch 2900 series)

คำอธิบาย :

VTP = Virtual Trunking Protocol เป็นโปรโตคอลที่ช่วยให้ง่ายต่อการสร้าง VLAN ในสวิตซ์บนเครือข่าย ถ้าเป็น cisco จะนิยามว่าเป็นโปรโตคอลพิเศษที่ใช้เพื่อช่วยให้ง่ายต่อการสร้าง ลบ และเปลี่ยนชื่อของ VLAN ในเน็ตเวิร์ค ผ่านพอร์ต Trunk สิ่งที่ต้องศึกษาและต้องรู้ในเรื่อง VTP ก็คือ

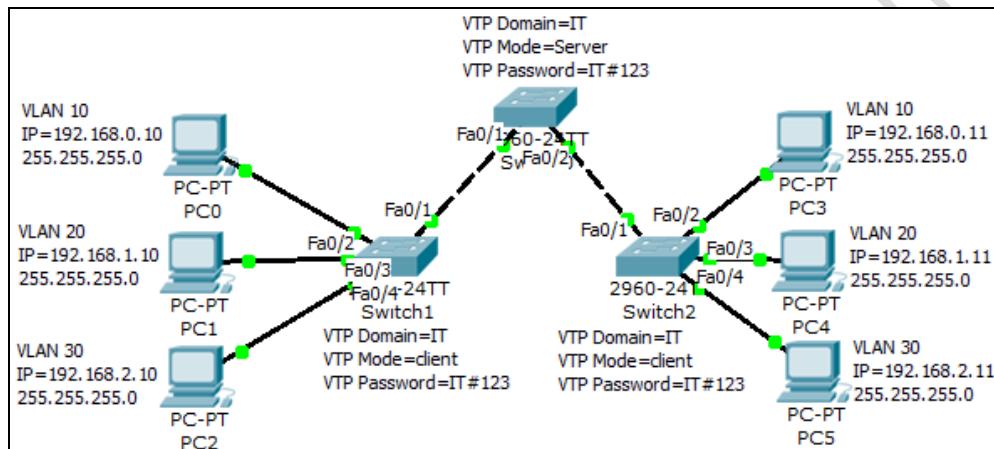
VTP Domains กำหนดชื่อของ VTP Domain

VTP Modes กำหนด Mode การทำงานของ Domain

VTP Password กำหนด Password เพื่อป้องกัน Domain

VTP เอาไว้ใช่ว่าเราที่เราต้องการเช็ต VLAN บนสวิตซ์หลายตัวครับ โดยเราจะทำการสร้าง VLAN DATABASE ขึ้นมาที่สวิตซ์ตัวหนึ่ง แล้วตั้งให้เป็น VTP Server จากนั้นที่สวิตซ์ตัวอื่นๆ ก็ตั้งให้เป็น VTP Client โดยที่ Server และ Client ต้องอยู่ใน VTP Domains เดียวกัน หลังจากนั้นก็ enable โพรโทคอลให้สวิตซ์สื่อสารถึงกัน ตัว Client ก็จะรับ VLAN Database มาจาก Server โดยอัตโนมัติ โดยที่เราไม่ต้องเข้าไปสร้างเองในทุกๆ สวิตซ์ VTP จะมีประโยชน์มากถ้าเราต้องสร้าง VLAN โดยใช้สวิตซ์หลายตัว

แผนผังการเชื่อมต่อ :



รายการอุปกรณ์ :

อุปกรณ์	IP Address	Subnet Mask	VLAN
PC0	192.168.0.10	255.255.255.0	VLAN 10
PC3	192.168.0.11	255.255.255.0	VLAN 10
PC1	192.168.1.10	255.255.255.0	VLAN 20
PC4	192.168.1.11	255.255.255.0	VLAN 20
PC2	192.168.2.10	255.255.255.0	VLAN 30
PC5	192.168.2.11	255.255.255.0	VLAN 30
Switch0	-	-	Trunk Fa0/1, Fa0/2

ขั้นตอนการเชื่อมต่อ :

- เลือก PC0  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.0.10, Subnet Mask=255.255.255.0
- เลือก PC3  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.0.11, Subnet Mask=255.255.255.0
- เลือก PC1  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.1.10, Subnet Mask=255.255.255.0

4. เลือก PC4  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.1.11, Subnet Mask=255.255.255.0
5. เลือก PC2  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.2.10 Subnet Mask=255.255.255.0
6. เลือก PC5  $\Rightarrow$  Desktop  $\Rightarrow$  IP Configuration  $\Rightarrow$  กำหนดหมายเลข IP เป็น 192.168.2.11, Subnet Mask=255.255.255.0
7. เลือก Switch0  $\Rightarrow$  CLI  $\Rightarrow$  <ENTER>

บันเครื่อง Switch0

```

Switch0#configure terminal <ENTER> เข้าสู่โหมดการคอนฟิก
Switch0(config)#vtp domain IT <ENTER> กำหนดโดเมนชื่อ IT
Switch0(config)#vtp mode server <ENTER> กำหนดโหมดการทำงานเป็น server
Switch0(config)#vtp password IT#123 <ENTER> กำหนดรหัสผ่านของโดเมน IT
Switch0(config)#vlan 10 <ENTER> สร้าง vlan 10 บนเครื่อง Switch0
Switch0(config-vlan)#name Staff <ENTER> ตั้งชื่อให้ vlan 10 เป็นของ Staff
Switch0(config-vlan)#exit <ENTER>
Switch0(config)#vlan 20 <ENTER> สร้าง vlan 20 บนเครื่อง Switch0
Switch0(config-vlan)#name Students <ENTER> ตั้งชื่อให้ vlan 20 เป็นของ Students
Switch0(config-vlan)#exit <ENTER>
Switch0(config)#vlan 30 <ENTER> สร้าง vlan 30 บนเครื่อง Switch0
Switch0(config-vlan)#name Guest <ENTER> ตั้งชื่อให้ vlan 30 เป็นของ Guest
Switch0(config-vlan)#exit <ENTER>
Switch0(config)#vlan 99 <ENTER> สร้าง vlan 99 บนเครื่อง Switch0 เพื่อเป็นพอร์ต manage
Switch0(config-vlan)#name Management <ENTER> ตั้งชื่อให้ vlan 99 เป็นของ Management
Switch0(config-vlan)#exit <ENTER>
Switch0(config)#interface fastEthernet 0/1 <ENTER> เข้าสู่อินเทอร์เฟส Fa0/1
Switch0(config-if)#switchport mode trunk <ENTER> เปลี่ยนเป็นโหมด Trunk
Switch0(config-if)#switchport trunk native vlan 99 <ENTER> กำหนด Fa0/1 ให้เข้าสู่ vlan 99 ซึ่งเป็น Trunk port
Switch0(config-vlan)#exit <ENTER>
Switch(config)#interface fastEthernet 0/2 <ENTER> เข้าสู่อินเทอร์เฟส Fa0/2
Switch(config-if)#switchport mode trunk <ENTER> เปลี่ยนเป็นโหมด Trunk
Switch(config-if)#switchport trunk native vlan 99 <ENTER> กำหนด Fa0/2 ให้เข้าสู่ vlan 99 ซึ่งเป็น Trunk port
Switch0(config-vlan)#exit <ENTER>

```

8. บัน Switch1, Switch2 ให้ทำการคอนฟิกเฉพาะ vtp domain, mode และรหัสผ่าน เท่านั้น ข้อมูล vlan ทั้งหมดจะถูกสำเนาจาก Switch0 ทันที
- บันเครื่อง Switch1, Switch2 ให้คอนฟิกเหมือนกันดังนี้

```

Switch1#configure terminal <ENTER> เข้าสู่โหมดการคอนฟิก
Switch1(config)#vtp domain IT <ENTER> กำหนดโดเมนชื่อ IT
Switch1(config)#vtp mode client <ENTER> กำหนดโหมดการทำงานเป็น client
Switch1(config)#vtp password IT#123 <ENTER> กำหนดรหัสผ่านของโดเมน IT

```

การทดสอบ :

- ทดสอบว่าเครื่อง Switch1, Switch2 ได้รับข้อมูลของ vlan มาเรียบร้อยแล้ว โดยใช้คำสั่ง show vlan
- ให้ทำการทดสอบการเชื่อมต่อโดย การ ping ภายใน vlan เดียวกัน คือ PC0 และ PC3, PC2 และ PC4, PC3 และ PC5 ต้องสามารถเชื่อมต่อ กันได้ แต่ถ้า ping ข้าม vlan จะไม่สามารถ ping กันได้
- ทดสอบโดยการทำงานของ VTP โดยใช้คำสั่ง show vtp status

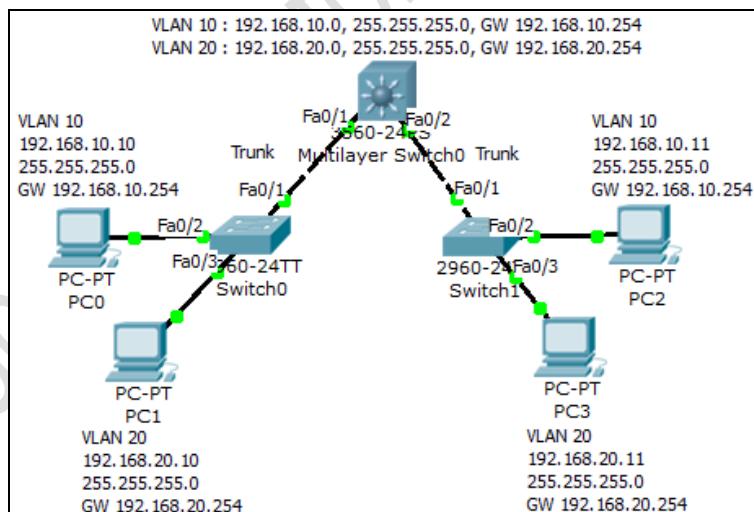


### Scenario 21: การคอนฟิก Switch L3 to L2 InterVLANS (Trunk Port)

คำอธิบาย :

