ใบงานที่5

การวิเคราะห์แพ็คเก็ตอย่างละเอียด

(แนะนำเทคนิคการเฝ้ามองแพ็คเก็ตอย่างเป็นระบบ)

จุดประสงค์

1) เพื่อให้เข้าใจเกี่ยวกับการวิเคราะห์แพ็คเก็ตได้อย่างละเอียด

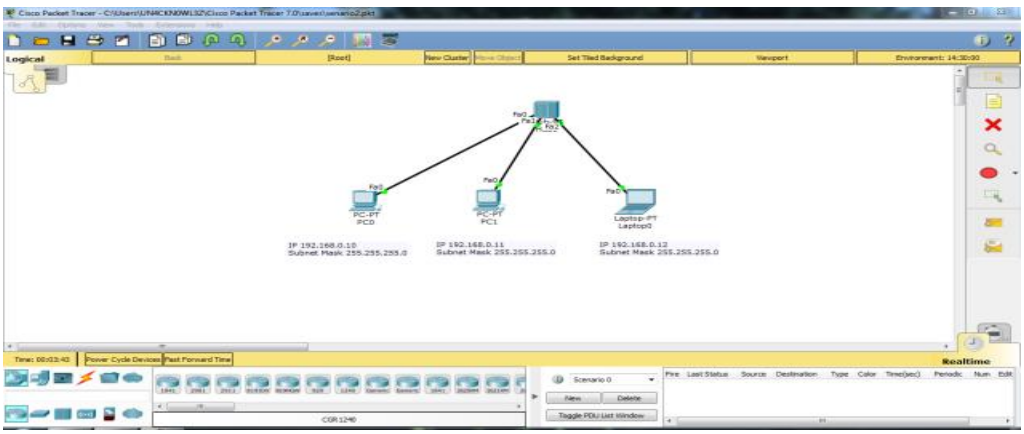
2) เพื่อให้รู้ขั้นตอนวิธีการวิเคราะห์แพ็คเก็ตอย่างละเอียด

3) เพื่อเฝ้าดูแพ็คเก็ตแบบต่อเนื่อง หรือเมื่อต้องการเฝ้ามองทีละ step ได้

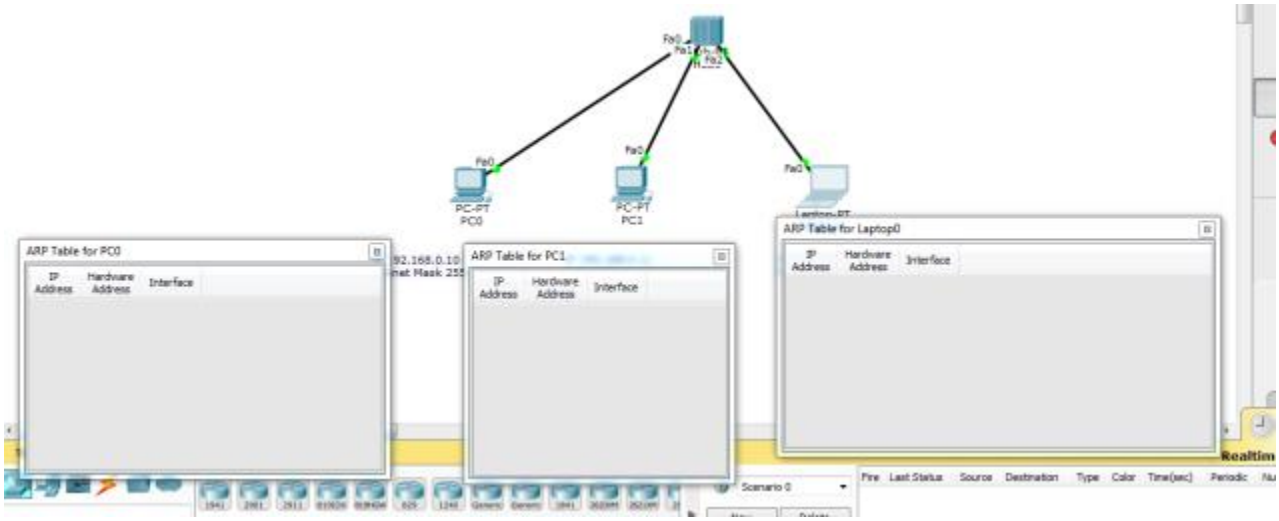
Cisco Packet Tracer เป็นโปรแกรมสำหรับจำลองระบบเครือข่าย (Networking Simulation Tool) ที่พัฒนาโดย Cisco ช่วยให้นักเรียนสามารถจำลองการเชื่อมต่อของระบบเครือข่าย จำลองการทำงานของอุปกรณ์จริงในระบบ Network ช่วยอำนวยความสะดวกในการเรียนการสอนเกี่ยวกับเทคโนโลยีเครือข่ายที่ซับซ้อน ช่วยให้นักเรียนสามารถสร้างเครือข่ายที่มีอุปกรณ์ได้ไม่จำกัดจำนวน กระตุ้นให้ฝึกฝน ค้นพบ และแก้ไขปัญหาต่างๆ เกี่ยวกับระบบเน็ตเวิร์ค

การวิเคราะห์แพ็คเก็ตอย่างละเอียด

Scenario จะนำ lab จากบทความที่แล้วมาใช้ โดยจะเป็นการวิเคราะห์ packet ในโปรโตคอล ICMP และ ARP เริ่มจากนำ lab จากครั้งที่แล้วมาเตรียมไว้

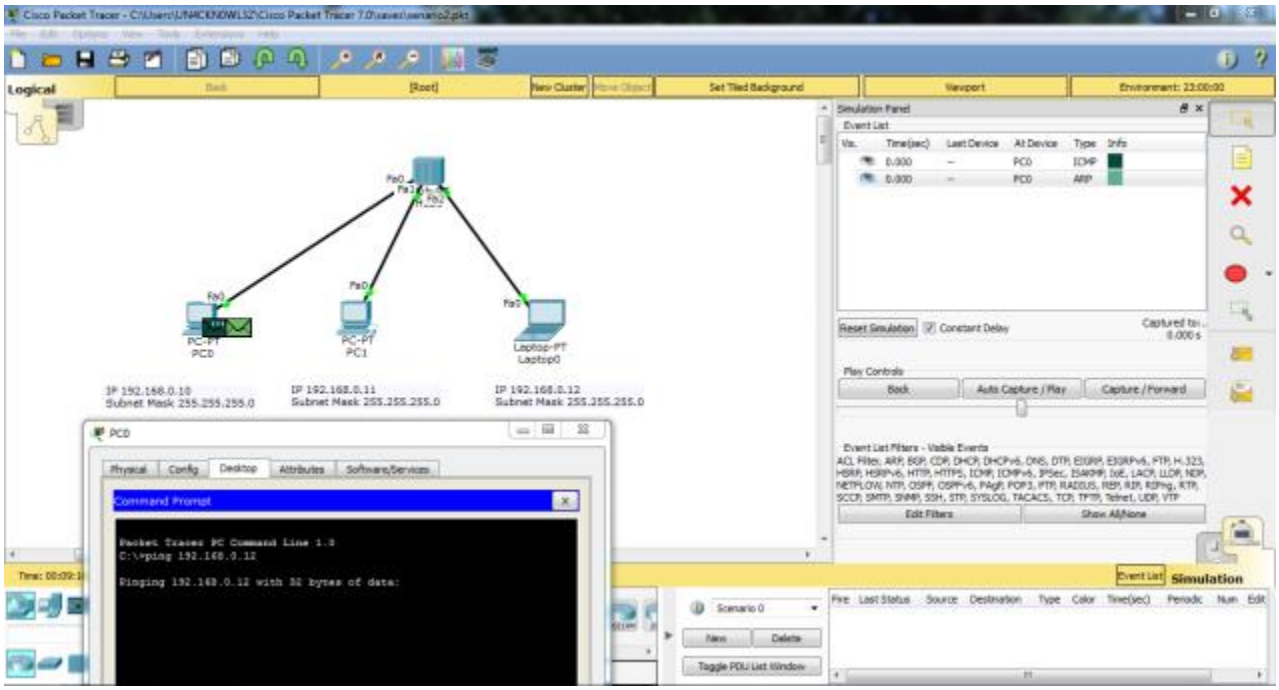


ขั้นตอนแรกก็ใช้ inspect เช็ค device แต่ละเครื่องก่อนว่ามี ARP Table แล้วหรือป่าว ซึ่งตอนนี้ยังไม่การเรียกใช้โปรโตคอล ARP แต่ละเครื่องก็จะยังไม่มี ARP Table (ARP เป็นโปรโตคอลที่ทำหน้าที่สอบถามว่าหมายเลข IP Address ที่ต้องการติดต่อมีหมายเลข MAC ใดและ Reverse ARP เป็นการถามกลับว่าหมายเลข MAC ที่ต้องการติดต่อตรงกับหมายเลข IP Address ใด)



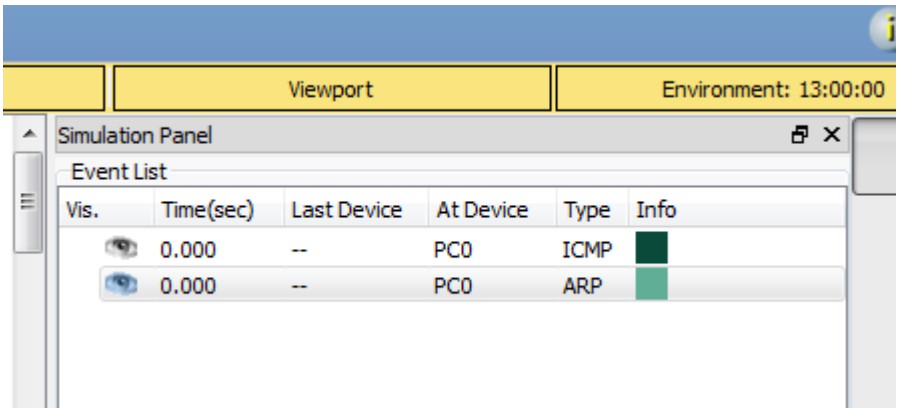
จากนั้นก็ให้ใช้โหมด Simulation ในการ สังเกตพฤติกรรมการทำงานของแพ็คเก็ต

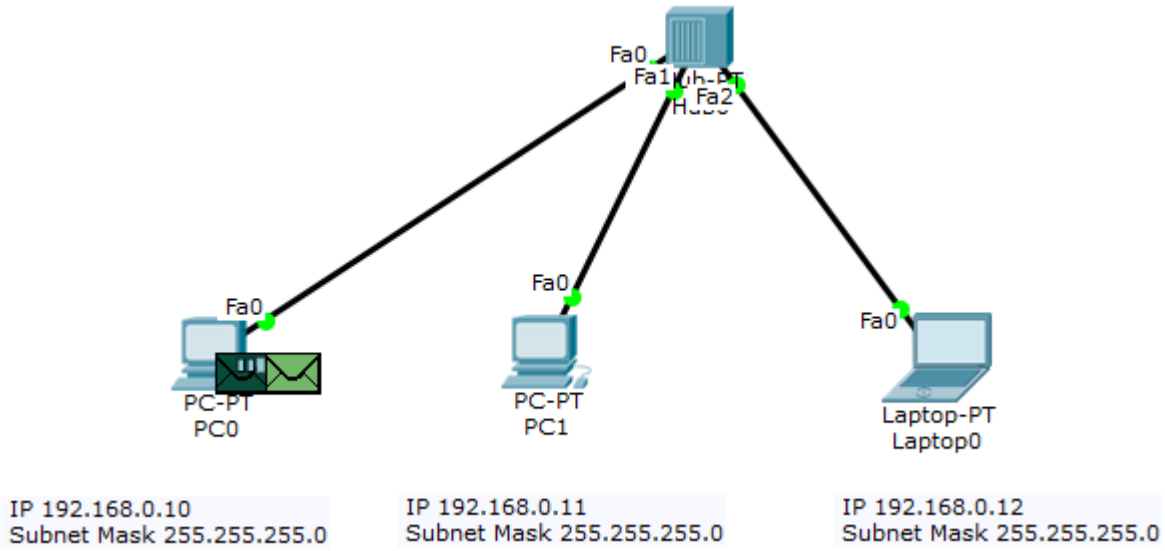
โดยจะให้ PC0 ping ไปหา Laptop0 (ping 192.168.0.12)



