

ใบงานปฏิบัติการที่ 1 สำรวจเครือข่ายด้วยคำสั่งพื้นฐานและ Wireshark

รายการ	รายละเอียด
รายวิชา	RBE2003 โครงข่ายคอมพิวเตอร์ (Computer Network)
สัปดาห์ที่	1
หัวข้อบรรยายที่เกี่ยวข้อง	องค์ประกอบของเครือข่าย ประเภทและโทโพโลยี แบบจำลอง OSI และ TCP/IP การห่อหุ้มข้อมูล
เวลาปฏิบัติการ	2 ชั่วโมง
ผู้สอน	อาจารย์ ดร.อภิรักษ์ อธิติภูมิ
ชื่อ-รหัสนักศึกษา	
กลุ่มที่	 วันที่ปฏิบัติการ / /

1. วัตถุประสงค์

เมื่อทำใบงานนี้เสร็จ นักเรียนจะสามารถ

1. อ่านค่าที่อยู่ IP, subnet mask, default gateway และที่อยู่ MAC ของเครื่องตนเองจากบรรทัดคำสั่งได้
2. ใช้คำสั่ง ping, tracert/traceroute, arp และ nslookup เพื่อตรวจสอบการเชื่อมต่อและอธิบายผลที่ได้
3. ติดตั้งและใช้ Wireshark ดักจับแพ็กเก็ต แล้วชี้ได้ว่าส่วนหัวของแต่ละชั้นในแบบจำลอง TCP/IP อยู่ตรงไหนของแพ็กเก็ต
4. วาดผังเครือข่ายห้องปฏิบัติการจากข้อมูลที่สำรวจได้ และเปิดใช้ Cisco Packet Tracer สร้างผังเดียวกันได้