จากที่กล่าวมาแล้วใน Scenario ที่ 20 ว่าเมื่อต้องการเชื่อม vlan ที่สร้างใน switch L2 หลายๆ vlan ให้สามารถเชื่อมต่อกันได้ต้องอาศัย อุปกรณ์ที่ทำงานในระดับเลเยอร์ที่ 3 ใน Scenario นี้จึงขอแนะนำการเชื่อม vlan ใน switch L2 ให้สามารถคุยกันข้าม vlan ได้

แผนผังการเชื่อมต่อ :



จากรูป switch L2 จะสร้าง vlan ไว้ 2 vlan คือ vlan 10 และ 20 โดยพอร์ต Fa0/1 จะทำหน้าที่เป็น Trunk เพื่อเชื่อมไปยัง switch L3 ใน switch L3 จะสร้าง vlan 10 และ 20 เช่นเดียวกับ switch L2 เช่น เดียวกัน แต่มีการกำหนดหมายเลข IP ให้กับ vlan 10 คือ 192.168.10.254, Subnet Mask คือ 255.255.255.0 และ vlan 20 กำหนดเป็น 192.168.20.254, 255.255.255.0 เพื่อรับการเชื่อมต่อที่มาจาก switch L2 (ถ้า switch L2 มีจำนวนมากๆ อาจจะประยุกต์เอาวิธีการแบบ vtp มาใช้แทนการสร้าง vlan แบบ manual ก็ได้) สำหรับเครื่อง PC ให้กำหนดหมายเลข IP, Subnet Mask และ Gateway (ใช้อักษรย่อคือ GW) ตามรูป

ขั้นตอนการคอนฟิก :

1. บนเครื่อง Switch0 และ Switch1 (Switch L2) ให้คอนฟิกเหมือนกันทุกประการ โดยสร้าง vlan 10, 20 บน Switch database

! สร้าง vlan 10 และ 20

```
Layer2-Switch#configure terminal <ENTER>
```

```
Layer2-Switch(config)#vlan 10 <ENTER>
```

```
Layer2-Switch(config-vlan)#end <ENTER>
```

```
Layer2-Switch(config)#vlan 20 <ENTER>
```

```
Layer2-Switch(config-vlan)#end <ENTER>
```

! กำหนดให้พอร์ต Fa0/2 เป็นสมาชิก vlan 10

```
Layer2-Switch(config)#interface fastethernet0/2 <ENTER>
```

```
Layer2-Switch(config-if)#switchport mode access <ENTER>
```

```
Layer2-Switch(config-if)#switchport access vlan 10 <ENTER>
```

```
Layer2-Switch(config-if)#end <ENTER>
```

! กำหนดให้พอร์ต Fa0/3 เป็นสมาชิก vlan 20

```
Layer2-Switch(config)#interface fastethernet0/3 <ENTER>
```

```
Layer2-Switch(config-if)#switchport mode access <ENTER>
```

```
Layer2-Switch(config-if)#switchport access vlan 20 <ENTER>
```

```
Layer2-Switch(config-if)#end <ENTER>
```

! สร้าง Trunk บน Fa0/1

```
Layer2-Switch(config)#interface fastethernet0/1 <ENTER>
```

```
Layer2-Switch(config-if)#switchport mode trunk <ENTER>
```

```
Layer2-Switch(config-if)#switchport trunk encapsulation dot1q <ENTER>
```

```
Layer2-Switch(config-if)#end <ENTER>
```

2. บนเครื่อง Multilayer Switch (Switch L3) สร้าง vlan 10, 20 และ Trunk

! สร้าง vlan database คือ vlan 10, 20

```
Layer3-Switch#configure terminal <ENTER>
```

```
Layer3-Switch(config)#vlan 10 <ENTER>
```

```
Layer3-Switch(config-vlan)#end <ENTER>
```

```
Layer3-Switch(config)#vlan 20 <ENTER>
```

```
Layer3-Switch(config-vlan)#end <ENTER>
```

! สร้าง Trunk พอร์ต บน Fa0/1 และ Fa0/2

```
Layer3-Switch(config)#interface fastethernet0/1 <ENTER>
```

```

Layer3-Switch(config-if)#switchport mode trunk <ENTER>
Layer3-Switch(config-if)#switchport trunk encapsulation dot1q <ENTER>
Layer3-Switch(config-if)#end <ENTER>
Layer3-Switch(config)#interface fastethernet0/2 <ENTER>
Layer3-Switch(config-if)#switchport mode trunk <ENTER>
Layer3-Switch(config-if)#switchport trunk encapsulation dot1q <ENTER>
Layer3-Switch(config-if)#end <ENTER>

```

! คอนฟิก IP, Subnet Mask และ Gateway ให้ vlan 10, 20

```

Layer3-Switch(config)#interface vlan10 <ENTER>
Layer3-Switch(config-if)#ip address 192.168.10.254 255.255.255.0 <ENTER>
Layer3-Switch(config-if)#no shut <ENTER>
Layer3-Switch(config)#interface vlan20 <ENTER>
Layer3-Switch(config-if)#ip address 192.168.20.254 255.255.255.0 <ENTER>
Layer3-Switch(config-if)#no shut <ENTER>

```

3. ที่เครื่อง PC0, PC1, PC2, PC3 ให้กำหนด IP, Subnet Mask และ Gateway  
ดังต่อไปนี้

PC0 : IP=192.168.10.10, Subnet Mask=255.255.255.0, GW=192.168.10.254

PC1 : IP=192.168.20.10, Subnet Mask=255.255.255.0, GW=192.168.20.254

PC2 : IP=192.168.10.11, Subnet Mask=255.255.255.0, GW=192.168.10.254

PC3 : IP=192.168.20.11, Subnet Mask=255.255.255.0, GW=192.168.20.254

การทดสอบ :

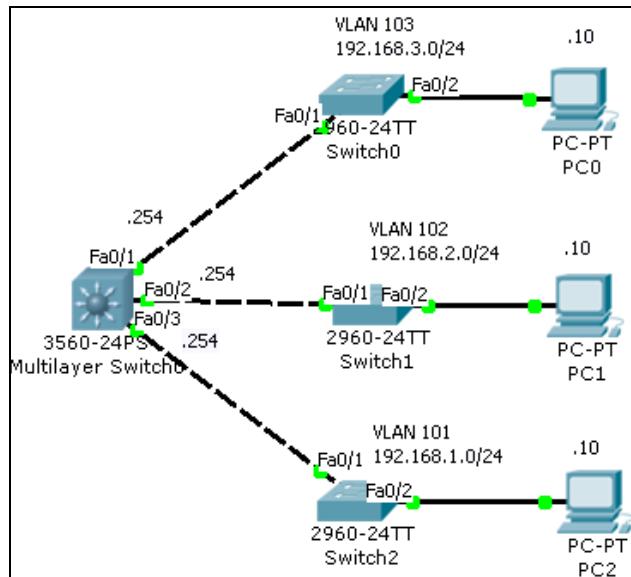
1. ทดสอบโดยการ ping จาก PC0 ไปยังเครื่อง PC1, PC2 และ PC3 ทุกๆ เครื่องต้องสามารถสื่อสารกันได้ทั้งหมด



### Scenario 22: การคอนฟิก Switch L3 InterVLANs (Route VLAN)

คำอธิบาย :

ใน Scenario นี้จะกล่าวถึงการสร้าง vlan บนอุปกรณ์แลเยอร์ 3 ซึ่งอุปกรณ์ดังกล่าวมีคุณสมบัติการเร้าต์ระหว่าง vlan อญ্যแລ้ว โดยไม่จำเป็นต้องใช้ Trunk แต่อุปกรณ์แลเยอร์ที่ 2 ที่นำมาเชื่อมต่อกับอุปกรณ์แลเยอร์ที่ 3 ควรจะทำหน้าที่เป็นแค่ access เท่านั้น ไม่ควรทำ vlan ที่สวิตช์ L2 เพิ่มอีก (ใช้เฉพาะ vlan 1 ที่เป็นค่า default เท่านั้น) สรุปคืออุปกรณ์ในแลเยอร์ 2 จะทำหน้าที่เป็นแค่อุปกรณ์ที่เชื่อมต่ออุปกรณ์ปลายทาง เช่น PC, printer เป็นต้น เข้าสู่เครือข่ายเท่านั้น  
แผนผังการเชื่อมต่อ :



จากรูป switch L3 (3560) จะสร้าง vlan ไว้ 3 vlan คือ vlan 101 (192.168.1.0/24 และ gateway คือ .254), vlan 102 (192.168.2.0/24), vlan 103 (192.168.3.0/24) และให้ port Fa0/1 เป็นสมาชิก vlan 101, Fa0/2 เป็นสมาชิก vlan 102 และ Fa0/3 เป็นสมาชิก vlan 103 ตามลำดับ โดยมีสวิชต์ L2 ทำหน้าที่เชื่อมต่ออุปกรณ์ปลายทางเข้าสู่เครือข่ายผ่าน vlan 1 เครื่องลูกข่ายจะกำหนดให้เป็นสมาชิกของแต่ละ vlan โดยใช้หมายเลขไอพีคือ .10 (สำหรับเครื่องหมายเหลือไว้ .10 ที่อยู่บน vlan 101 จะกำหนดค่าดังนี้ IP=192.168.1.10, subnet=255.255.255.0, gateway=192.168.1.254) ตามรูป