จากนั้นโปรแกรมก็จะหยุดการส่ง packet รอจนกว่าเราจะกด Capture/Forward

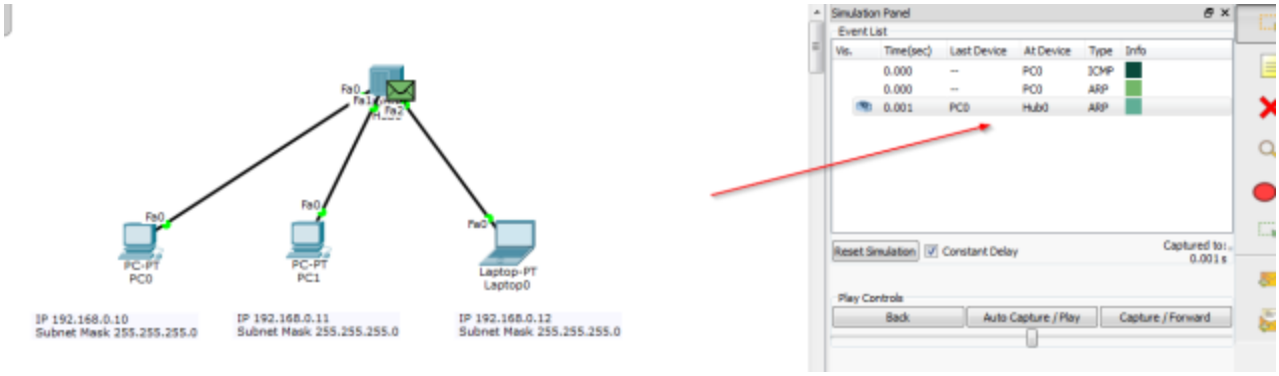
จะเห็นว่ามีแพ็คเก็ต ICMP และ ARP วิ่งจากเครื่อง PC0 ที่เวลา 0.000 วินาที)



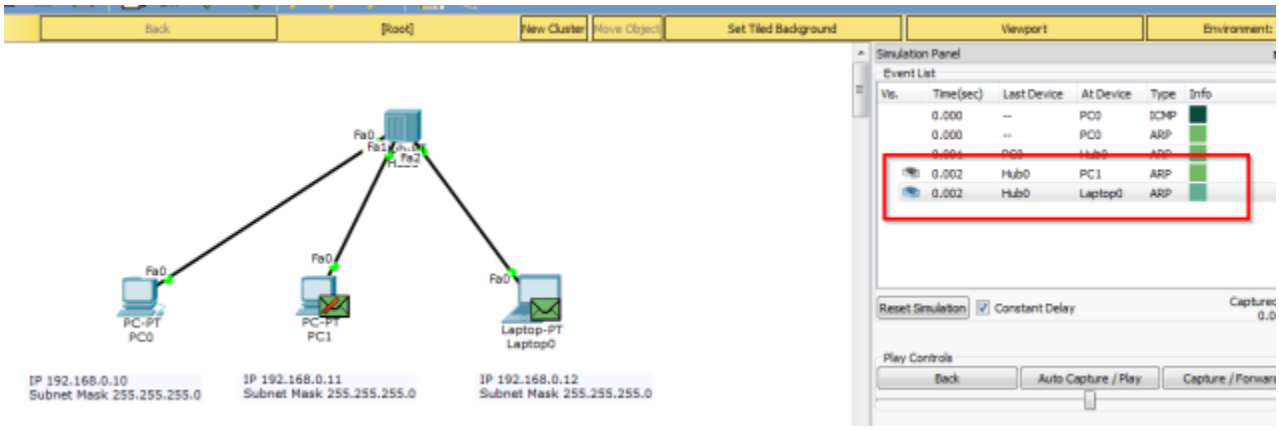


เนื่องจากคำสั่ง ping นั้นใช้หมายเลข IP Address ในการทดสอบ ณ สถานะการณ์ ปัจจุบันเครื่อง PC0 ไม่ทราบว่าเครื่องเป้าหมาย (192.168.0.12) คือใคร เพราะในตาราง ARP Table ยังไม่มีข้อมูลใดๆ เลย ดังนั้นเครื่อง PC0 จึงส่งแพ็คเก็ต ARP กระจาย ออกไปยังทุกๆ พอร์ตยกเว้นตัวมันเอง (พอร์ต PC0)

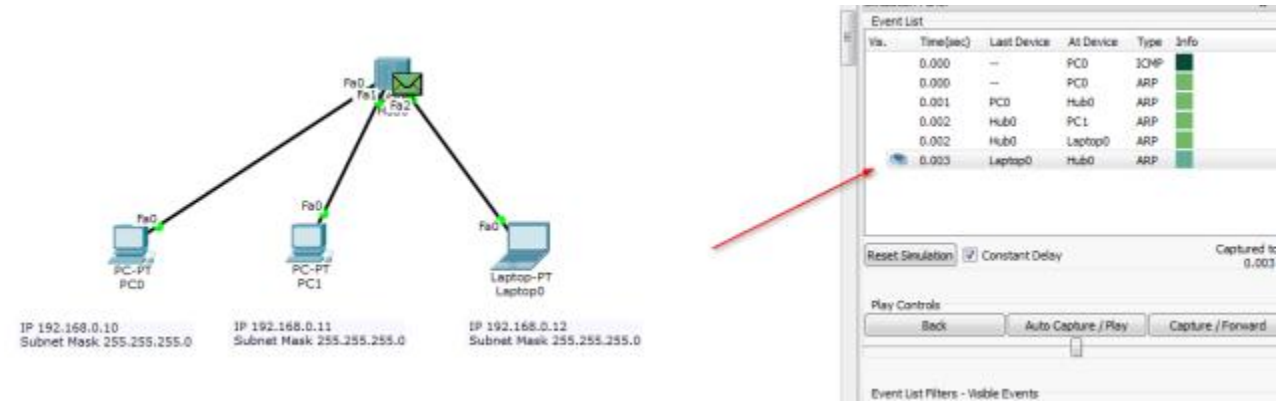
แพ็คเก็ต ARP จะส่งต่อไปยัง HUB (เวลา 0.001 ใน Even List)



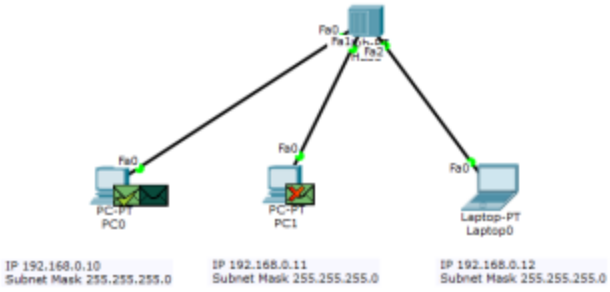
HUB จะส่งแพ็คเก็ต ARP ต่อไปยัง PC1 และ Labtop0 พร้อมกัน (เวลา 0.002 ใน Even List)

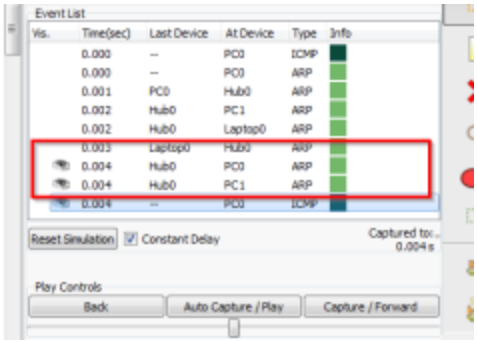


Labtop0 จะตอบกลับ ARP reply กลับมา เนื่องจากเป็นเครื่องที่มี IP Address เท่ากับ 192.168.0.12 แต่ เครื่อง PC1 จะไม่ตอบกลับเพราะไม่ใช่ IP ของตนเอง

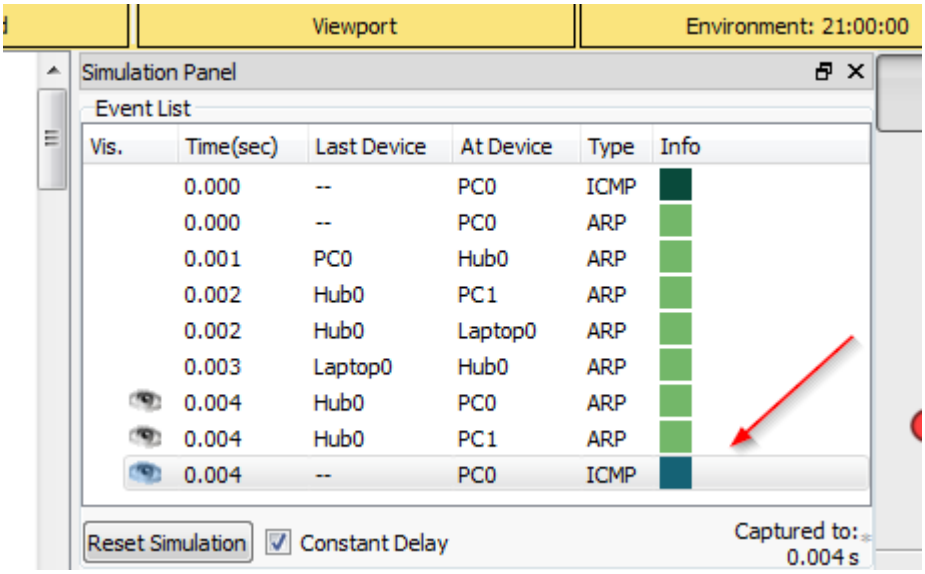


HUB จะกระจายแพ็คเก็ตที่ส่งมาจาก Laptop0 ไปยังทุกๆ เครื่องเนื่องจากคุณสมบัติ ของ HUB จะกระจายข้อมูลไปยังทุกๆ พอร์ตเสมอ