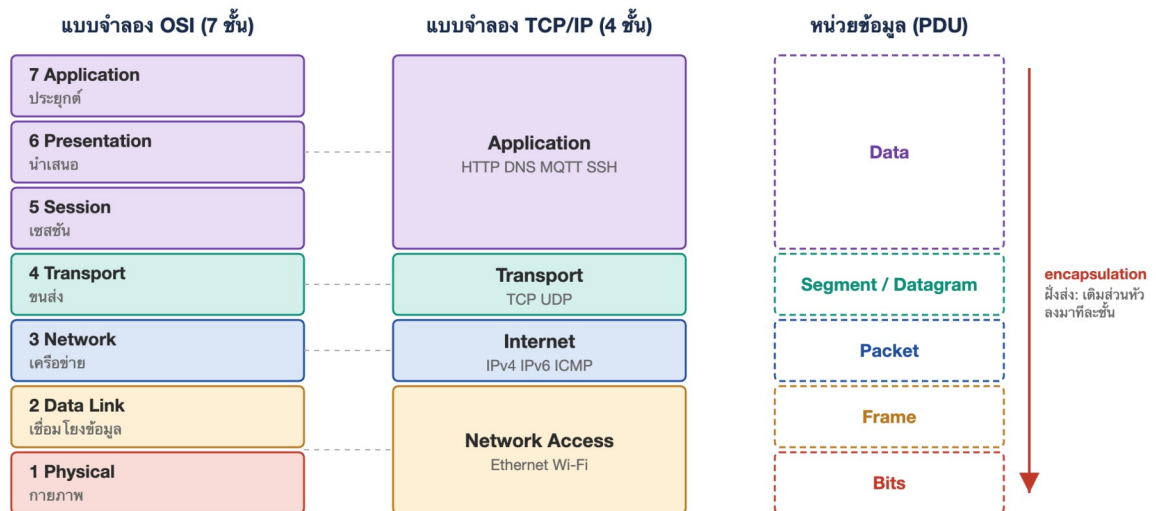
2. ความรู้พื้นฐานที่เกี่ยวข้อง

2.1 เครือข่ายคืออะไร และหุ่นยนต์เกี่ยวข้องอะไรด้วย

เครือข่ายคอมพิวเตอร์คือกลุ่มของอุปกรณ์ที่เชื่อมต่อกันเพื่อแลกเปลี่ยนข้อมูล องค์ประกอบพื้นฐานมี 4 อย่าง ได้แก่ **อุปกรณ์ปลายทาง** (end device เช่น คอมพิวเตอร์ ตัวควบคุมหุ่นยนต์ เซนเซอร์) **อุปกรณ์ตัวกลาง** (intermediary device เช่น สวิตช์ เราเตอร์ access point) **สื่อสัญญาณ** (สายทองแดง ไบแก้วนํ้าแสง คลื่นวิทยุ) และ **กฎการสื่อสาร** หรือโพรโทคอล ลองนึกภาพหุ่นยนต์เคลื่อนที่ในโรงงาน ตัวหุ่นยนต์ต้องส่งตำแหน่งของตนไปยังเซิร์ฟเวอร์ รับคำสั่งจากผู้ควบคุม และอาจต้องดึงแผนที่จากคลาวด์ ทั้งหมดนี้วิ่งผ่านเครือข่าย ถ้าเครือข่ายช้าหรือหลุด หุ่นยนต์ก็ “หุนหันพลันแล่น” ทันที นี่คือเหตุผลที่วิศวกรหุ่นยนต์ต้องเข้าใจเครือข่ายไม่น้อยกว่าวิศวกรเครือข่ายเอง

2.2 แบบจำลอง OSI และ TCP/IP

การออกแบบเครือข่ายใช้หลักการ “แบ่งชั้น” (layering) แต่ละชั้นทำหน้าที่เฉพาะและให้บริการชั้นที่อยู่เหนือมันโดยไม่ต้องรู้รายละเอียดชั้นล่าง แบบจำลอง OSI มี 7 ชั้น ส่วนแบบจำลอง TCP/IP ที่ใช้งานจริงบนอินเทอร์เน็ตมี 4 ชั้น ดังรูปที่ 1.1 สังเกตว่าชั้น 5–7 ของ OSI ถูกยุบรวมเป็นชั้นประยุกต์ (Application) ของ TCP/IP และชั้น 1–2 รวมเป็นชั้น Network Access



รูปที่ 1.1 เปรียบเทียบแบบจำลอง OSI 7 ชั้นกับ TCP/IP 4 ชั้น และชื่อหน่วยข้อมูล (PDU) ของแต่ละชั้น

เมื่อโปรแกรมส่งข้อมูล ข้อมูลจะไหลลงจากชั้นบนสู่ชั้นล่าง แต่ละชั้นจะ **เติมส่วนหัว (header)** ของตนเข้าไปข้างหน้า เรียกกระบวนการนี้ว่า **การห่อหุ้ม (encapsulation)** หน่วยข้อมูลของแต่ละชั้นจึงมีชื่อต่างกัน ได้แก่ data → segment (TCP) หรือ datagram (UDP) → packet (IP) → frame (Ethernet) → bits ฝั่งรับจะแกะส่วนหัวออกทีละชั้นในทางกลับกัน เรียกว่า de-encapsulation ในตอนที่ 3 ของใบงานนี้นักศึกษาจะได้เห็นส่วนหัวเหล่านี้ซ้อนกันจริง ๆ ใน Wireshark