#### ขั้นตอนการคอนฟิก :

1. บนเครื่องสวิชต์ L3 (3560) สร้าง vlan 101, 102, 103 และกำหนดอิปีให้กับแต่ละ vlan ดังนี้

```
! สร้าง vlan 101, 102, 103
Switch(config)#interface vlan 101 <ENTER> โหมด config ให้สร้าง vlan 101
Switch(config-if)#ip address 192.168.1.254 255.255.255.0 <ENTER> กำหนดอิปีสำหรับ
vlan 101 เพื่อเป็น gateway ให้กับเครื่องลูกข่าย
Switch(config-if)#int vlan 102 <ENTER>
Switch(config-if)#ip address 192.168.2.254 255.255.255.0 <ENTER>
Switch(config-if)#int vlan 103 <ENTER>
Switch(config-if)#ip address 192.168.3.254 255.255.255.0 <ENTER>
สร้าง vlan 102, 103 พร้อมกับกำหนดอิปีให้แต่ละ vlan ตามลำดับ
```

- ! กำหนด port ให้เป็นสมาชิกของแต่ละ vlan

```
Switch(config)#interface fastEthernet 0/1 <ENTER> โหมด config เข้าสู่ port fa0/1
Switch(config-if)#switchport access vlan 103 <ENTER> กำหนดให้ fa0/1 เป็นสมาชิก vlan
103
Switch(config-if)#exit <ENTER> ออกไปยังโหมด config
```

```

Switch(config)#interface fastEthernet 0/2 <ENTER> เข้าสู่ fa0/2
Switch(config-if)#switchport access vlan 102 <ENTER> กำหนดเป็นสมาชิก vlan 102
Switch(config-if)#exit <ENTER> ออกไปยังโหมด config
Switch(config)#interface fastEthernet 0/3 <ENTER> เข้าสู่ fa0/3
Switch(config-if)#switchport access vlan 103 <ENTER> กำหนดเป็นสมาชิก vlan 103
เสร็จการคอนฟิกที่อุปกรณ์สวิชต์ L3

```

2. สำหรับนสวิชต์ L2 ไม่ต้องปรับแต่งค่อนฟิกใดๆ ทั้งสิ้น ต่อไปให้กำหนดไอพีให้กับเครื่อง PC0, PC1 และ PC3 ตามลำดับดังนี้

PC0 (vlan 103):

IP=192.168.3.10, subnet=255.255.255.0, gateway=192.168.3.254

PC1 (vlan 102):

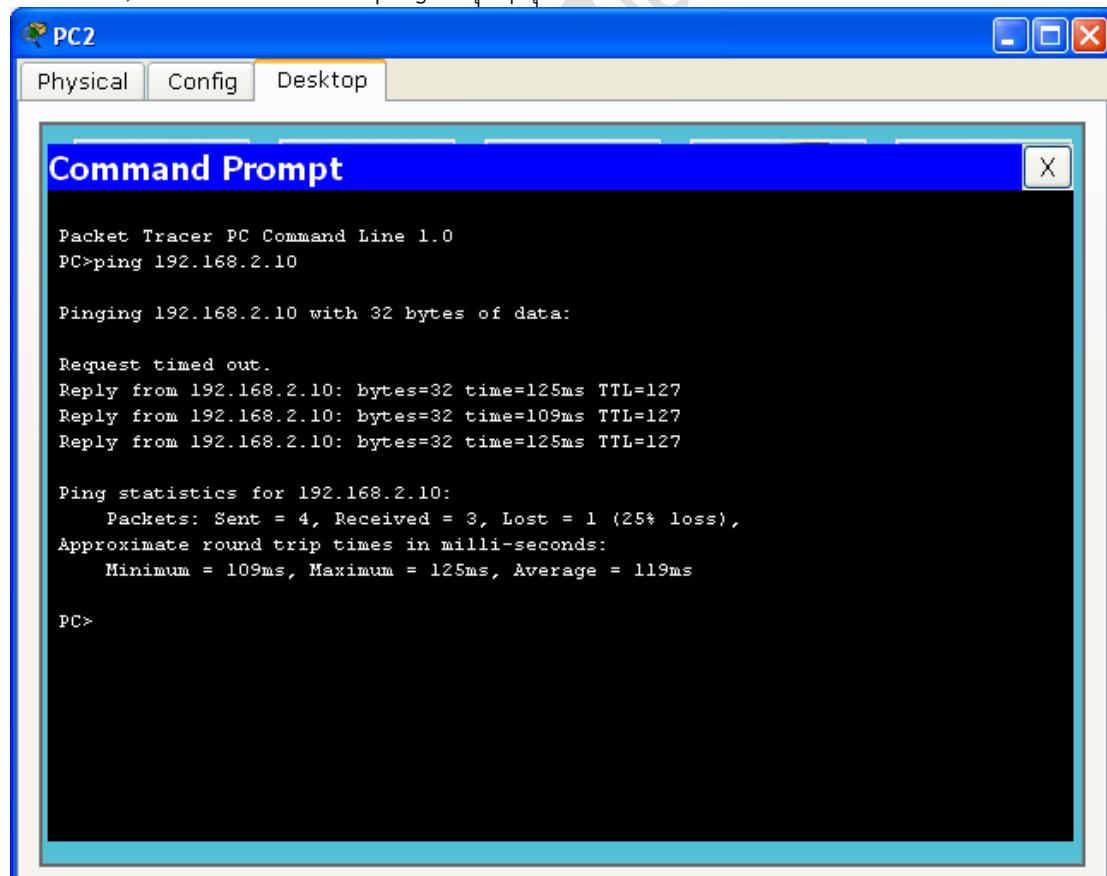
IP=192.168.2.10, subnet=255.255.255.0, gateway=192.168.2.254

PC2 (vlan 101):

IP=192.168.1.10, subnet=255.255.255.0, gateway=192.168.1.254

การทดสอบ :

ทดสอบโดยการ ping จาก PC0 ไปยังเครื่อง PC1, PC2 และ ping กลับทิศทางกันคือ PC2 ไปยัง PC3, PC1 เป็นต้น จะต้อง ping ได้ทุกๆ จุดจึงจะถือได้ว่าระบบการค่อนฟิกทั้งหมดสำเร็จ



ทดสอบ ping จากเครื่อง PC2 ไปยัง PC1 สำเร็จ

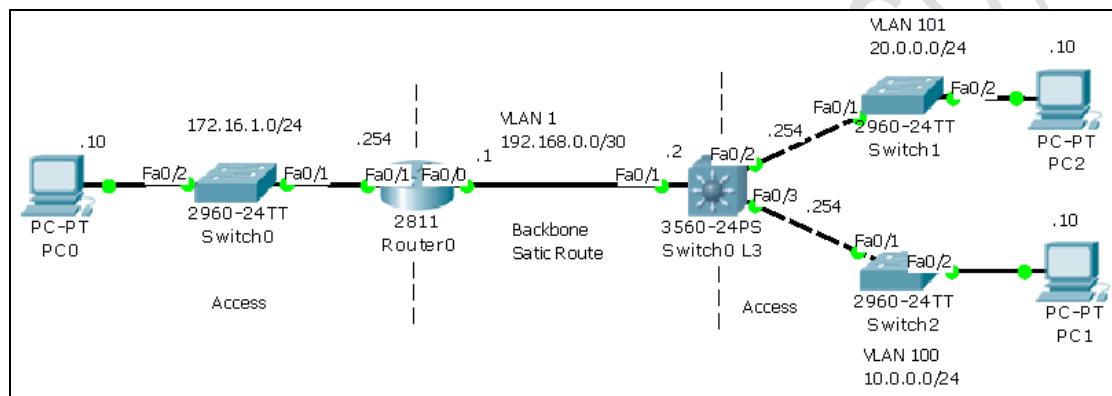


### Scenario 23: การคุณพิก Switch L3 กับ Router และ Static Routing

คำอธิบาย :

ความสามารถของเราเตอร์และสวิตช์ในปัจจุบันใกล้เคียงกันมาก แทบจะแยกไม่ออกว่า ต่างกันอย่างไร มีอยู่จุดหนึ่งที่เห็นได้ชัดคือ เราเตอร์นั้นจะเชื่อมเครือข่ายที่แตกต่างกันให้สามารถสื่อสารกันได้ เช่น Ethernet topology กับ ATM หรือ Frame-relay เป็นต้น แต่สวิตช์มีความสามารถเชื่อมต่อเครือข่ายที่มีเทคโนโลยีเดียวกันเข้าด้วยกัน เช่น Ethernet กับ Ethernet เป็นต้น (แต่ปัจจุบันสวิตช์เริ่มจะมีความสามารถเชื่อมต่อเครือข่ายต่างๆ เข้ากันได้เหมือนเราเตอร์แล้ว ซึ่งเป็นสวิตช์รุ่นใหญ่ๆ เช่น 7000 series เป็นต้น)

แผนผังการเชื่อมต่อ :



ขั้นตอนการคุณพิก :