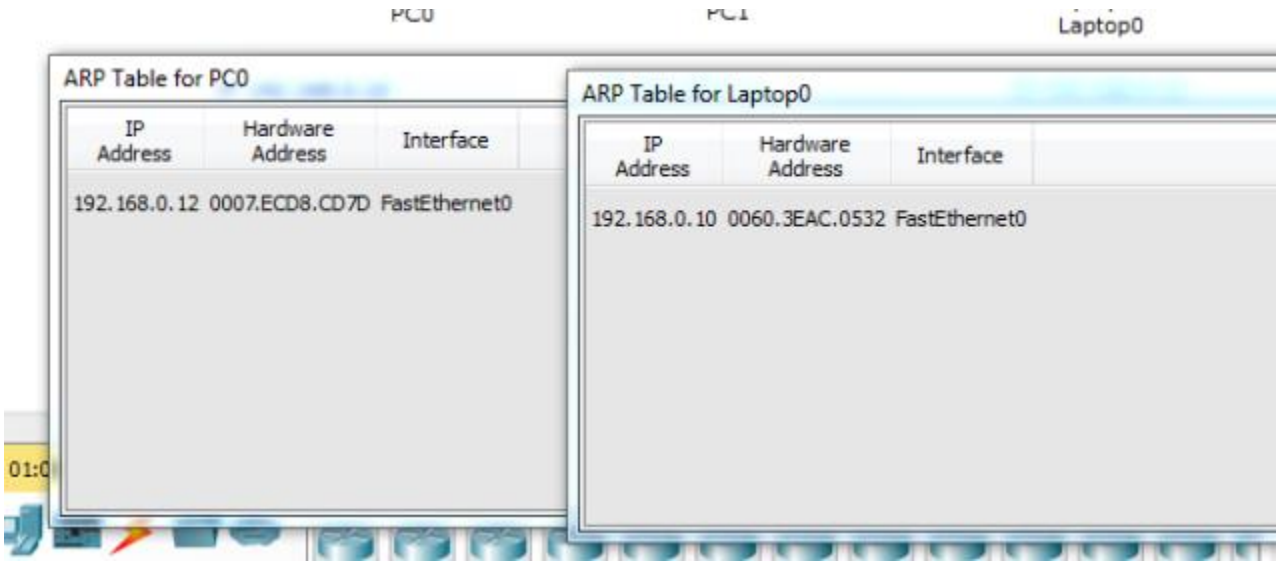




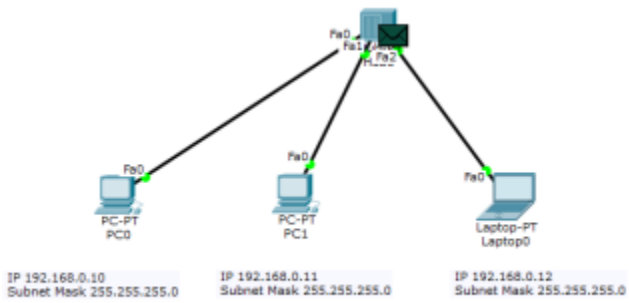
ในเวลาที่ 0.004 เครื่อง PC0 ก็จะทราบแล้วว่า IP 192.168.0.12 คือใครจึงทำการส่ง ICMP ออกไปยังเครื่องเป้าหมายทันที

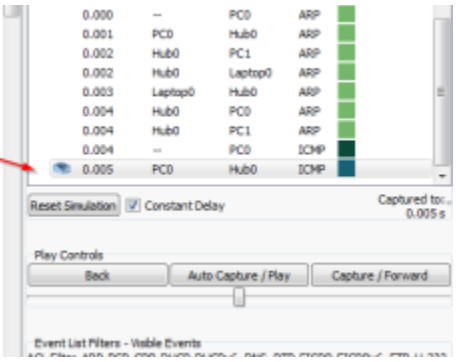


เมื่อถึงขั้นตอนนี้ ARP Table ของเครื่อง PC0 และ Labtop0 ก็จะถูก Update

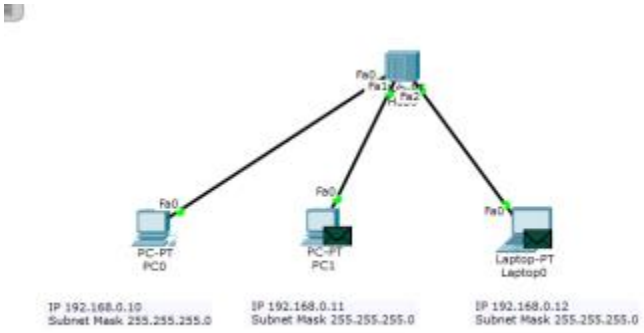


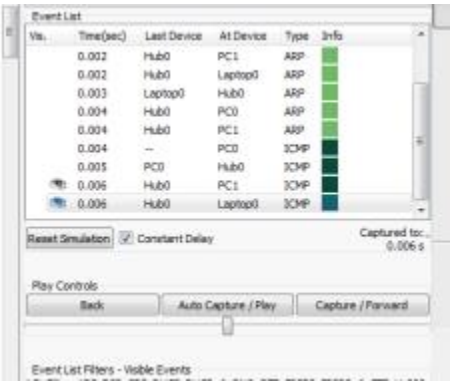
เวลาที่ 0.005 เครื่อง PC0 ส่ง ICMP อีกครั้งไปยัง HUB



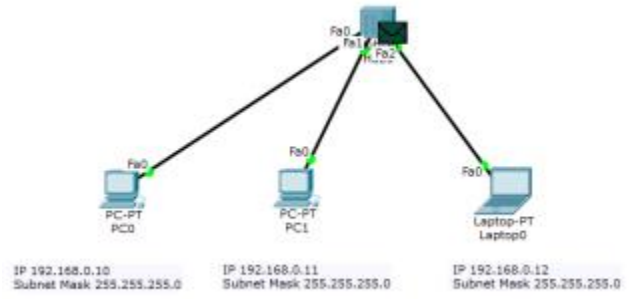


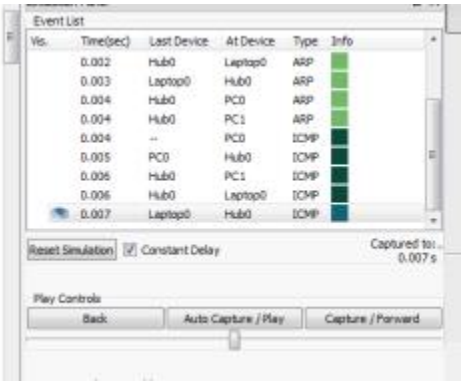
เวลาที่ 0.006 HUB จะกระจายแพ็คเก็ต ICMP ไปยังทุกๆ พอร์ต (คุณสมบัติของ HUB)



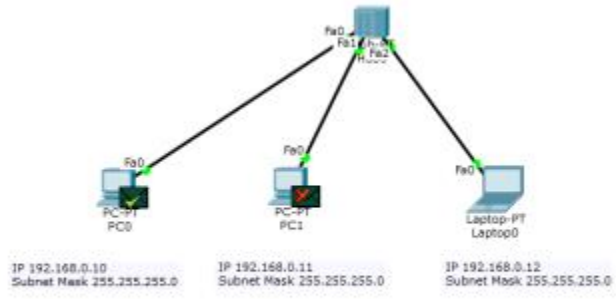


เวลาที่ 0.007 Labtop0 ส่งแพ็คเก็ต ICMP reply กลับไปยัง HUB

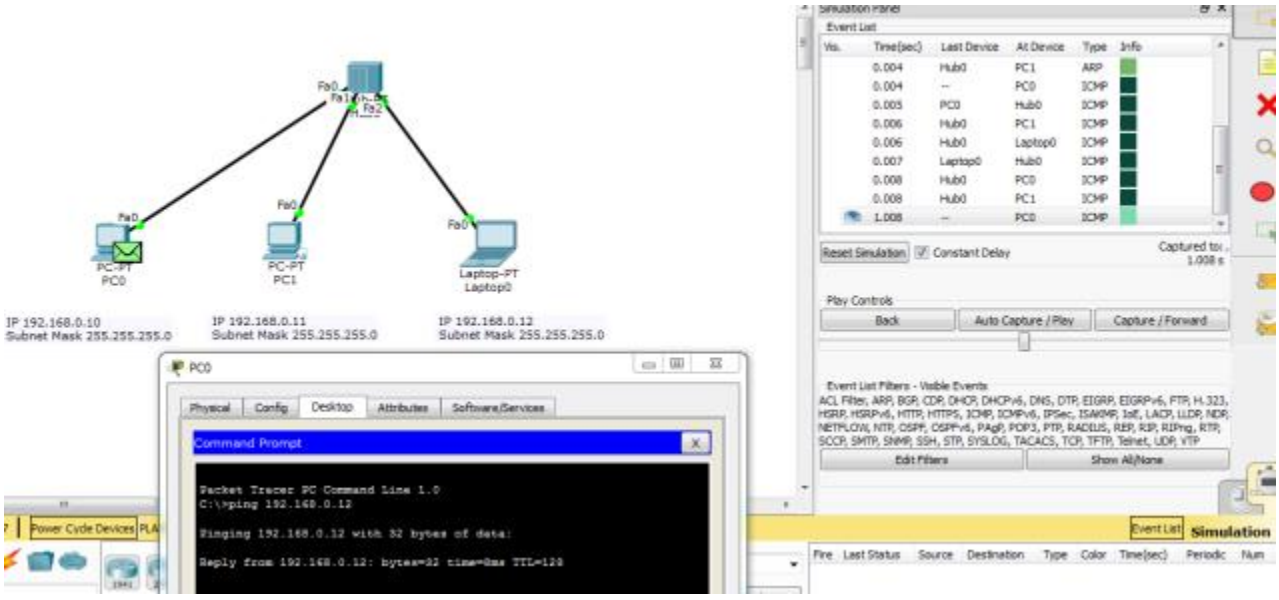




เวลาที่ 0.008 HUB จะกระจายแพ็คเก็ต ICMP ไปยังทุกๆ พอร์ต (คุณสมบัติของ HUB)

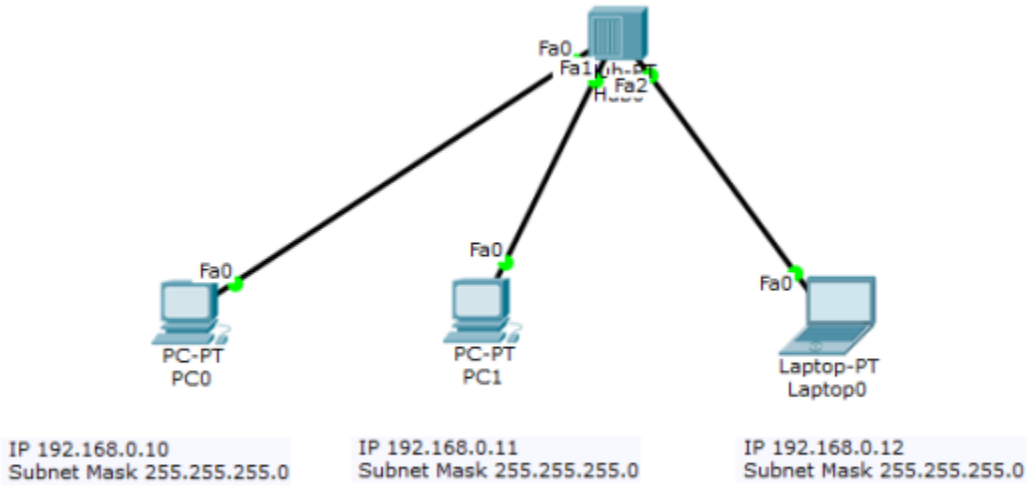


การเชื่อมต่อก็จะสำเร็จลง เมื่อทำการ ping ครั้งที่ 2 แพ็คเก็ตก็ยังคงเดินทางไปหาทุก เครื่องเหมือนเดิม (ตอบกลับเฉพาะเครื่องที่เป็นเป้าหมายเท่านั้น) เพราะคุณสมบัติของ HUB นั้นจะส่งไปยังทุกๆ พอร์ต แต่จะไม่เกิดกระบวนการ ARP ครั้งที่ 2 จนกว่า จะถึง เวลาที่ ARP Cache expire ซึ่งจะใช้เวลาประมาณ 10 นาที (600 วินาที)