2.3 ที่อยู่ 3 แบบที่ต้องแยกให้ได้

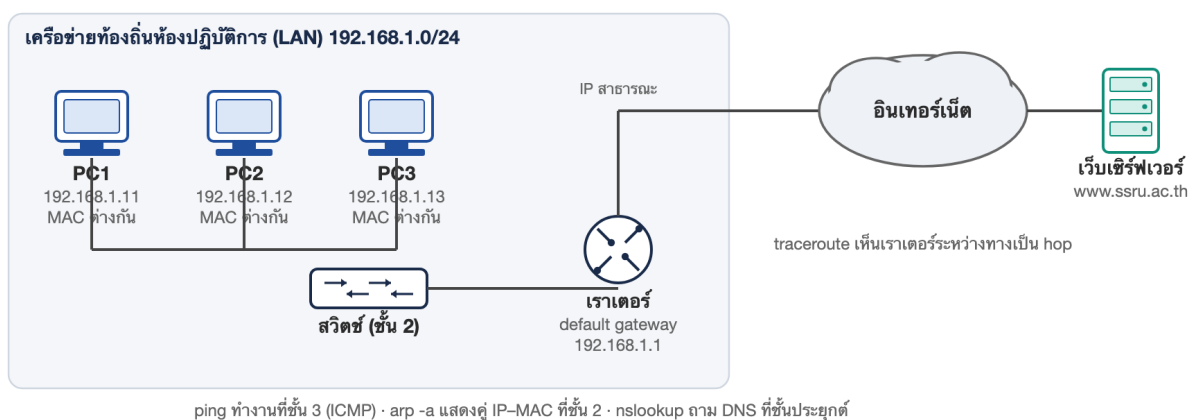
ที่อยู่	ชั้น	รูปแบบ	ตัวอย่าง	ใครกำหนด
ที่อยู่ MAC	2 (Data Link)	48 บิต เขียนเป็นเลขฐานสิบหก 6 คู่	3C:22:FB:1A:9E:07	ผู้ผลิตการ์ดเครือข่าย (3 คู่แรกคือ OUI ระบุผู้ผลิต)
ที่อยู่ IPv4	3 (Network)	32 บิต เขียนเป็นเลขฐานสิบ 4 กลุ่ม	192.168.1.25	ผู้ดูแลเครือข่ายหรือ DHCP
หมายเลข	4	16 บิต (0–65535)	80 (HTTP), 443	ระบบปฏิบัติการ/โปรแกรม

ที่อยู่	ชั้น	รูปแบบ	ตัวอย่าง	ใครกำหนด
เลข พอร์ต	(Trans port)		(HTTPS), 1883 (MQTT)	

ที่อยู่ MAC เปรียบเหมือนเลขบัตรประชาชนของการ์ดเครือข่าย ตีตามแต่กำเนิดและใช้ส่งข้อมูลภายในเครือข่ายท้องถิ่นเดียวกัน ส่วนที่อยู่ IP เปรียบเหมือนที่อยู่บ้าน เปลี่ยนได้เมื่อย้ายเครือข่าย และใช้ส่งข้อมูลข้ามเครือข่ายผ่านเราเตอร์ **Default gateway** คือที่อยู่ IP ของเราเตอร์ที่เครื่องเราจะส่งแพ็กเก็ตไปให้ทุกครั้งที่ปลายทางอยู่นอกเครือข่ายตนเอง

2.4 คำสั่งสำรวจเครือข่ายที่ต้องใช้วันนี้

งาน	Windows	macOS / Linux	สิ่งที่บอกเรา
ดูค่า IP ของเครื่อง	ipconfig /all	ifconfig หรือ ip addr	IP, mask, gateway, MAC, DNS server
ทดสอบไปถึงปลายทางไหม	ping <host>	ping -c 4 <host>	เวลาไป-กลับ (RTT) และอัตราการสูญหาย
ดูเส้นทางที่แพ็กเก็ตผ่าน	tracert <host>	traceroute <host>	เราเตอร์แต่ละตัว (hop) ระหว่างทาง
ดูตารางจับคู่ IP-MAC	arp -a	arp -a หรือ ip neigh	เพื่อนบ้านในเครือข่ายเดียวกันที่เคยติดต่อ
แปลงชื่อเป็น IP	nslookup <ชื่อ>	nslookup <ชื่อ> หรือ dig <ชื่อ>	DNS server ตอบ IP อะไร
ดูการเชื่อมต่อที่เปิดอยู่	netstat -an	netstat -an หรือ ss -tuna	พอร์ตและสถานะ TCP/UDP



รูปที่ 1.2 ผังเครือข่ายห้องปฏิบัติการแบบทั่วไปที่นักศึกษาจะสำรวจในใบงานนี้

3. เครื่องมือและอุปกรณ์ (ต่อกลุ่ม 2 คน)

รายการ	จำนวน	หมายเหตุ
คอมพิวเตอร์ที่เชื่อมต่อเครือข่ายห้องปฏิบัติการ	1 เครื่อง	Windows 10/11, macOS หรือ Linux
Wireshark รุ่นล่าสุด	1 ชุด	ดาวน์โหลดจาก https://www.wireshark.org (ติดตั้ง Npcap ด้วยบน Windows)
Cisco Packet Tracer 8.x	1 ชุด	สมัคร Cisco Networking Academy ฟรีเพื่อดาวน์โหลด
สิทธิ์ผู้ดูแลระบบบนเครื่อง	-	จำเป็นสำหรับการดักจับแพ็กเก็ต