1. บนเครื่องเราเตอร์ (2811) กำหนดไอเพ็คท์สำหรับใช้เป็น gateway ให้ fa0/0 สำหรับเชื่อมกับสวิตช์ 3560 และ fa0/1 สำหรับเชื่อมต่อกับเน็ตเวิร์ค 172.16.1.0 ตามไดอะแกรมด้านบน ดังนี้ บนเราเตอร์ 2811

```

Router(config)#interface fastEthernet 0/0 <ENTER> เข้าสู่ fa0/0 ในโหมด config
Router(config-if)#ip address 192.168.0.1 255.255.255.252 <ENTER> กำหนดไอเพ็คท์ให้ fa0/0 เป็น .1 และทำ subnet .252 ซึ่งจะใช้ออฟ์ไดเพียง 2 ไอเพ็คท์เท่านั้น (ไม่รวม Network ID และ Broadcast IP)
Router(config-if)#no shutdown <ENTER> สั่งให้ fa0/0 ทำงาน เพราะอินเทอร์เฟสของเราเตอร์โดยปกติจะปิดการทำงานไว้เสมอ แต่สวิตช์จะเปิดไว้เสมอ
Router(config-if)#exit <ENTER> ออกໄປไปโหมด config
Router(config)#intf fa0/1 <ENTER> เข้าสู่อินเทอร์เฟส fa0/1 เพื่อกำหนด gateway ให้เครื่องลูกข่ายของเราเตอร์
Router(config-if)#ip address 172.16.1.254 255.255.255.0 <ENTER> กำหนด gateway เป็น .254 และ subnet /24 หรือ 255.255.255.0 แม้ว่าออฟ์เป็น class B ก็ตาม แต่เมื่อทำ subnet ดังกล่าวแล้ว สามารถใช้เครื่องลูกข่ายได้เพียง 256 ไอเพ็คท์เท่านั้น
Router(config-if)#no shutdown <ENTER>
Router(config)#end <ENTER> ออกສູ່ໂຄງ config admin

```

Router#wr <ENTER> บันทึกข้อมูลการคอนฟิกบนเราเตอร์

2. บนสวีชต์ L3 (3560) ต้องสร้าง vlan 100 และ vlan 101 พร้อมกับกำหนดไดอีพีให้กับ vlan และไอพีที่ใช้เชื่อมต่อกับเราเตอร์ ตามลำดับดังนี้  
บนสวีชต์ L3 (3560)

```
Switch(config)#interface vlan 1 <ENTER> เข้าสู่ vlan 1 ในโหมด config
Switch(config-if)#ip address 192.168.0.2 255.255.255.252 <ENTER> กำหนด gateway ที่
เชื่อมต่อกับเราเตอร์เป็น .2 subnet คือ /30 หรือ 255.255.255.252
Switch(config-if)#no shutdown <ENTER> สั่งให้อินเทอร์เฟสทำงาน (เพื่อความมั่นใจว่า
อินเทอร์เฟสดังกล่าวทำงานแล้ว)
! ทดสอบโดยการ ping ไปยัง gateway ของเราเตอร์
Switch#ping 192.168.0.1 <ENTER>

! สร้าง vlan 100 และ 101 เพื่อใช้เป็น gateway ให้เน็ตเวิร์ค 10.0.0.0 และ 20.0.0.0
Switch(config)#interface vlan 100 <ENTER>
witch(config-if)#ip address 10.0.0.254 255.255.255.0 <ENTER>
Switch(config-if)#inte vlan 101 <ENTER>
Switch(config-if)#ip address 20.0.0.254 255.255.255.0 <ENTER>
Switch(config-if)#exit <ENTER>
Switch(config)#interface fa0/2 <ENTER> กำหนดให้ fa0/2 เป็นสมาชิก vlan 101
Switch(config-if)#switchport access vlan 101 <ENTER>
Switch(config-if)#inte fa0/3 <ENTER> กำหนดให้ fa0/3 เป็นสมาชิก vlan 100
Switch(config-if)#switchport access vlan 100 <ENTER>
```

3. กำหนดหมายเลขไอพีให้กับเครื่อง PC ทั้งหมดตาม diagram ด้านบน ดังนี้  
PC0 (ต่อหลังเราเตอร์):

IP=172.16.1.10, subnet=255.255.255.0, gateway=172.16.1.254

PC1 (ต่อหลังสวีชต์ L3 vlan 100):

IP=10.0.0.10, subnet=255.255.255.0, gateway=10.0.0.254

PC2 (ต่อหลังสวีชต์ L3 vlan 101):

IP=20.0.0.10, subnet=255.255.255.0, gateway=20.0.0.254

การทดสอบ :

- ทดสอบโดยการ ping gateway ของเน็ตเวิร์คที่เครื่อง PC ดังกล่าวต่อเชื่อมอยู่ เช่น PC0 ทดลอง ping ไปยังไอพี 172.16.1.254 และ 192.168.0.1 ซึ่งต้องมี การตอบสนองกลับมาจึงถือว่าถูกต้อง แต่ในขั้นตอนนี้จะยังไม่สามารถ ping ไปยังไอพีอื่นๆ เช่น 192.168.1.2 หรือ 10.0.0.X และ 20.0.0.X เนื่องจากยังไม่มี การทำ routing ให้กับเครือข่ายดังกล่าว

2. การกำหนด routing เป็นการบอกให้อุปกรณ์บนเครือข่ายทราบว่าข้อมูลหรือแพ็คเก็ตที่ต้องการส่งไปยังเครือข่ายอื่นๆ ควรจะไปทางไหน อย่างไร ซึ่งมี 2 แบบคือ static route และ dynamic route เมื่อกล่าวโดยย่อ static route ผู้ดูแลระบบจะเป็นผู้กำหนดเส้นทางเองทั้งหมด ส่วน dynamic route นั้นโปรแกรม routing ที่ฝึกมา กับเราเตอร์จะเป็นผู้หาเส้นทางเอง (แต่เบื้องต้นผู้ดูแลระบบ จะต้องมีการคอนฟิกวิธีการ routing ให้แกรมรู้ก่อนเสมอ ซึ่งจะกล่าวใน scenario ต่อๆ ไป)

#### การกำหนด Static route บนเราเตอร์

เมื่อสังเกตจาก Diagram ข้างบน เมื่อต้องการให้แพ็คเก็ตที่อยู่หลังเราเตอร์ส่งไปยังเน็ตเวิร์ค 10.0.0.0 หรือ 20.0.0.0 เราจะต้องบอกให้เราเตอร์ทราบว่าจะโยนข้อมูลไปอย่างไร ในที่นี้จะต้องกำหนดให้โยนไปที่ไอพีของสวิตช์ L3 ซึ่งอยู่ตรงกันข้ามกับเราเตอร์ ดังนี้

```
Router(config)#ip route 10.0.0.0 255.255.255.0 192.168.0.2 <ENTER> ในโหมด config  
กำหนดให้เราเตอร์โยนข้อมูลไปยังไอพี 192.168.0.2 ของสวิตช์ L3 เมื่อมีแพ็คเก็ตใดๆ ต้องการส่ง  
ข้อมูลไปยังเน็ตเวิร์ค 10.0.0.0 หรือ 20.0.0.0
```

```
Router(config)#ip route 20.0.0.0 255.255.255.0 192.168.0.2 <ENTER>
```

#### การกำหนด Static route บนสวิตช์ L3

ในทางกลับกันถ้าต้องการส่งข้อมูลจาก 10.0.0.0 หรือ 20.0.0.0 ไปยังเน็ตเวิร์ค 172.16.1.0 จะต้องโยนข้อมูลไปยังไอพีของเราเตอร์ผ่านทางกันข้าม และอย่างลืมว่าการคอนฟิกด้วยวิธีการ Static จะต้องทำ route ทั้ง 2 ข้างให้ครบก่อนข้อมูลจึงจะเดินทางได้อย่างสมบูรณ์

```
Router(config)#ip route 172.16.1.0 255.255.255.0 192.168.0.1 <ENTER> ในโหมด config  
กำหนดให้เราเตอร์โยนข้อมูลไปยังไอพี 192.168.0.1 ของเราเตอร์ เมื่อมีแพ็คเก็ตใดๆ ต้องการ  
ส่งข้อมูลไปยังเน็ตเวิร์ค 172.16.1.0
```

3. ทดสอบโดยการ ping จาก PC0 ไปยัง PC1 และ PC2 ต้องมีการตอบสนอง ถ้าไม่มีให้กลับไปตรวจสอบกับ diagram อีกครั้งและ ตรวจสอบคอนฟิกบนเราเตอร์ สวิตช์ว่าถูกต้องหรือยัง (ใช้คำสั่ง show running-config)

หมายเหตุ 1: ถ้าพิมพ์คำสั่งใดๆ ในเราเตอร์หรือสวิตช์ผิด และต้องการแก้ไขหรือลบออกให้ใช้คำว่า no และตามด้วยคำสั่งตั้งกล่าว ในโหมดเดิม เช่น

```
Router(config)#ip route 172.16.1.0 255.255.255.0 192.168.0.1 คำสั่งเก่าที่ผิด  
Router(config)#no ip route 172.16.1.0 255.255.255.0 192.168.0.1 ลบคำสั่งเก่าที่ผิดออก
```

หมายเหตุ 2: ในการนี้ที่เริ่มการทำงานของเราเตอร์ใหม่และยังไม่มีการคอนฟิกใดๆ เราเตอร์จะแสดงเมนูดังนี้คือ