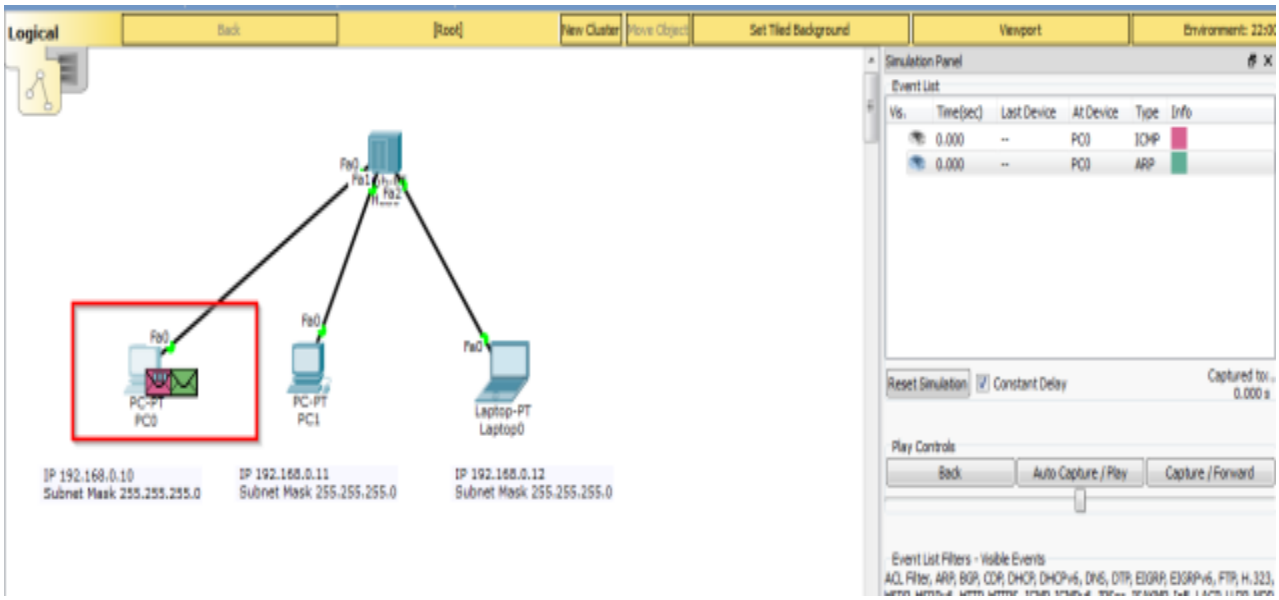
การวิเคราะห์แพ็คเก็ตใน Scenario 3 ได้ทำการวิเคราะห์ทิศทางการส่งข้อมูล สำหรับใน Scenario 4 นี้ จะพิจารณาแพ็คเก็ตในระดับที่ลึกซึ้งลงไปถึงระดับบิตข้อมูล Scenario ก็จะใช้ lab จาก Scenario 2 เช่นเดิมครับช

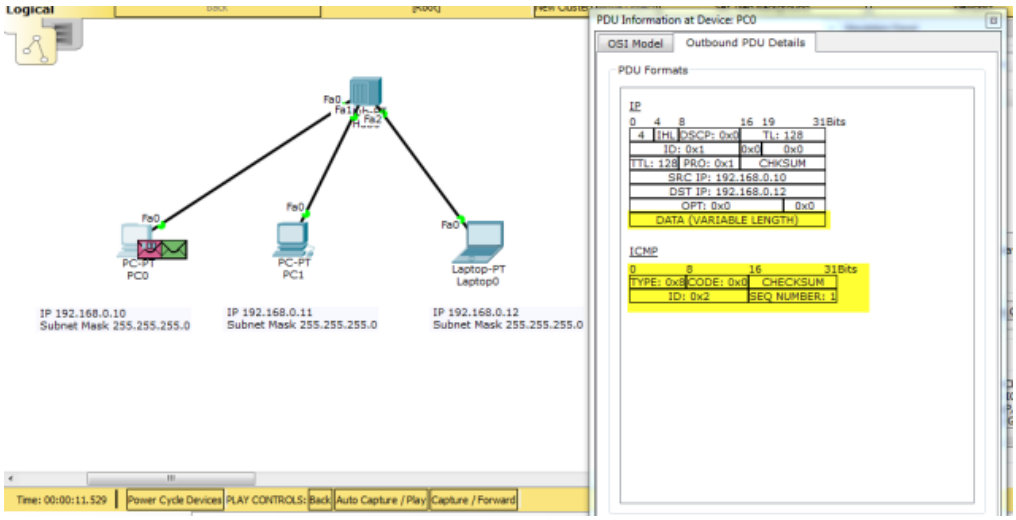
แผนผังการเชื่อมต่อ :



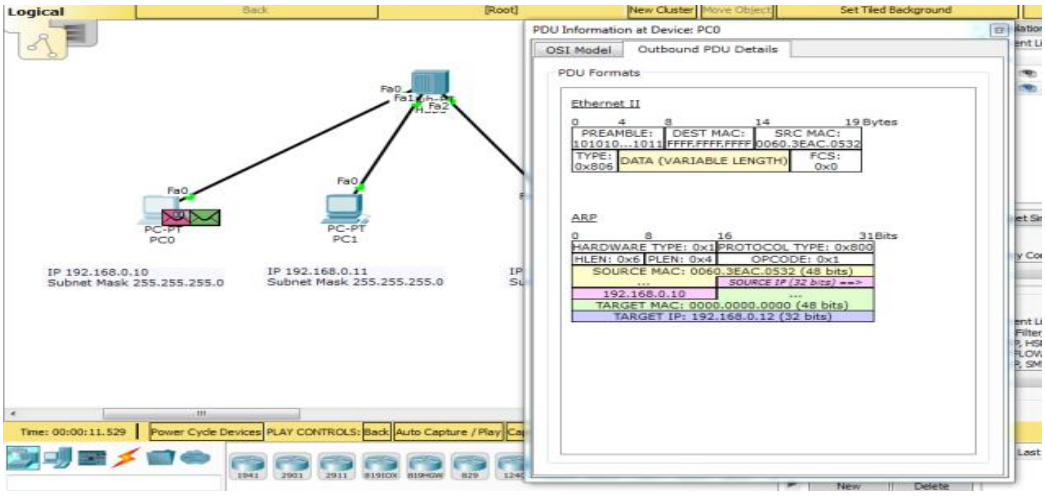
เริ่มต้นที่เครื่อง PC0 โดยการใช้คำสั่ง ping จาก Command Prompt ไปยังเครื่อง Labtop0 อีกครั้ง

ในโหมด Simulation เมื่อออกคำสั่ง ping แล้ว ให้ใช้ Inspect ตรวจสอบแพ็คเก็ต ที่มี รูปเป็นซองจดหมาย





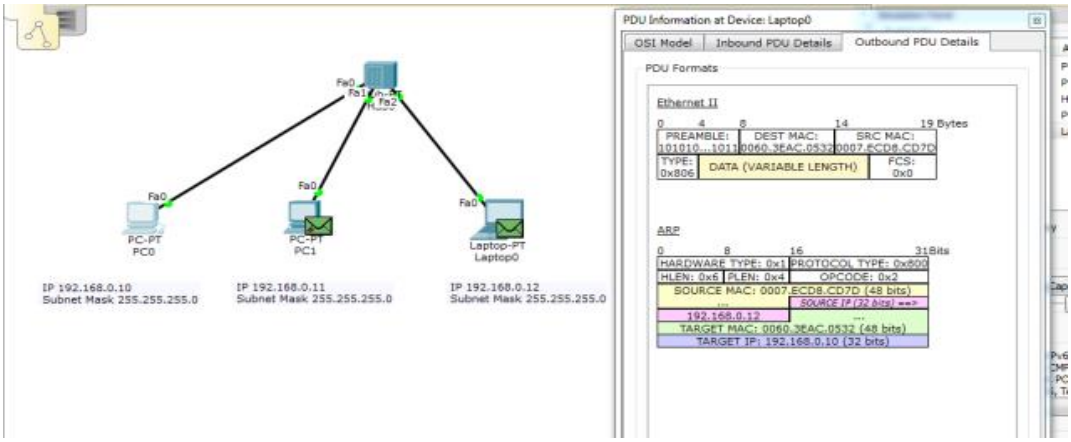
จากรูปข้างบนการสื่อสารข้อมูลในเน็ตเวิร์คจะแบ่งออกเป็นชั้นๆ ตามหลักการของ OSI Model จากในตัวอย่าง แพ็คเก็ตของ ICMP นั้นจะถูกซ่อนอยู่ใน IP (encapsulation) เพื่อให้แพ็คเก็ต IP นั้นเป็นผู้ส่งแพ็คเก็ต ICMP ไปให้ถึงปลายทาง ข้อมูลของ ICMP จะเป็นข้อมูลในส่วนของ DATA ใน IP แพ็คเก็ต โดย ICMP แพ็คเก็ตมี ขนาดเท่ากับ 32 บิต x 2 คือ 64 บิต ประกอบไปด้วย Type มีขนาด 8 บิต เอาไว้บอกว่าเป็น โพรโทคอล ICMP ชนิด Echo Request, CODE มีค่าเท่ากับ 0, CHECKSUM เป็นค่าที่ใช้ สำหรับตรวจสอบความผิดพลาดของข้อมูล, ID มีค่าเป็น 2, SEQ NUMBER คือลำดับของ แพ็คเก็ต ซึ่งจะเปลี่ยนไปเรื่อยๆ ในที่นี้คือ 1



จากรูปข้างบน แสดงข้อมูลของแพ็คเก็ต ARP ที่อาศัยโพรโทคอล Ethernet (ทำงานในเลเยอร์ที่ 2) ส่งไปยังปลายทาง ข้อมูลที่อยู่ใน DATA ของ Ethernet frame จะเป็นแพ็คเก็ตของ ARP มีข้อมูลคือ HARDWARE TYPE=1, PROTOCOL TYPE=0x800, HLEN=ความยาวของ Header, PLEN=ความยาวของเนื้อข้อมูล, OPCODE=0x1, SOURCE MAC=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) สังเกตุว่าใน Ethernet frame จะ DEST MAC= FFF.FFF.FFF แสดง ว่าเป็นการ broadcast ข้อมูลไปทุกๆ เครื่อง

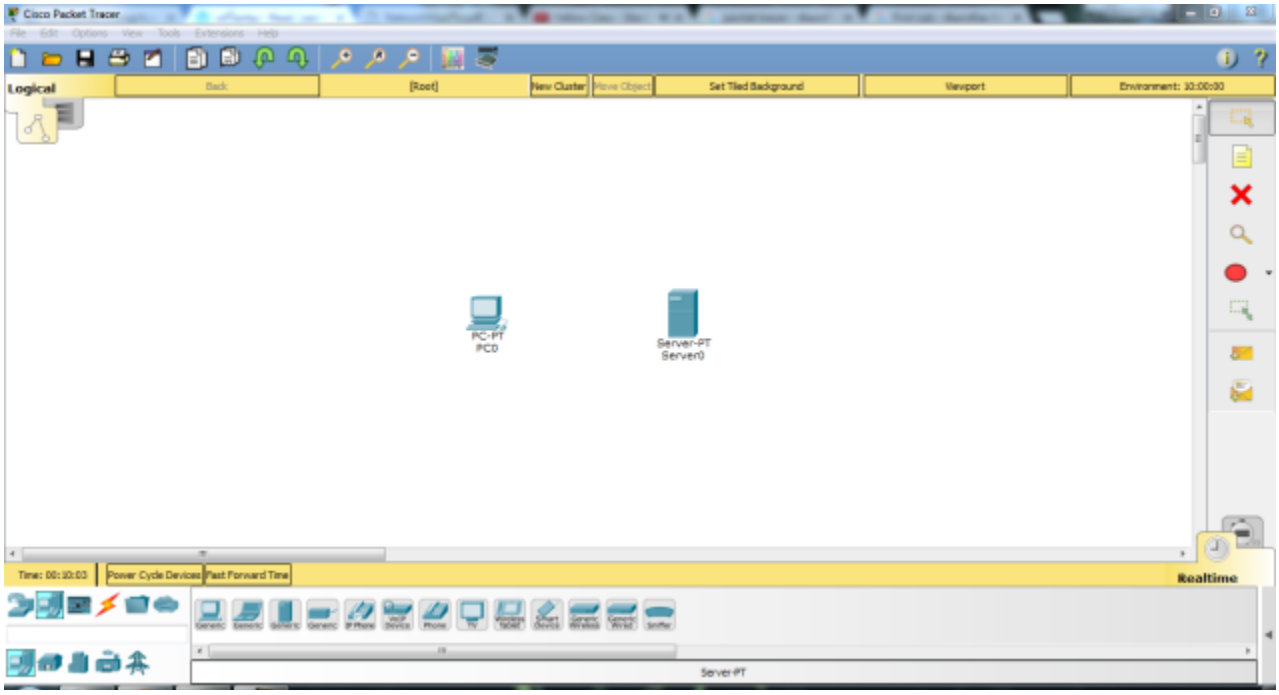
เมื่อเครื่องปลายทาง ได้รับแพ็คเก็ตแล้วจะส่ง ARP Reply กลับไปยังเครื่องที่ส่งข้อมูลมา โดยการ update ค่า SOURCE MAC, SOURCE IP, TARGET MAC, TARGET IP ในARP frame