4. ข้อควรระวัง

- ดักจับแพ็กเก็ตเฉพาะบนเครื่องของตนเองและเครือข่ายห้องปฏิบัติการที่ผู้สอนอนุญาตเท่านั้น การดักจับข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาตผิดกฎหมายตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- ห้าม ping หรือ traceroute ไปยังเซิร์ฟเวอร์ภายนอกด้วยความถี่สูงหรือใช้ตัวเลือก flood
- ไฟล์ .pcapng ที่บันทึกไว้อาจมีข้อมูลส่วนตัว (คุกกี้ รหัสผ่านที่ไม่เข้ารหัส) ห้ามนำไปเผยแพร่

5. ขั้นตอนการปฏิบัติ

ตอนที่ 1 อ่านค่าเครือข่ายของเครื่องตนเอง (20 นาที)

1. เปิด Command Prompt (Windows) หรือ Terminal (macOS/Linux)
2. พิมพ์คำสั่งดูค่า IP ตามตารางในหัวข้อ 2.4 หากการ์ดเครือข่ายที่ใช้งานอยู่ (สถานะ connected และมีค่า IP) แล้วบันทึกลงตารางที่ 1.1
3. เปรียบเทียบค่าที่ได้กับเพื่อนกลุ่มข้างเคียง 2 กลุ่ม แล้วบันทึกลงตารางที่ 1.1 เช่นกัน

ตารางที่ 1.1 ค่าเครือข่ายของเครื่องในห้องปฏิบัติการ

รายการ	เครื่องของกลุ่มเรา	กลุ่มข้างเคียง 1	กลุ่มข้างเคียง 2
ชื่อการ์ดเครือข่าย (Ethernet/Wi-Fi)			
ที่อยู่ MAC			
ผู้ผลิตการ์ด (ค้น OUI 3 คู่แรกจาก https://maclookup.app)			
ที่อยู่ IPv4			

รายการ	เครื่องของกลุ่ม เรา	กลุ่มข้างเคียง 1	กลุ่มข้างเคียง 2
Subnet mask			
Default gateway			
DNS server			
ได้ IP มาจาก DHCP หรือตัวเอง			

4. สังเกตว่าส่วนใดของที่อยู่ IP ที่เหมือนกันทั้ง 3 เครื่อง และส่วนใดที่ต่างกัน ส่วนที่เหมือนกันคือ **หมายเลขเครือข่าย** ส่วนที่ต่างกันคือ **หมายเลขโฮสต์** เขียนคำตอบ

หมายเลขเครือข่ายของห้องปฏิบัติการคือ จำนวนบิตของส่วนเครือข่าย (นับจาก mask) คือ

ตอนที่ 2 ทดสอบการเชื่อมต่อด้วย ping, tracert และ nslookup (30 นาที)

1. ping ไปยัง 4 ปลายทางต่อไปนี้ ปลายทางละ 4 ครั้ง แล้วบันทึกผลลงตารางที่ 1.2 ได้แก่ (ก) 127.0.0.1 (loopback ของเครื่องเอง) (ข) default gateway (ค) เครื่องของกลุ่มข้างเคียง (ง) www.ssru.ac.th

ตารางที่ 1.2 ผลการ ping

ปลายทาง	ที่อยู่ IP ที่ตอบ กลับ	ส่งไป/ได้รับ (แพ็ก เก็ต)	RTT ต่ำสุด (ms)	RTT เฉลี่ย (ms)	RTT สูงสุด (ms)	TTL
127.0.0.1						
default gateway						
กลุ่มข้าง เคียง						
www.ssru. ac.th						

2. ใช้ tracert (หรือ traceroute) ไปยัง www.google.com บันทึกจำนวน hop ทั้งหมด ที่อยู่ IP ของ hop ที่ 1 และ hop สุดท้าย และสังเกตว่า hop ใดตอบกลับด้วยเครื่องหมาย * (หมดเวลารอ)
จำนวน hop ทั้งหมด hop ที่ 1 คือ (ควรตรงกับ default gateway หรือไม่
.....) hop ที่ไม่ตอบ (ถ้ามี) คือ hop ที่
3. ใช้ nslookup แปลงชื่อ 3 ชื่อต่อไปนี้ แล้วบันทึกผลลงตารางที่ 1.3 ได้แก่ www.ssru.ac.th, www.ros.org และ mqtt.eclipseprojects.io