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no ← ให้เลือก no <ENTER>

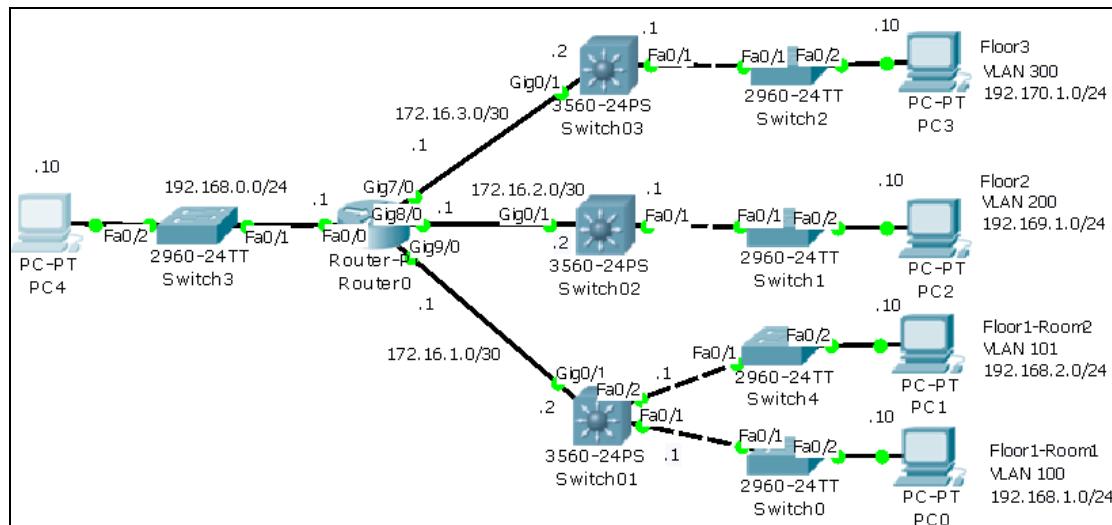


## Scenario 24: การคอนฟิกให้ Router ควบคุมสวิตช์ L3 หลายๆ ตัว

คำอธิบาย :

ใน Scenario นี้จะแสดงการใช้เราเตอร์ควบคุมการทำงานของสวิตช์ L3 หลายๆ ตัวเข้าไว้ด้วยกัน คล้ายกับมีสำนักงานอยู่ 1 ตึกและประกอบไปด้วย 3 ชั้น แต่ละชั้นมีแต่ละแผนกอยู่ ดังนั้นตามหลักการคือ ควรจะให้ L3 ควบคุม vlan ของแต่ละห้องในแต่ละชั้น จากนั้นให้เราเตอร์หรือสวิตช์ L3 คุณภาพสูงควบคุม L2 ในแต่ละชั้นอีกทีหนึ่ง ดัง Diagram

แผนผังการเชื่อมต่อ :



ขั้นตอนการเชื่อมต่อ :

ใน Diagram ข้างต้นการเชื่อมต่อระหว่างเราเตอร์ (ควรใช้ Router-PT สำหรับทดสอบใน scenario นี้) และสวิตช์ L3 ในแต่ละชั้นจะเชื่อมด้วย Gigabit Ethernet (Gig) ซึ่งผู้ใช้งานจำเป็นต้องติดตั้ง Module เพิ่มที่เราเตอร์คือ The single-port Cisco Gigabit Ethernet Network Module (part number PT-ROUTER-NM-1CGE) จำนวน 3 พอร์ตบนเราเตอร์ (สำหรับขั้นตอนการติดตั้งให้กลับไปดูในบทแรกๆ เรื่องของเพิ่มถอนอินเทอร์เฟส)

ขั้นตอนการคอนฟิก :

- บันเครื่องเราเตอร์ (Router-PT) จะต้องค่อนฟิก ซึ่งประกอบไปด้วย

Interface	IP/Subnet
Fa0/0	192.168.0.1/255.255.255.0 หรือ /24
Gig9/0	172.16.1.1/255.255.255.252 หรือ /30
Gig8/0	172.16.2.1/255.255.255.252 หรือ /30
Gig7/0	172.16.3.1/255.255.255.252 หรือ /30

ด้วยคำสั่งดังนี้

```
! อินเทอร์เฟส Fa0/0
Router(config)#interface fastEthernet 0/0 <ENTER>
Router(config-if)#ip address 192.168.0.1 255.255.255.0 <ENTER>
Router(config-if)#no shutdown <ENTER>
```

```
! บนอินเทอร์เฟส Gig9/0
```

```
Router(config)#interface gigabitEthernet 9/0 <ENTER>
```

```
Router(config-if)#ip address 172.16.1.1 255.255.255.252 <ENTER> subnet = /30
```

```
Router(config-if)#no shutdown <ENTER>
```

```
! บนอินเทอร์เฟส Gig8/0
```

```
Router(config)#interface gigabitEthernet 8/0 <ENTER>
```

```
Router(config-if)#ip address 172.16.2.1 255.255.255.252 <ENTER> subnet = /30
```

```
Router(config-if)#no shutdown <ENTER>
```

```
! บนอินเทอร์เฟส Gig7/0
```

```
Router(config)#interface gigabitEthernet 7/0 <ENTER>
```

```
Router(config-if)#ip address 172.16.3.1 255.255.255.252 <ENTER> subnet = /30
```

```
Router(config-if)#no shutdown <ENTER>
```

2. บนสวิชต์ L3 (Switch01) ขั้นที่ 1 ต้องสร้าง vlan อย่างน้อย 2 vlan คือ vlan 100 และ 101 และกำหนดไดอีพีให้แต่ละ vlan ดังนี้

Interface	Vlan name	IP/Subnet
Gig0/1	Vlan 1	172.16.1.2/255.255.255.252 หรือ /30
Fa0/1	Vlan 100	192.168.1.1/255.255.255.0 หรือ /24
Fa0/2	Vlan 101	192.168.2.1/255.255.255.0 หรือ /24

ด้วยคำสั่งดังนี้ (สำหรับผู้เริ่มต้นสังเกตุให้ดีว่าการคอนฟิกจะเปลี่ยนโหมดไปตาม หน้าที่ เช่น โหมด admin จะเป็นสัญลักษณ์ #, โหมด config เป็น (config)#, โหมดอินเทอร์เฟส เป็น (config-if)# เป็นต้นของให้ระวังด้วย ถ้ายังไม่เข้าใจให้อ่านเพิ่มเติมได้จาก หนังสือ network simulation เล่ม 1 ของผู้เขียนควบคู่ไปด้วย หรือจากหนังสือท้ายเล่มประกอบ)

```
! อินเทอร์เฟส vlan 1
```

```
Switch01(config)#interface vlan 1 <ENTER>
```

```
Switch01(config-if)#ip address 172.16.1.2 255.255.255.252 <ENTER> กำหนดไดอีพีให้ vlan 1 เพื่อใช้เชื่อมต่อกับเราเตอร์ (ถามว่าทำไมต้องใช้ vlan 1 ในการเชื่อมต่อ ไม่เห็นเราเตอร์ต้องทำงานกับ vlan เลย ขอตอบว่า คุณสมบัติของสวิชต์ L3 คือ vlan ดังนั้นการเชื่อมต่อทุกๆ อย่าง สวิชต์ L3 จะต้องมี vlan เข้ามายุ่งเกี่ยวเสมอ ส่วนทำไม่ต้องใช้ vlan 1 ตอบว่า ไม่จำเป็นก็ได้ จะสร้าง vlan ใหม่ขึ้นมาทดแทน vlan 1 ก็ได้ แต่ในเบื้องต้นเป็นที่ทราบกันดีว่าทุกๆ พอร์ตจะอยู่ที่ vlan 1 เสมอ จึงสามารถใช้งานพอร์ตต่างๆ ได้ทันที โดยไม่จำเป็นต้องย้ายพอร์ตไป vlan ใหม่ที่สร้างขึ้น)
```

```
Switch01(config-if)#no shutdown <ENTER>
```

ไม่ต้องย้ายพอร์ต Gig0/1 มาที่ vlan 1 เพราะอยู่ที่ vlan 1 โดย default อยู่แล้ว

! สร้าง vlan 100 และ 101

```
Switch01(config)#interface vlan 100 <ENTER>
Switch01(config-if)#ip address 192.168.1.1 255.255.255.0 <ENTER>
Switch01(config-if)#int vlan 101 <ENTER>
Switch01(config-if)#ip address 192.168.2.1 255.255.255.0 <ENTER>
```

! ย้ายพอร์ต Fa0/1 มาเป็นสมาชิกของ vlan 100 และ Fa0/2 มาเป็นสมาชิกของ vlan 101

```
Switch01(config)#interface fastEthernet 0/1 <ENTER>
Switch01(config-if)#switchport access vlan 100 <ENTER>
Switch01(config-if)#int fa0/2 <ENTER>
Switch01(config-if)#switchport access vlan 101 <ENTER>
```

### 3. บนสวีช์ L3 (Switch02) ขั้นที่ 2 ต้องสร้าง vlan 200 และกำหนดค่าดังนี้

Interface	Vlan name	IP/Subnet
Gig0/1	Vlan 1	172.16.2.2/255.255.255.252 หรือ /30
Fa0/1	Vlan 200	192.169.1.1/255.255.255.0 หรือ /24

! อินเทอร์เฟส vlan 1

```
Switch02(config)#interface vlan 1 <ENTER>
Switch02(config-if)#ip address 172.16.2.2 255.255.255.252 <ENTER>
Switch02(config-if)#no shutdown <ENTER> !!! อาย่าลืมต้องสั่งให้ vlan 1 ทำงานด้วย
```

! สร้าง vlan 200

```
Switch02(config)#interface vlan 100 <ENTER>
Switch02(config-if)#ip address 192.169.1.1 255.255.255.0 <ENTER>
```

! ย้ายพอร์ต Fa0/1 มาเป็นสมาชิกของ vlan 200

```
Switch02(config)#interface fastEthernet 0/1 <ENTER>
Switch02(config-if)#switchport access vlan 200 <ENTER>
```