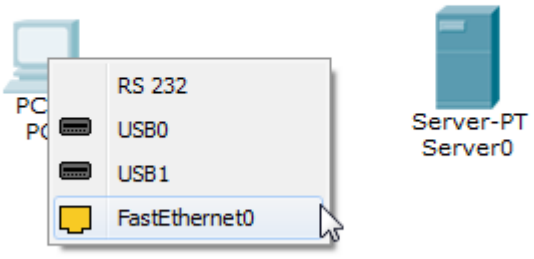
ค่าของ SOURCE IP เป็น 192.168.0.10 และ TARGET IP เป็น 192.168.0.12 เมื่อ ตอบกลับ จะสลับค่าเป็น SOURCE IP เป็น 192.168.0.12 และ TARGET IP เป็น 192.168.0.10 เช่นเดียวกัน ค่าของ MAC ก็จะสลับตามหมายเลข IP สำหรับแพ็คเก็ตอื่นๆ ก็ จะสามารถสังเกตุได้ด้วยวิธีการเดียวกัน

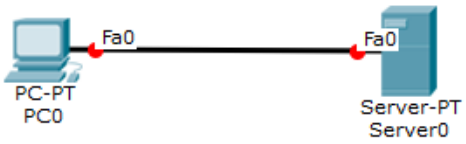
เทคนิคการเฝ้ามองแพ็คเก็ตอย่างเป็นระบบ

ขั้นตอนแรกให้เลือก End Device –> ลาก generic pc กับ generic server ไปวาง



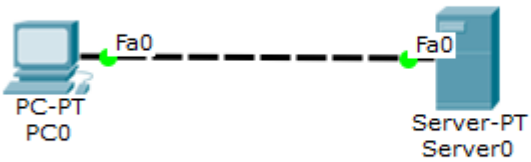
ทีนี้ให้เลือก connection เป็น Copper Straight Through (เส้นสีดำไม่มีเส้นประ) ทำการเชื่อมต่อ เลือก port เป็น FastEthernet



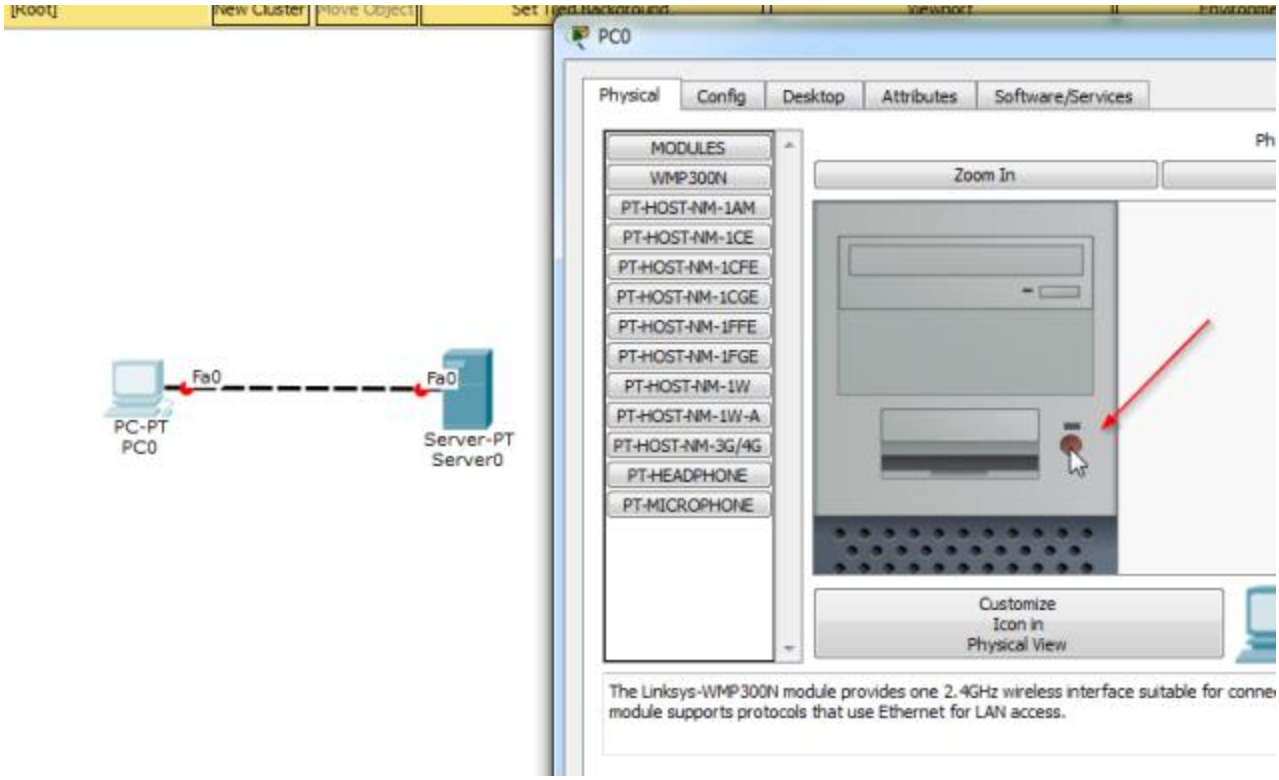


แต่จะเห็นว่า link เป็น สีแดง ที่เป็นแบบนี้เพราะว่าเลือก สาย ผิด อิอิ ต้องเปลี่ยนใหม่เป็น Copper Cross Over แทน ลบสายเดิมได้โดยการ กดที่ ปุ่ม delete สีแดง

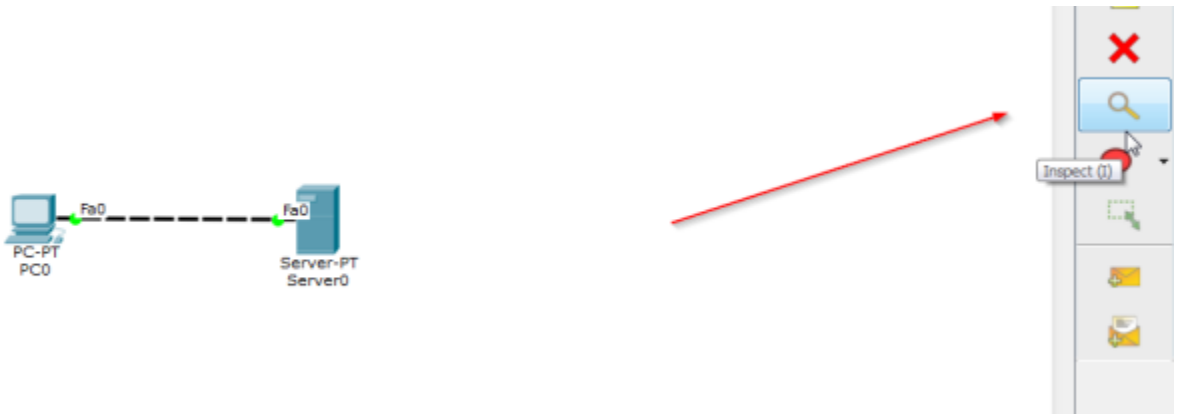
สถานะของลิงค์จะเป็นสีเขียว แสดงว่าใช้งานได้แล้ว

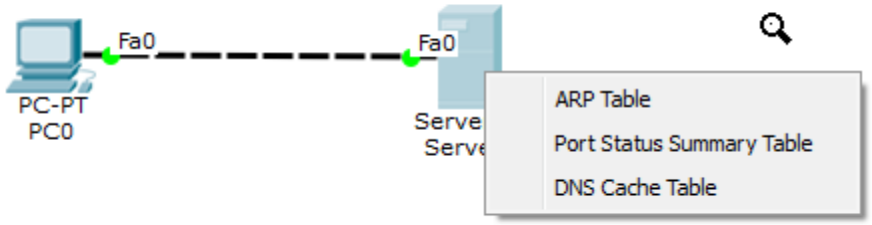


ทดลองเปิด-ปิด device ได้ โดนดับเบิลคลิกที่ pc ไปยังแท็บ physical แล้วกดที่ ปุ่ม power ตามรูป



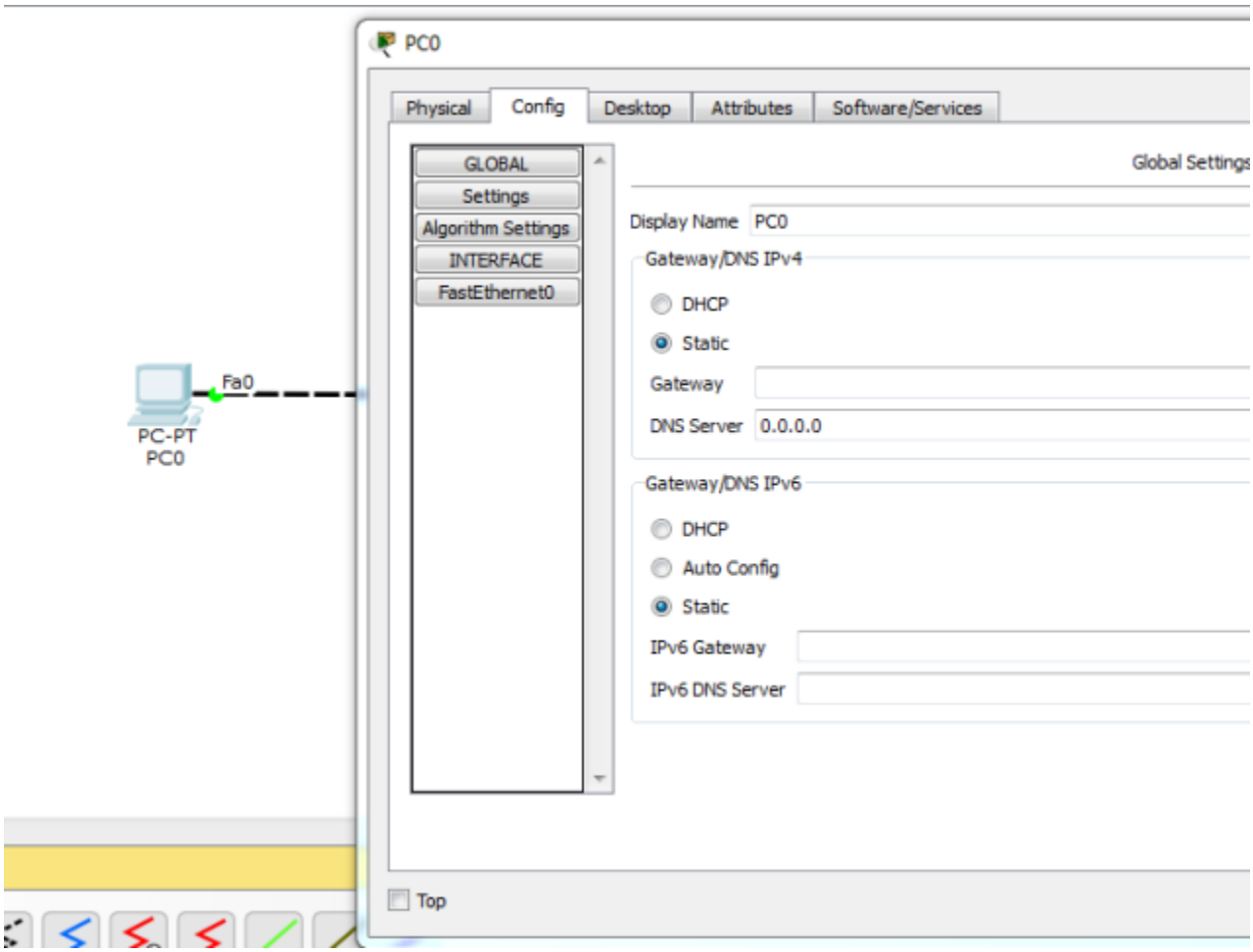
จากนั้นทดลองตรวจสอบค่าของเครื่อง PC และ Server โดยใช้ Inspect คลิกที่เครื่อง ทั้งสอง ให้ทำการตรวจสอบ ARP Table, Port Status Summary Table และ DNS Cache Table



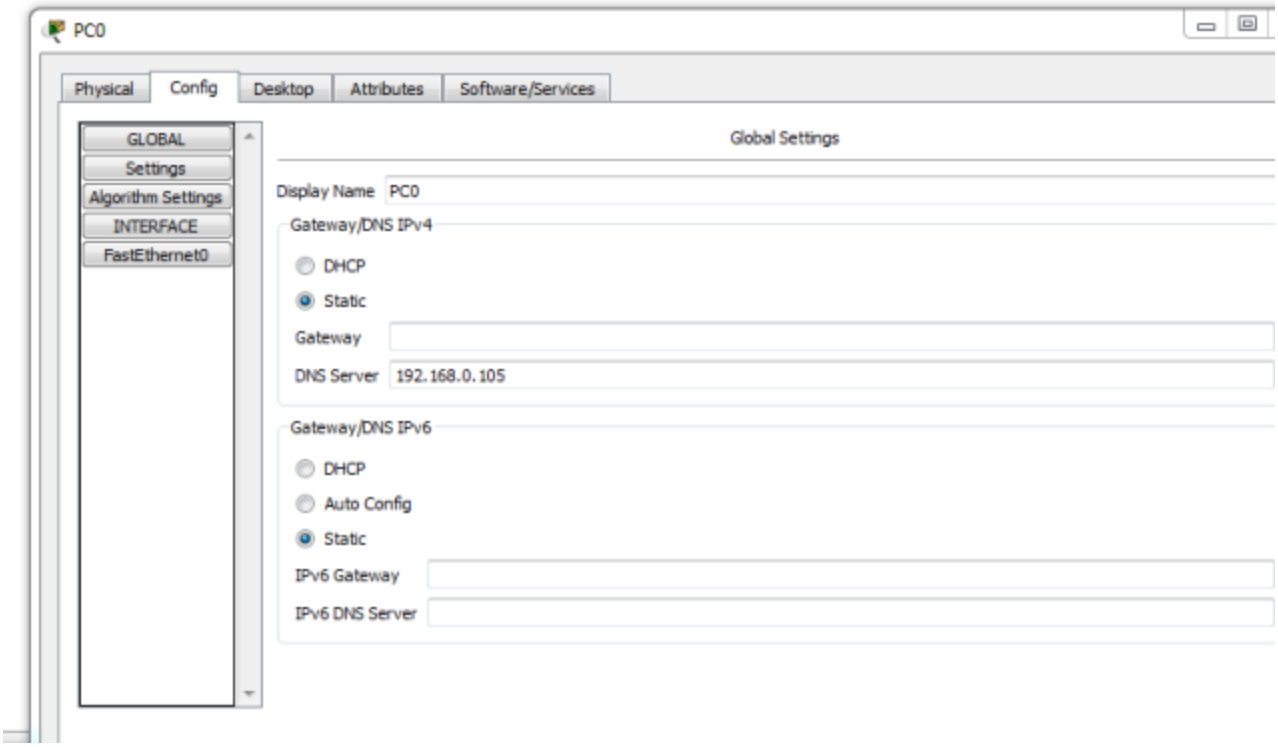


ตอนนี้ ARP Table, Port Status Summary Table และ DNS Cache Table จะยังไม่มีค่าใดๆ config อยู่

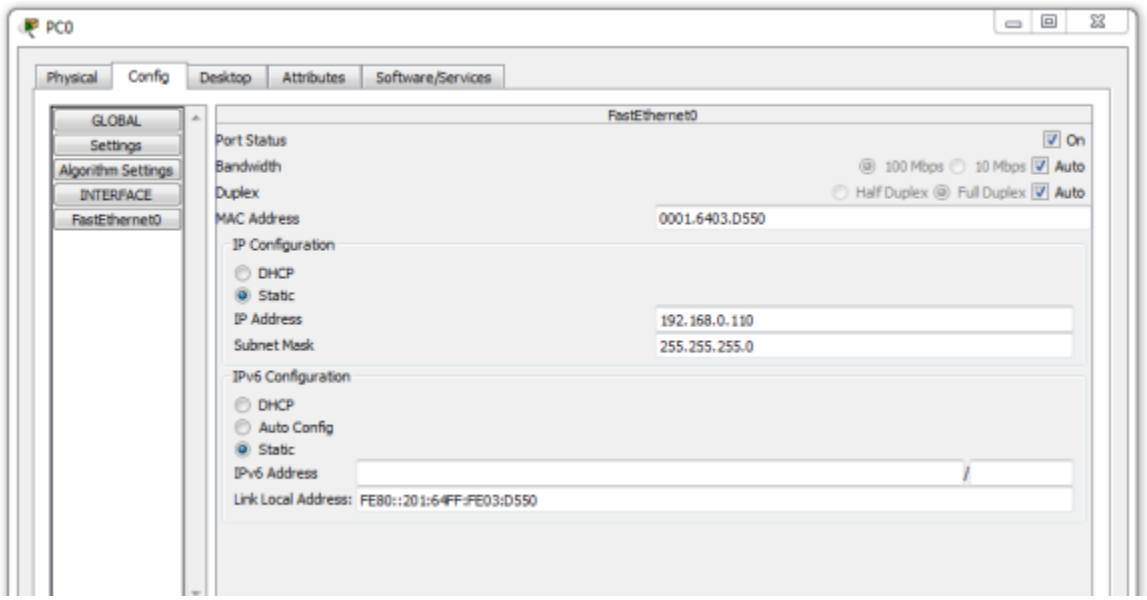
ต่อไปจะเป็นการกำหนด IP Address ให้กับ device ทำได้โดยการ ดับเบิลคลิก ที่ pc แล้วไปที่แท็บ config



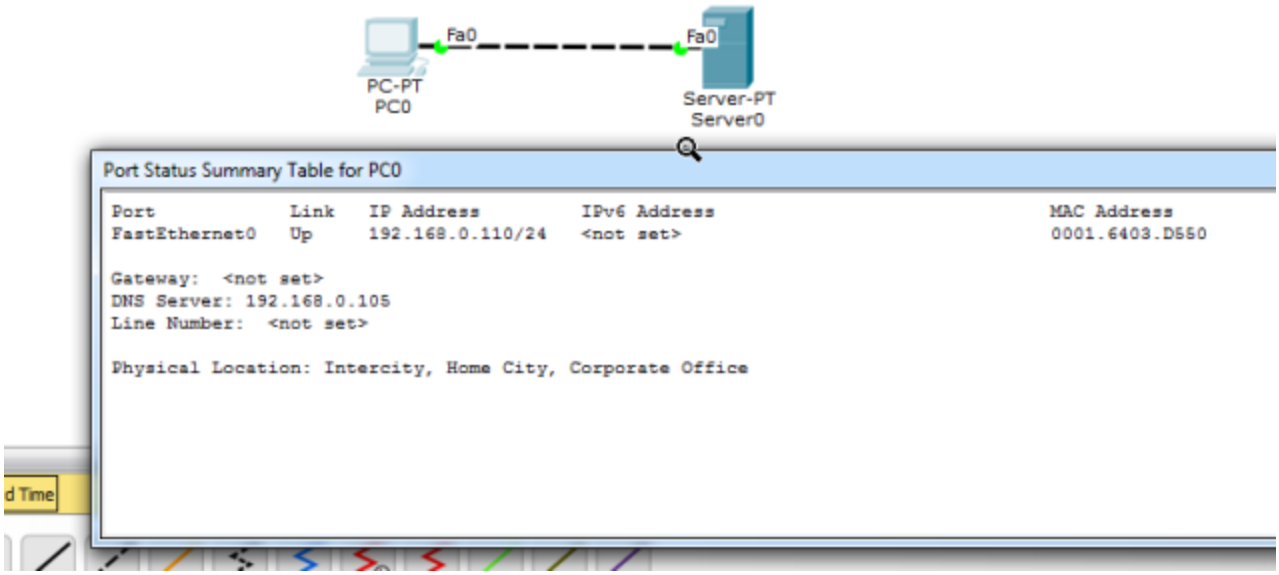
กำหนด DNS Server เป็น 192.168.0.105



เลือกอินเทอร์เฟสชนิด FastEthernet ให้กำหนด IP Address เป็น 192.168.0.110

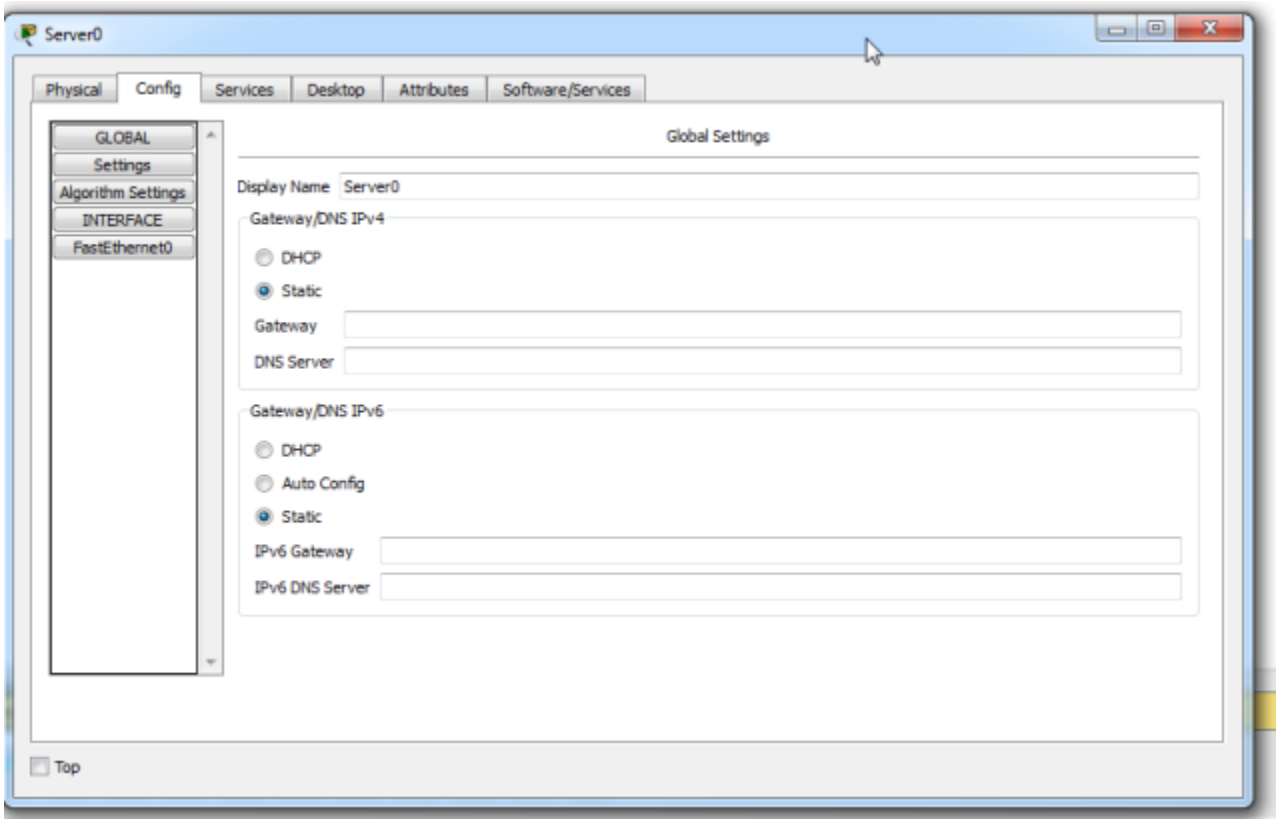


แล้วทดสอบโดยใช้ Inspect (ยกเลิก Inspect ให้กดปุ่ม esc) อีกครั้ง ที่ Port Status จะปรากฏหมายเลข MAC Address และ IP Address