### 4. บนสวีช์ L3 (Switch03) ขั้นที่ 3 ต้องสร้าง vlan 300 และกำหนดค่าดังนี้

Interface	Vlan name	IP/Subnet
Gig0/1	Vlan 1	172.16.3.2/255.255.255.252 หรือ /30
Fa0/1	Vlan 300	192.170.1.1/255.255.255.0 หรือ /24

! อินเทอร์เฟส vlan 1

```
Switch03(config)#interface vlan 1 <ENTER>
Switch03(config-if)#ip address 172.16.3.2 255.255.255.252 <ENTER>
```

```
Switch03(config-if)#no shutdown <ENTER> !!! อย่าลืมต้องสั่งให้ vlan 1 ทำงานด้วย
```

! สร้าง vlan 300

```
Switch03(config)#interface vlan 300 <ENTER>
```

```
Switch03(config-if)#ip address 192.170.1.1 255.255.255.0 <ENTER>
```

! ย้ายพอร์ต Fa0/1 มาเป็นสมาชิกของ vlan 300

```
Switch03(config)#interface fastEthernet 0/1 <ENTER>
```

```
Switch03(config-if)#switchport access vlan 300 <ENTER>
```

#### 5. กำหนดໄໂພຂອງເຄື່ອງ PC ຕັ້ງນີ້

ເຄື່ອງ PC	Vlan name	IP/Subnet
PC0	Vlan 100	192.168.1.10/255.255.255.0
PC1	Vlan 101	192.168.2.10/255.255.255.0
PC2	Vlan 200	192.169.1.10/255.255.255.0
PC3	Vlan 300	192.170.0.10/255.255.255.0
PC4	No vlan	192.168.0.10/255.255.255.0

#### 6. ทำการกำหนด Static Route ບນເຮົາເຕືອນຕັ້ງຕ່ອໄປນີ້

```
Router(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.2 <ENTER> ສໍາຮັບເຮົາຕີໄປ  
ຢັງເນື້ຕວີກ 192.168.1.0
```

```
Router(config)#ip route 192.168.2.0 255.255.255.0 172.16.1.2 <ENTER> ເຮົາຕີໄປຢັງ  
ເນື້ຕວີກ 192.168.2.0
```

```
Router(config)#ip route 192.169.1.0 255.255.255.0 172.16.2.2 <ENTER> ເຮົາຕີໄປຢັງ  
ເນື້ຕວີກ 192.169.1.0
```

```
Router(config)#ip route 192.170.1.0 255.255.255.0 172.16.3.2 <ENTER> ເຮົາຕີໄປຢັງ  
ເນື້ຕວີກ 192.170.1.0
```

#### 7. ทำการกำหนด Static Route ບນສວິຟ້ຕ് Switch01 ດັ່ງຕ່ອໄປນີ້

```
Switch01(config)#ip route 192.168.0.0 255.255.255.0 172.16.1.1 <ENTER>
```

```
Switch01(config)#ip route 192.169.1.0 255.255.255.0 172.16.1.1 <ENTER>
```

```
Switch01(config)#ip route 192.170.1.0 255.255.255.0 172.16.1.1 <ENTER>
```

#### 8. ทำการกำหนด Static Route ບນສວິຟ້ຕ് Switch02 ດັ່ງຕ່ອໄປນີ້

```
Switch02(config)#ip route 192.168.0.0 255.255.255.0 172.16.2.1 <ENTER>
```

```
Switch02(config)#ip route 192.168.1.0 255.255.255.0 172.16.2.1 <ENTER>
```

```
Switch02(config)#ip route 192.168.2.0 255.255.255.0 172.16.2.1 <ENTER>
```

```
Switch02(config)#ip route 192.170.1.0 255.255.255.0 172.16.2.1 <ENTER>
```

### 9. ทำการกำหนด Static Route บนสวิตช์ Switch03 ดังต่อไปนี้

```
Switch03(config)#ip route 192.168.0.0 255.255.255.0 172.16.3.1 <ENTER>
Switch03(config)#ip route 192.168.1.0 255.255.255.0 172.16.3.1 <ENTER>
Switch03(config)#ip route 192.168.2.0 255.255.255.0 172.16.3.1 <ENTER>
Switch03(config)#ip route 192.169.1.0 255.255.255.0 172.16.3.1 <ENTER>
```

การทดสอบ :

เมื่อการค่อนพิกเสร็จสมบูรณ์เครื่อง PC ทุกๆ เครื่องจะต้องสามารถ ping กันได้ทั้งหมด

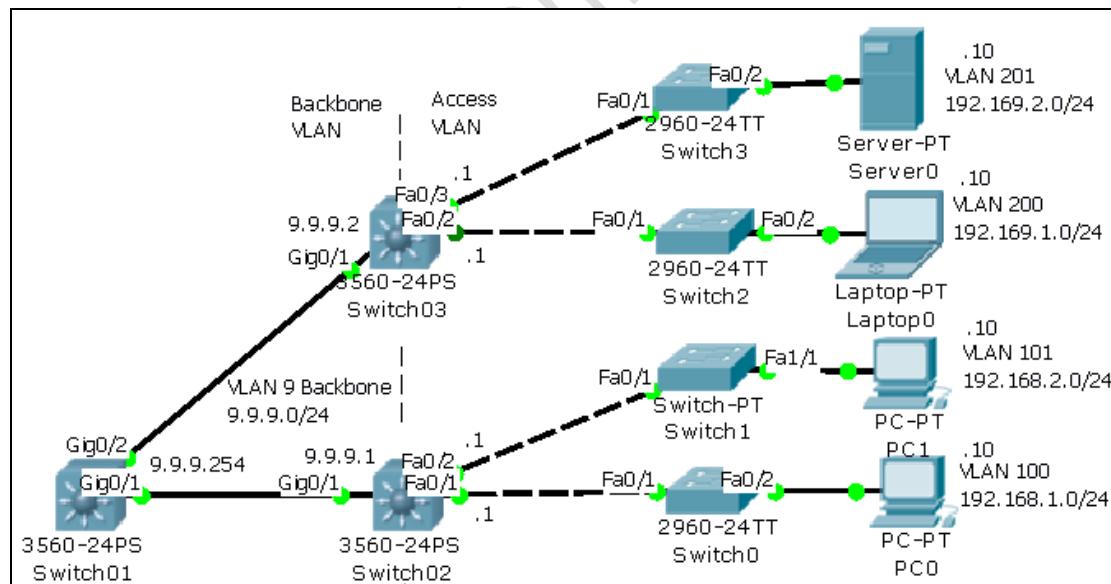


### Scenario 25: การค่อนพิกให้สวิตช์ L3 ควบคุมสวิตช์ L3 หลายๆ ตัว

คำอธิบาย :

ใน Scenario นี้จะแสดงการใช้สวิตช์ L3 ควบคุมการทำงานของสวิตช์ L3 หลายๆ ตัวเข้าไว้ด้วยกัน หลักการคล้าย Scenario ที่ 24 แต่ในสถานะการณ์นี้ สมมุติว่าไม่มีเราเตอร์ โดยใช้สวิตช์ควบคุมการทำงานแทน

แผนผังการเชื่อมต่อ :



ขั้นตอนการเชื่อมต่อ :

ใน Diagram ข้างต้น สวิตช์ L3 แต่ละตัวเชื่อมต่อโดยใช้ Vlan Backbone เดียวกัน ซึ่งมีความพิเศษกว่าเครือข่ายอื่นๆ เเละมีอินเทอร์เฟส Gig0/1 และ Gig0/2 จะอยู่ใน Vlan เดียวกัน ซึ่งการเชื่อมต่อที่ผ่านมาจะใช้ Vlan ในส่วนของ Backbone แยกกัน

ขั้นตอนการค่อนพิก :

1. บนสวิตช์ (Switch01) ประกอบไปด้วย

Interface	IP/Subnet	Vlan
-----------	-----------	------

Gig0/1	9.9.9.1/255.255.255.0	Vlan 9
Gig0/2	9.9.9.2/255.255.255.0	Vlan 9
Vlan 9	9.9.9.254/255.255.255.0	Vlan 9

ขั้นตอนการคอนฟิกด้วยคำสั่งดังต่อไปนี้

```
! สร้าง vlan 9
Switch01(config)#interface vlan 9 <ENTER>
Switch01(config-if)#ip address 9.9.9.254 255.255.255.0 <ENTER> กำหนดอิโอพีสำหรับ
vlan 9
Switch01(config-if)#exit <ENTER>
Switch01(config)#interface gigabitEthernet 0/1 <ENTER> ย้าย Gig0/1 จาก vlan 1 ไปยัง
vlan 9 ที่สร้างขึ้นใหม่
Switch01(config-if)#switchport access vlan 9 <ENTER>
Switch01(config-if)#intf gig0/2 <ENTER> ย้าย Gig0/2 จาก vlan 1 ไปยัง vlan 9
Switch01(config-if)#switchport access vlan 9 <ENTER>
```

2. บนสวิตช์ L3 (Switch02) ขั้นที่ 1 ต้องสร้าง vlan 2 vlan คือ vlan 100 และ 101  
พร้อมกำหนดอิโอพีให้แต่ละ vlan ดังนี้

Interface	Vlan name	IP/Subnet
Gig0/1	Vlan 9	9.9.9.1/255.255.255.0
Fa0/1	Vlan 100	192.168.1.1/255.255.255.0
Fa0/2	Vlan 101	192.168.2.1/255.255.255.0

คำสั่งที่ค่อนฟิกบน Switch02

```
! สร้างอินเทอร์เฟส vlan 9
Switch02(config)#interface vlan 9 <ENTER> สร้าง vlan 9 เพื่อใช้เชื่อมเป็น backbone
Switch02(config-if)#ip address 9.9.9.1 255.255.255.0 <ENTER> กำหนดอิโอพีของ
backbone
Switch02(config-if)#intf vlan 100 <ENTER> สร้าง vlan 100 เพื่อควบคุมขั้นที่ 1 ห้อง 1
Switch02(config-if)#ip address 192.168.1.1 255.255.255.0 <ENTER>
Switch02(config-if)#intf vlan 101 <ENTER> สร้าง vlan 101 เพื่อควบคุมขั้นที่ 1 ห้อง 2
Switch02(config-if)#ip address 192.168.2.1 255.255.255.0 <ENTER>
Switch02(config-if)#exit <ENTER>
Switch02(config)#interface gigabitEthernet 0/1 <ENTER>
Switch02(config-if)#switchport access vlan 9 <ENTER> ย้าย gig0/1 เข้า vlan 9
Switch02(config-if)#intf fa0/1 <ENTER>
Switch02(config-if)#switchport access vlan 100 <ENTER> ย้าย Fa0/1 เข้า vlan 100
Switch02(config-if)#intf fa0/2 <ENTER>
Switch02(config-if)#switchport access vlan 101 <ENTER> ย้าย Fa0/2 เข้า vlan 101
```

3. บนสวิชต์ L3 (Switch03) ขั้นที่ 2 ต้องสร้าง vlan 2 vlan คือ vlan 200 และ 201  
พร้อมกำหนดไอพีให้แต่ละ vlan ดังนี้

Interface	Vlan name	IP/Subnet
Gig0/1	Vlan 9	9.9.9.2/255.255.255.0
Fa0/2	Vlan 200	192.169.1.1/255.255.255.0
Fa0/3	Vlan 201	192.169.2.1/255.255.255.0

คำสั่งที่คอนฟิกบน Switch03

```
! สร้างอินเทอร์เฟส vlan 9
Switch03(config)#interface vlan 9 <ENTER> สร้าง vlan 9 เพื่อใช้เป็น backbone
Switch03(config-if)#ip address 9.9.9.2 255.255.255.0 <ENTER> กำหนดไอพีของ
backbone
Switch03(config-if)#int vlan 200 <ENTER> สร้าง vlan 200 เพื่อควบคุมชั้นที่ 2 ห้อง 1
Switch03(config-if)#ip address 192.169.1.1 255.255.255.0 <ENTER>
Switch03(config-if)#int vlan 201 <ENTER> สร้าง vlan 201 เพื่อควบคุมชั้นที่ 2 ห้อง 2
Switch03(config-if)#ip address 192.169.2.1 255.255.255.0 <ENTER>
Switch03(config-if)#exit <ENTER>
Switch03(config)#interface gigabitEthernet 0/1 <ENTER>
Switch03(config-if)#switchport access vlan 9 <ENTER> ย้าย gig0/1 เข้า vlan 9
Switch03(config-if)#int fa0/2 <ENTER>
Switch03(config-if)#switchport access vlan 200 <ENTER> ย้าย Fa0/2 เข้า vlan 200
Switch(config-if)#int fa0/3 <ENTER>
Switch03(config-if)#switchport access vlan 201 <ENTER> ย้าย Fa0/3 เข้า vlan 201
```

4. กำหนดไอพีของเครื่อง PC ตาม Diagram ดังนี้

เครื่อง PC	Vlan name	IP/Subnet
PC0	Vlan 100	192.168.1.10/255.255.255.0
PC1	Vlan 101	192.168.2.10/255.255.255.0
Labtop0	Vlan 200	192.169.1.10/255.255.255.0
Server0	Vlan 201	192.169.2.10/255.255.255.0

5. ทำการกำหนด Static Route บนสวิชต์ Switch01 ดังต่อไปนี้

```
Switch01(config)#ip route 192.168.1.0 255.255.255.0 9.9.9.1 <ENTER>
Switch01(config)#ip route 192.168.2.0 255.255.255.0 9.9.9.1 <ENTER>
Switch01(config)#ip route 192.169.1.0 255.255.255.0 9.9.9.2 <ENTER>
Switch01(config)#ip route 192.169.2.0 255.255.255.0 9.9.9.2 <ENTER>
```

7. ทำการกำหนด Static Route บนสวิชต์ Switch02 ดังต่อไปนี้

```
Switch02(config)#ip route 192.169.1.0 255.255.255.0 9.9.9.254 <ENTER>
Switch02(config)#ip route 192.169.2.0 255.255.255.0 9.9.9.254 <ENTER>
```

8. ทำการกำหนด Static Route บนสวิชต์ Switch03 ดังต่อไปนี้

```
Switch03(config)#ip route 192.168.1.0 255.255.255.0 9.9.9.254 <ENTER>
Switch03(config)#ip route 192.168.2.0 255.255.255.0 9.9.9.254 <ENTER>
```

การทดสอบ :

เมื่อการค่อนพิกเสร็จสมบูรณ์เครื่อง PC ทุกๆ เครื่องจะต้องสามารถ ping กันได้ทั้งหมด

## บทที่ 4

### Workshop on Packet Tracer Simulation (Video Training)

ในบทนี้จะอธิบายถึงวิธีการออกแบบและติดตั้งเครือข่ายโดยใช้โปรแกรม Packet ในรูปแบบของวีดิโอดังนี้ ผู้อ่านสามารถเลือก Workshop ที่ต้องการโดยการอ่านคำอธิบายสั้นๆ ได้จากบทนี้ก่อน จากนั้นจึงทำการเปิด Video ในแผ่น DVD ที่แนบมา กับหนังสือเล่มนี้ โดยผู้ใช้จำเป็นต้องใช้เครื่องมือเหล่านี้คือ

1. โปรแกรม Packet Tracer ตั้งแต่เวอร์ชัน 5.3 ขึ้นไป
2. โปรแกรมที่สามารถเล่นไฟล์ประเภทมัลติมีเดียได้ (.avi)
3. ลำโพง

หมายเหตุ ใน Workshop ตั้งแต่ 1-36 ยังไม่ครอบคลุมคุณสมบัติทั้งหมดของโปรแกรม Packet Tracer ที่มีให้ เนื่องจากข้อมูลที่บันทึกอยู่ในรูปของวีดิโอนั้นค่อนข้างใหญ่ ซึ่งถ้าอธิบายให้ครบถ้วน เนื้อหา จะต้องใช้ DVD หลายแผ่น ผู้เขียนหวังเป็นอย่างยิ่งว่าอาจจะมีโอกาสบันทึกเนื้อหาที่ยังขาดอยู่ ในหนังสือเล่มถัดไป

#### **Workshop 0:** เปื้องต้นก่อนตอนพิจารณา

คำกล่าวแนะนำเบื้องต้นเกี่ยวกับหนังสือของผู้เขียน

#### **Workshop 1:** Introduction to Packet Tracer 5.3

เป็นการแนะนำ Packet Tracer เปื้องต้น เพิ่มเติมจากที่อธิบายแล้วในหนังสือ

#### **Workshop 2:** How to Packet Tracer 5.3

เริ่มต้นการใช้งานใช้งานโปรแกรม Packet Tracer

#### **Workshop 3:** การเพิ่ม/ลด อุปกรณ์

แสดงตัวอย่างการเพิ่มลดอุปกรณ์ เช่น เพิ่มอุปกรณ์ การ์ดอินเทอร์เฟสให้เราเตอร์ การเชื่อมสายสัญญาณ เป็นต้น

#### **Workshop 4:** การใช้คำสั่ง IOS เปื้องต้น

อธิบายการใช้คำสั่งระบบปฏิบัติการของ Cisco คือ IOS ว่ามีหลักการทำงานอย่างไร มีหมวดอะไรบ้าง แต่ละหมวดทำงานอย่างไร เป็นต้น

#### **Workshop 5:** การเริ่มต้นคอนฟิกอุปกรณ์โดยผ่าน console

สาธิตการปรับแต่งค่า Console เพื่อให้ผู้ใช้งานเปื้องต้นสามารถเข้าไป config อุปกรณ์ได้โดยผ่านทาง console (ซึ่งมีความจำเป็นมาก)

#### **Workshop 6:** การคอนฟิกอุปกรณ์โดยผ่านพอร์ต串ครอล Telnet

สาขิตการปรับแต่งเมื่อผู้ใช้ต้องการ Remote เข้าไป config อุปกรณ์เราเตอร์ หรือสวิชต์ ผ่านเครือข่ายเน็ตเวิร์ค เพื่อช่วยประหยัดเวลาในการทำงาน และควบคุมเครือข่ายจากจุดเดียว

#### **Workshop 7:** การคอนฟิกอุปกรณ์โดยผ่านโปรแกรม Secure Shell

สาขิตการปรับแต่งเมื่อผู้ใช้ต้องการ Remote แบบปลอดภัยเข้าไป config อุปกรณ์เครือข่าย

#### **Workshop 8:** การคอนฟิก loopback interface

สาขิตการสร้างเครือข่ายที่ใช้สำหรับทดสอบ โดยไม่จำเป็นต้องใช้อุปกรณ์ end device เพิ่มเติม ช่วยลดงบประมาณ ประหยัดเวลา และสะดวก