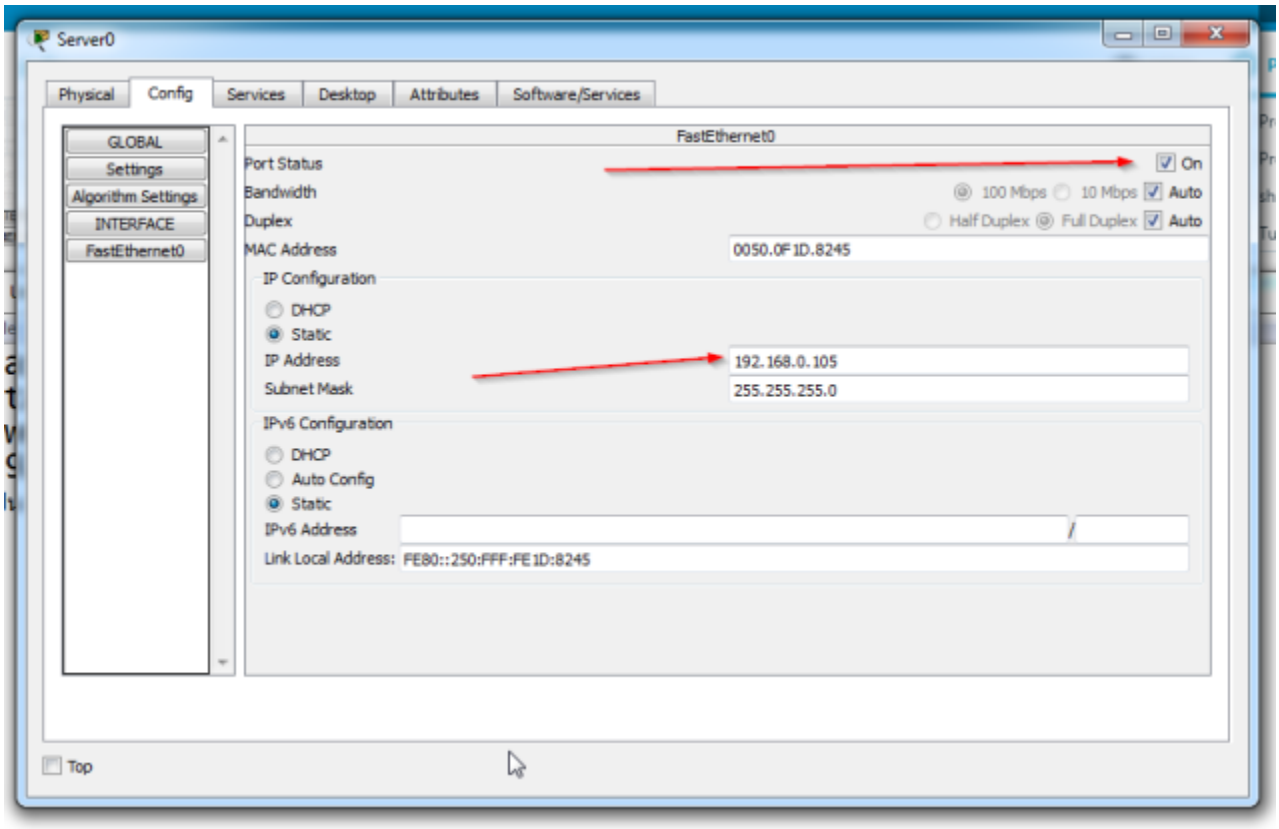


เมื่อต้องการกำหนดค่า Bandwidth,Duplex, DHCP, IPv6 ก็สามารถกำหนดได้ในเมนูนี้เช่นเดียวกัน การกำหนดค่า IP Address, Subnet Mask, Default Gateway, DNS Server สามารถกำหนดได้ในแท็บ Desktop >> IP Configuration ได้เช่นเดียวกัน

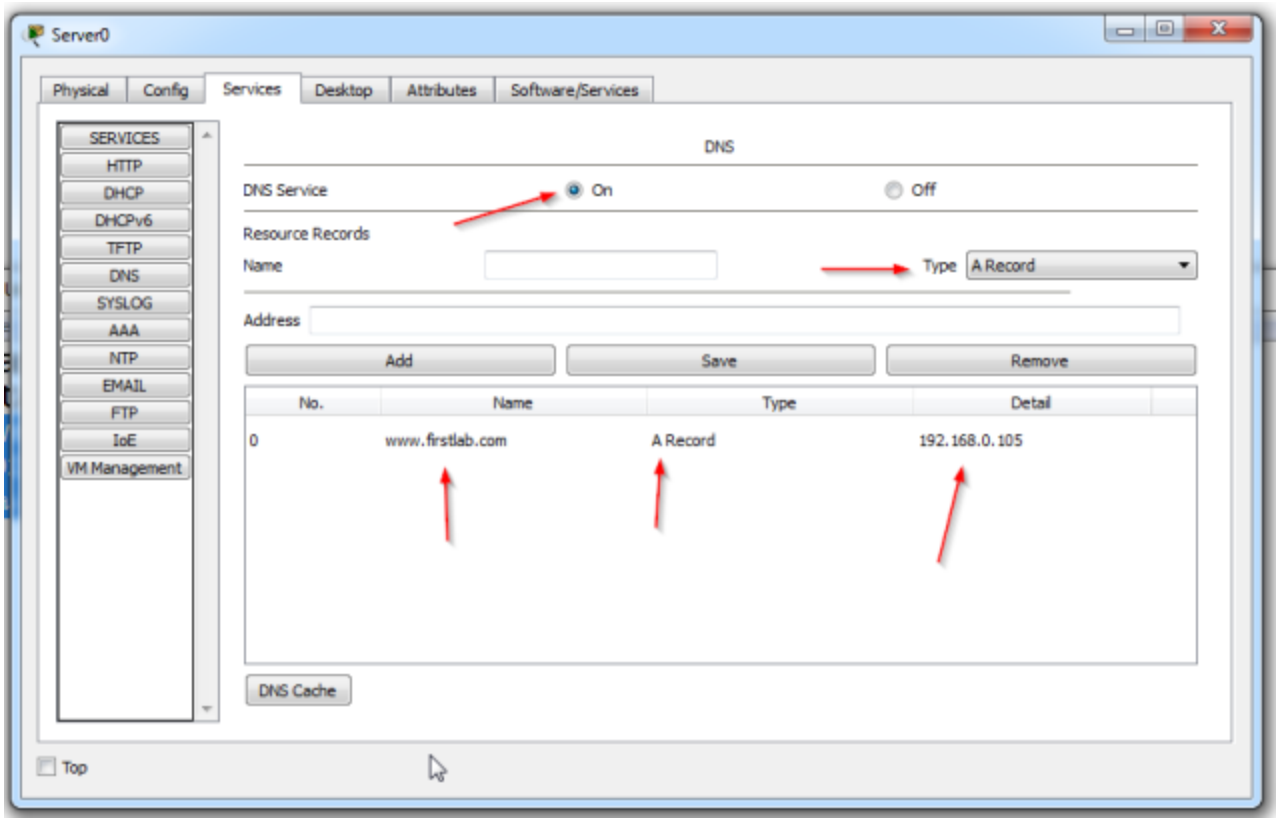
ขั้นตอนต่อไป ให้แก้ไขคอพฟิกเครื่อง Server โดยการดับเบิ้ลคลิกที่ Server >> Config



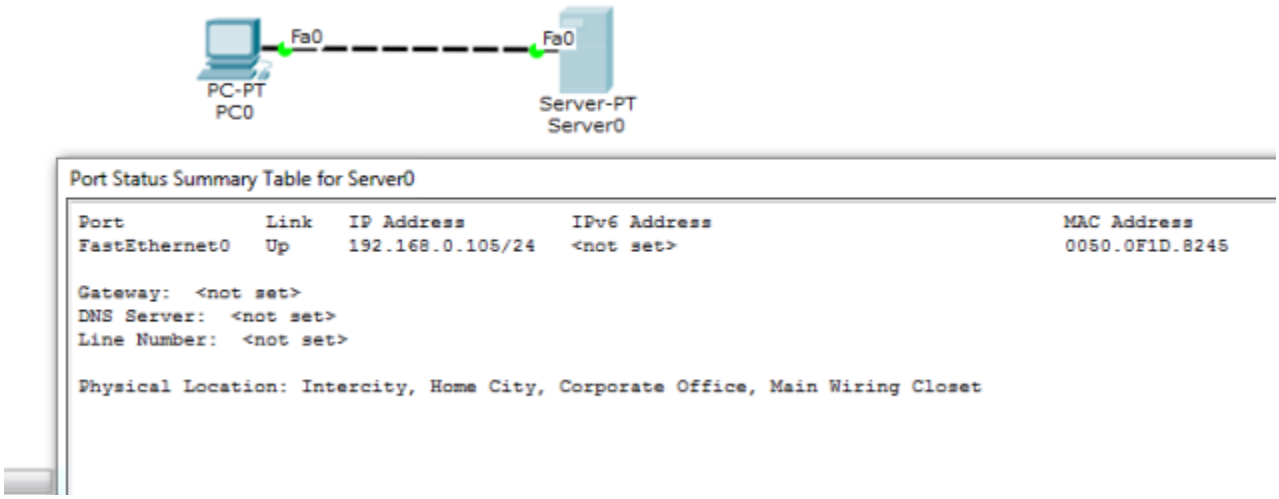
FastEthernet กำหนด IP Address เป็น 192.168.0.105 ตรวจสอบ Port Status เป็น On



จากนั้นไปที่แท็บ Services เลือก DNS แท็บ กำหนดในช่อง Name เป็น ***http://www.firstlab.com*** type เป็น A Record และ ช่อง Address เป็น 192.168.0.105 คลิก Add สุดท้ายอย่าให้ตรวจสอบว่า DNS Service มีสถานะเป็น On หรือไม

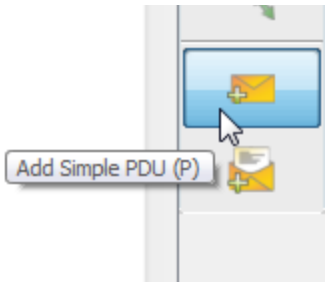


ตรวจสอบเครื่อง Server อีกครั้ง โดยใช้ Inspect



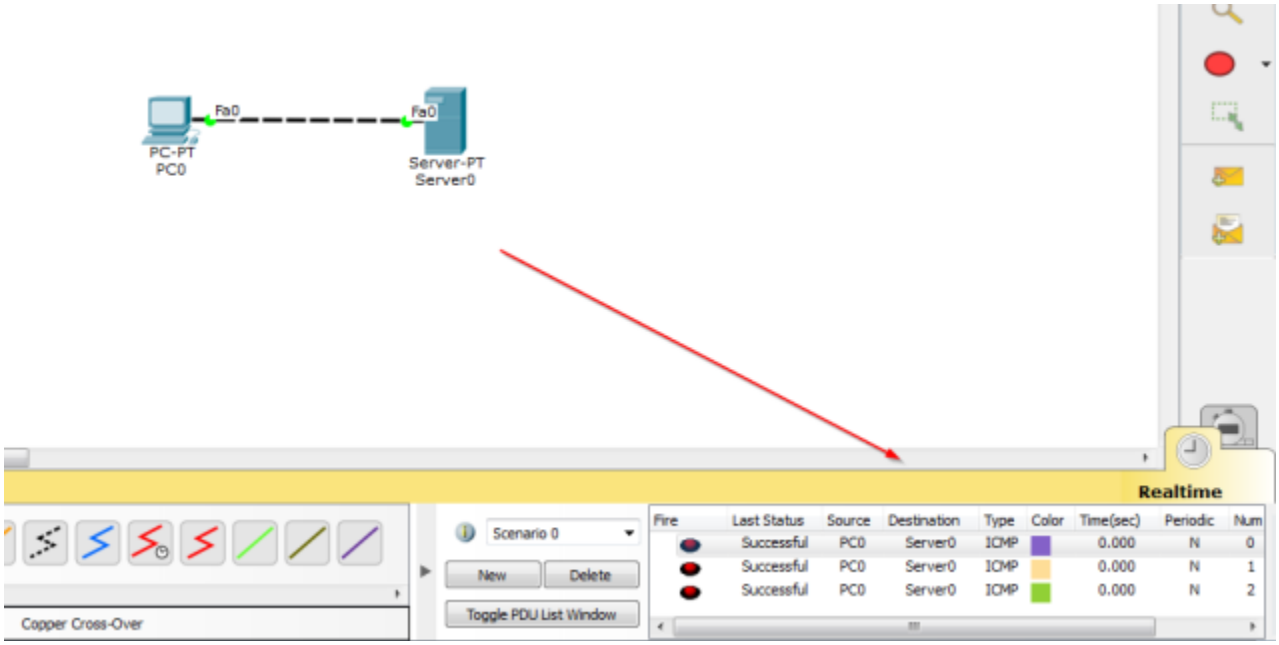
ทดลองสร้างข้อมูล (Add Simple PDU) เพื่อทดสอบการเชื่อมต่อในโหมด Realtime

คลิกเลือก Add Simple PDU

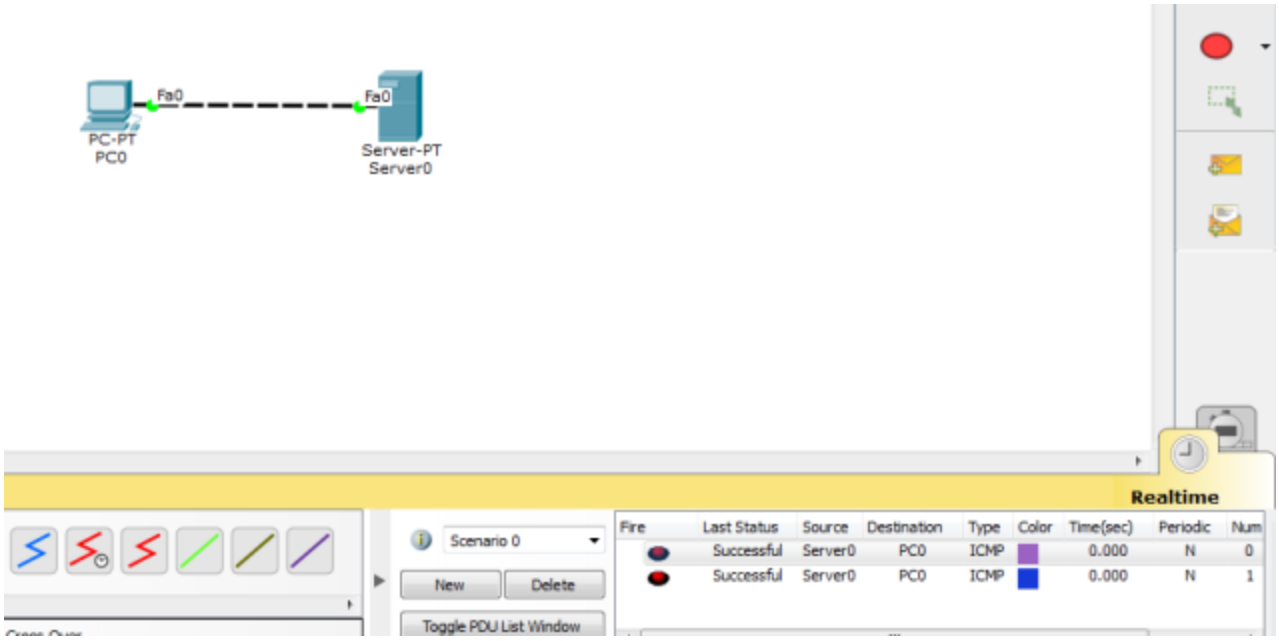


Add Simple PDU หมายถึงโพรโทคอลชนิดหนึ่งที่ใช้สำหรับทดสอบเครื่องปลายทางว่าทำงานอยู่หรือไม่ (เรียกว่า ping message หรือเรียกว่า echo request)

คลิกที่เครื่อง PC 1 ครั้ง และคลิกที่เครื่อง Server อีก 1 ครั้ง เมื่อ ping สำเร็จจะมี message ที่เรียกว่า echo reply ตอบกลับมาจาก Server ให้ดูผลลัพธ์การทำงานได้ในส่วน User Created Packet Window อยู่ด้านขวาล่าง



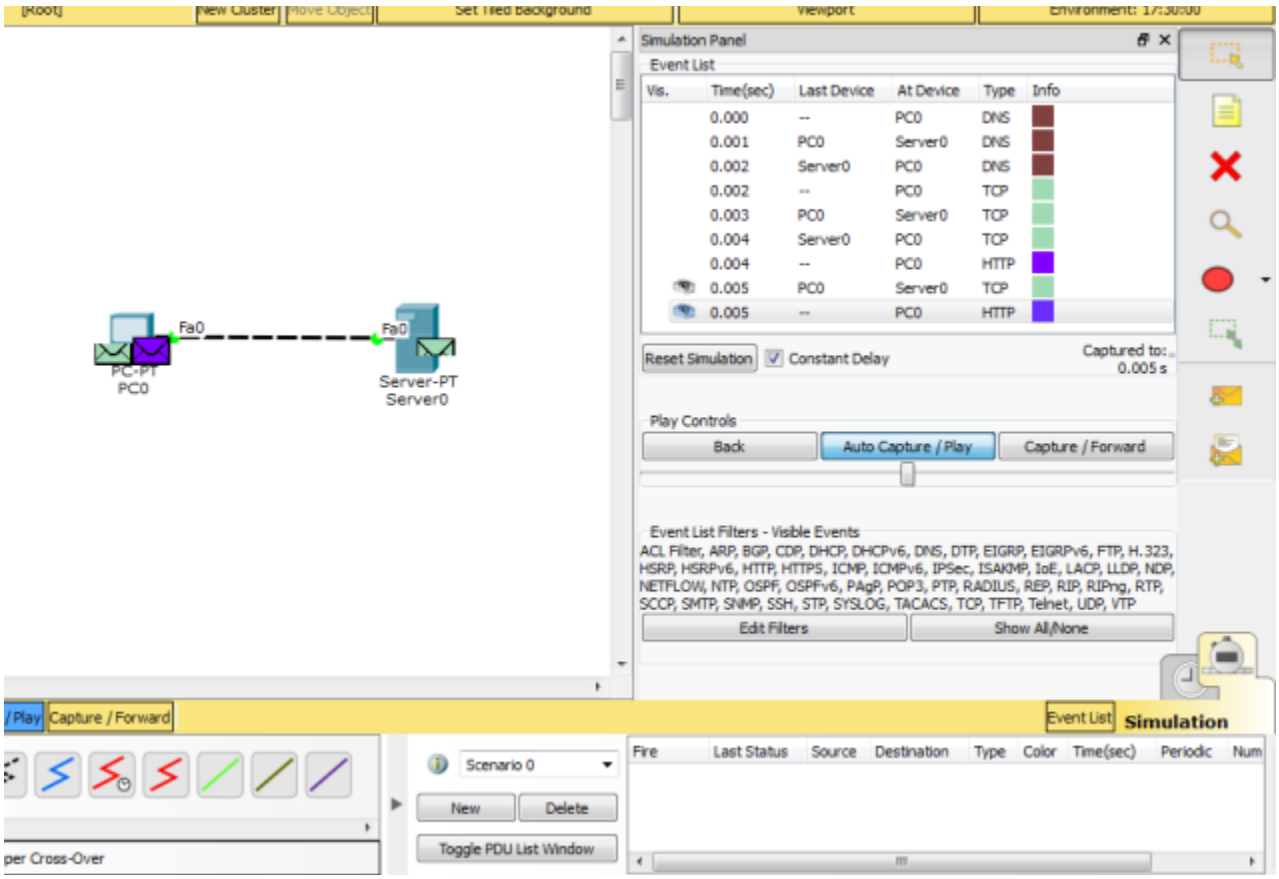
สำหรับข้อมูลที่ แสดงใน Scenario จะแสดง Last Status ว่า Successful แปลว่าการทำงานสำเร็จ (จากตัวอย่าง Source=Pacman, Destination=Web Server, Type=ICMP เป็นต้น) ลองทดสอบ ping กลับทิศทางอีกครั้งว่าเป็นอย่างไร เป็นอันสิ้นสุดการทดสอบด้วยการ ใช้ Simple PDU (ping request/reply)



ทดสอบการทำงานของเว็บเซิร์ฟเวอร์ โดยใช้โปรแกรม Browser ที่ฝั่งไคล์แอนท์ โดยคลิกที่เครื่อง PC เลือกแท็บ Desktop เลือก Web Browser ในช่อง URL ใส่ข้อมูลเป็น http://www.firstlab.com เสร็จแล้วกดปุ่ม go โปรแกรมจะแสดงข้อมูลใน Web Browser

ทดลองเปลี่ยนโหมดการทำงานเป็น Simulation ซึ่งในโหมดนี้ผู้ใช้สามารถควบคุมเวลาการทำงานได้ ส่งผลให้เวลาในการทำงานของโปรแกรมจะช้ากว่าปกติ และผู้ใช้ ก็สามารถสังเกตพฤติกรรมของข้อมูลได้ชัดเจน

โดย คลิก ที่ Desktop >> Web Browser >> ใส่ในช่อง URL เป็น http://www.firstlab.com กดปุ่ม go กลับไปยัง workspace แล้ว สังเกตุที่ Even List จะปรากฏ โพรโทคอล DNS อยู่และมีซองจดหมายปรากฏบนเครื่อง PC ด้วย ให้เลือก Auto Capture/Play เมื่อต้องการเฝ้าดูแพ็คเก็ตแบบต่อเนื่อง หรือเมื่อต้องการเฝ้ามองทีละ step ให้เลือก Capture/Forward



สังเกตุว่า ในการทดสอบครั้งนี้จะมีโพรโทคอลปรากฏใน Even List 2 ชนิดคือ DNS และ TCP (Web Server) เนื่องจากเครื่อง PC จะต้องสอบถามชื่อผ่าน Domain Name Server ก่อนเสมอ เพื่อแปลง URL (www.firstlab.com) เป็นหมายเลข IP Address จากนั้น PC จึงใช้หมายเลขไอพีดังกล่าวเข้าใช้บริการเว็บเซิร์ฟเวอร์ต่อไป

สมาชิกภายในกลุ่ม

นาย	พิชญุตม์	ห้วยห้อง	161404710050
นาย	ศุภวัฒน์	ศรีสุขใส	161404710056
นาย	เลิศชัย	ภิกขุวาโย	161404710059
นาย	วรรษพจน์	จาระวรรณ	161404710061
นาย	ทิวัตถ์	จันทรานุสรณ์	161404710040