#### **Workshop 9:** การคอนฟิก vlan บน switch L2

สาขิตการสร้างเครือข่ายเสมือนบนอุปกรณ์สวิชต์ระดับเลเยอร์ที่ 2

#### **Workshop 10:** การคอนฟิก IP & Backup & Restore Configuration file บน Switch L2

สาขิตการสำรองข้อมูล configuration file, IOS operating system เพื่อใช้ในกรณีฉุกเฉิน

#### **Workshop 11:** การคอนฟิก vlan บน switch L3

สาขิตการสร้าง VLAN บนอุปกรณ์สวิชต์ L3 (3560) ว่ามีขั้นตอนอย่างไร

#### **Workshop 12:** การคอนฟิก static route บนเราเตอร์

สาขิตการคอนฟิก static route บนเราเตอร์ว่ามีขั้นตอนอย่างไร ซึ่งจะใช้เป็นพื้นฐานในการสร้างเครือข่ายที่มีความซับซ้อนต่อไป

#### **Workshop 13:** การคอนฟิก static route บน Switch L3

สาขิตการคอนฟิก static route บนสวิชต์ว่ามีขั้นตอนอย่างไร

#### **Workshop 14:** การคอนฟิก static route ระหว่าง Router และ Switch L3

สาขิตการคอนฟิก static route ระหว่าง Router และ Switch L3 ให้สามารถส่งข้อมูลกันได้เนื่องจากบางครั้งหน่วยงานหรือองค์ อาจจะใช้ Router ทำหน้าที่เป็น gateway เชื่อมต่ออินเทอร์เน็ต และใช้ Switch L3 ควบคุมเครือข่ายภายใน จึงจำเป็นต้อง เข้าใจการเชื่อมต่อระหว่างอุปกรณ์ทั้ง 2 ตัวเข้าด้วยกัน

#### **Workshop 15:** การเชื่อมต่อ Router ด้วยสาย Serial Interface

สาขิตการเชื่อมต่อและคอนฟิกเราเตอร์ด้วยสายชนิด Serial เนื่องจากเป็นสายที่พิเศษกว่าแบบอื่นๆ คือ สามารถกำหนดแบบดิจิตท์ ได้เอง โดยการกำหนด Clock Rate

#### **Workshop 16:** การเชื่อมต่อ Network บนโปรแกรม Packet Tracer เข้าด้วยกันโดยผ่าน Cloud (Multiuser)

สาธิตการเชื่อมต่อเครือข่ายที่ทำงานอยู่บนโปรแกรม Packet Tracer ที่อยู่ต่างที่กันให้สามารถเชื่อมต่อเป็นเครือข่ายที่มีขนาดใหญ่ได้ (สมมุติเป็นเครือข่ายอินเทอร์เน็ตซ้อนอยู่บนเครือข่ายอินเทอร์เน็ตจริงอีกชั้นหนึ่ง)

#### **Workshop 17: การค่อนฟิก Dynamic Routing (RIPv2)**

สาธิตการเชื่อมต่อเครือข่ายด้วยโพรโทคอล RIP ซึ่งเป็นโพรโทคอลพื้นฐานที่สำคัญที่ใช้กับเครือข่ายภายใน หรือ Intranet

#### **Workshop 18: การค่อนฟิก Dynamic Routing OSPF(Single Area)**

สาธิตการเชื่อมต่อเครือข่ายด้วยโพรโทคอล OSPF ซึ่งเป็นโพรโทคอลพื้นฐานที่สำคัญมากที่ใช้กับเครือข่ายภายใน หรือ Intranet โดยใช้ Area เดียว

#### **Workshop 19: การค่อนฟิก Dynamic Routing OSPF(Multiple Area)**

สาธิตการเชื่อมต่อเครือข่ายด้วยโพรโทคอล OSPF โดยใช้หลาย Area

#### **Workshop 20: การค่อนฟิก OSPF Authentication**

สาธิตการเชื่อมต่อเครือข่ายด้วยโพรโทคอล OSPF โดยมีการยืนยันตัวตนของอุปกรณ์เพื่อป้องการถูก Hack

#### **Workshop 21: การค่อนฟิก Dynamic Routing EIGRP**

สาธิตการเชื่อมต่อเครือข่ายด้วยโพรโทคอล EIGRP ซึ่งเป็นโพรโทคอลแบบ Dynamic ของ Cisco

#### **Workshop 22: การค่อนฟิก DHCP ข้ามเครือข่ายด้วย IP Helper**

สาธิตการสร้าง DHCP Server และให้สามารถ forward ข้อมูลของโพรโทคอล DHCP ข้ามเครือข่ายได้ เพราะในสถานะการณ์จริงองค์กรต่างๆ นิยมติดตั้ง DHCP Server บน เน็ตเวิร์คได้เน็ตเวิร์คหนึ่ง ส่งผลให้ไม่สามารถแยกไอพีข้าม VLAN ได้

#### **Workshop 23: การค่อนฟิกให้เราเตอร์ทำหน้าที่เป็น DHCP Server**

สาธิตการสร้าง DHCP Server บนอุปกรณ์ Router เอง เนื่องจากได้เปรียบทางด้านความเร็ว และการกระจายความผิดพลาดของ DHCP Server

#### **Workshop 24: การค่อนฟิก OSPF กับ EIGRP โดยใช้ Redistribution**

สาธิตการสร้างเครือข่ายที่มีโพรโทคอลตั้งแต่ 2 ชนิดขึ้นไปทำงานอยู่ด้วยกัน ใน workshop นี้จะสาธิตการทำงานของ OSPF ให้ทำงานร่วมกับ EIGRP

#### **Workshop 25: การค่อนฟิก Standard ACL (1)**

อธิบายหลักการทำงาน สาขิตการสร้างไฟร์วอลล์บนเราเตอร์ เรียกว่า ACL โดยเป็น ACL ชนิดทั่วๆ ไป (Standard) สามารถตรวจสอบการทำงานได้เฉพาะเลเยอร์ที่ 3 ของ OSI Model

#### **Workshop 26:** การคอนฟิก Standard ACL (2)

สาขิตการสร้าง ACL แบบ Standard และมีการอธิบายรายละเอียดการใช้งานที่เพิ่มขึ้น

#### **Workshop 27:** การคอนฟิก Standard ACL (3)

สาขิตการสร้าง ACL แบบ Standard เพิ่มขึ้น

#### **Workshop 28:** การคอนฟิก Extended ACL (1)

อธิบายหลักการทำงาน สาขิตการ ACL โดยเป็น ACL ชนิดพิเศษ (Extended) สามารถตรวจสอบการทำงานได้เฉพาะเลเยอร์ที่ 3, 4 ของ OSI Model

#### **Workshop 29:** การคอนฟิก Extended ACL (2)

สาขิตการสร้าง ACL แบบ Extended เพิ่มขึ้น

#### **Workshop 30:** การคอนฟิก Extended ACL (3)

สาขิตการสร้าง ACL แบบ Extended อย่างละเอียด และประยุกต์ใช้งานจริง

#### **Workshop 31:** การคอนฟิก Link สำรอง โดยใช้ Floating Static Route

สาขิตการสร้าง link สำหรับ เพื่อใช้สำหรับกรณีที่ เครือข่ายหลักไม่สามารถใช้งานได้

#### **Workshop 32:** การคอนฟิก Static NAT

สาขิตการค่อนฟิก NAT แบบ Static ซึ่งเป็นที่นิยมใช้งานในปัจุบัน เพื่อให้สามารถเชื่อมต่อเครือข่ายอินเทอร์เน็ตได้

#### **Workshop 33:** การค่อนฟิก Static/Dynamic NAT ร่วมกับ ACL

สาขิตการประยุกต์ใช้งานในเครือข่ายที่ทำงานจริงในปัจุบัน คือ การผสมผสานระหว่าง Dynamic NAT + Static และ ACL เข้าด้วยกัน

#### **Workshop 34:** การค่อนฟิก Switch L3 ร่วมกับ Router

สาขิตการประยุกต์ใช้งานอุปกรณ์สวิชต์ L3 ทำหน้าที่เป็น Backbone network ในองกรณ์ และใช้ Router ทำหน้าที่เชื่อมต่อเป็น gateway กับ ISP

#### **Workshop 35:** การค่อนฟิก BGP เปื้องต้าน

สาขิตการค่อนฟิกโพรโทคอล BGP ซึ่งเป็นโพรโทคอลที่ใช้สำหรับเชื่อมต่อเครือข่าย WAN ในปัจุบัน

### Workshop 36: การใช้งาน Activity Wizard

สาธิตการใช้งาน Activity Wizard ซึ่งมีประโยชน์อย่างมากสำหรับอาจารย์หรือคุณครูที่สอนด้านระบบเครือข่าย คุณสมบัตินี้จะช่วยให้สร้างบนเรียนหรือแบบทดสอบการสร้างเครือข่ายแบบ step-by-step ทำให้ผู้เรียนเข้าใจเครือข่ายได้อย่างรวดเร็ว และอาจารย์ก็สามารถสร้างข้อสอบได้อย่างมีประสิทธิภาพ

**หมายเหตุ:** สุดท้ายนี้ผู้เขียนหวังเป็นอย่างยิ่งว่าหนังสือเล่มนี้ น่าจะมีประโยชน์ไม่น้อยก็น้อยสำหรับผู้ที่ชื่นชอบระบบเครือข่าย สำหรับเนื้อหาทั้งหมดยังไม่ครอบคลุมระบบเครือข่ายทั้งหมด ซึ่งหวังอีกรึว่าอาจจะมีเล่มที่ 3 ออกมาให้ผู้สนใจทุกท่านได้อ่านกันอีก (ถ้ามีโอกาส) สวัสดีครับ

สุชาติ คุ้มมะณี  
suchart.k@msu.ac.th