ตารางที่ 1.3 ผลการค้นชื่อด้วย DNS

ชื่อโดเมน	DNS server ที่ตอบ	ที่อยู่ IPv4 ที่ได้	มีที่อยู่ IPv6 ด้วยหรือไม่	จำนวน IP ที่ตอบกลับ
www.ssru.ac.th				
www.ros.org				
mqtt.eclipseproject s.io				

4. พิมพ์ **arp -a** แล้วนับจำนวนรายการในตาราง ARP ค้นหาว่ามีที่อยู่ MAC ของ default gateway และของเครื่องกลุ่มข้างเคียงที่เพิ่ง ping ไปหรือไม่

จำนวนรายการ ARP MAC ของ default gateway คือ ตรงกับที่เพื่อนกลุ่มอื่นเห็นหรือไม่

ตอนที่ 3 ดักจับแพ็กเก็ตด้วย Wireshark และหาส่วนหัวของแต่ละชั้น (40 นาที)

1. เปิด Wireshark เลือกการ์ดเครือข่ายที่ใช้งานอยู่ (การ์ดที่มีกราฟเส้นขยับ) แล้วกดปุ่มครีบลามสีน้ำเงินเพื่อเริ่มดักจับ
2. ระหว่างดักจับ ให้กลับไปที่บรรทัดคำสั่งแล้วสั่ง **ping -n 4 <default gateway>** (Windows) หรือ **ping -c 4 <default gateway>** (macOS/Linux) จากนั้นเปิดเว็บเบราว์เซอร์ไปที่ <http://neverssl.com> (เว็บที่ตั้งใจไม่เข้ารหัสเพื่อการศึกษา)
3. หยุดดักจับ (ปุ่มสี่เหลี่ยมสีแดง) แล้วพิมพ์ **icmp** ในช่อง display filter กด Enter จะเห็นเฉพาะแพ็กเก็ต ping
4. คลิกแพ็กเก็ต Echo (ping) request แพ็กเก็ตแรก ในบานหน้าต่างกลาง (packet details) จะเห็นบรรทัดที่อยู่อยู่ 4-5 บรรทัด แต่ละบรรทัดคือส่วนหัวของหนึ่งชั้น ให้ทางออกที่ละบรรทัดแล้วบันทึกตารางที่ 1.4

ตารางที่ 1.4 ส่วนหัวของแต่ละชั้นในแพ็กเก็ต ICMP Echo Request

บรรทัดใน Wireshark	ชั้นในแบบจำลอง TCP/IP	ชั้นใน OSI	ค่าที่อยู่ต้นทางที่เห็น	ค่าที่อยู่ปลายทางที่เห็น	ขนาด (ไบต์)
Frame	(ชั้นกายภาพ ข้อมูลที่ Wireshark เพิ่มเอง)	1	-	-	
Ethernet II					14
Internet Protocol Version 4					
Internet Control Message Protocol			-	-	

5. เปลี่ยน display filter เป็น **http** คลิกแพ็กเก็ต GET แพ็กเก็ตแรก ครั้งนี้จะเห็นบรรทัดเพิ่มขึ้นมาอีก 1 บรรทัดระหว่าง IPv4 กับ HTTP บันทึกชื่อบรรทัดนั้นและหมายเลขพอร์ตต้นทาง/ปลายทาง บรรทัดที่เพิ่มขึ้นคือ พอร์ตต้นทาง พอร์ตปลายทาง เหตุใดแพ็กเก็ต ping จึงไม่มีบรรทัดนี้
6. คลิกขวาที่แพ็กเก็ต GET เลือก Follow → HTTP Stream อ่านข้อความที่เบราว์เซอร์ส่งไปและ เซิร์ฟเวอร์ตอบกลับ จับภาพหน้าจอเก็บไว้ส่ง
7. บันทึกไฟล์ดักจับเป็น **lab01_<รหัสนักศึกษา>.pcapng** (File → Save As)

ตอนที่ 4 วาดผังเครือข่ายและสร้างใน Packet Tracer (30 นาที)

1. จากข้อมูลตอนที่ 1-2 วาดผังเครือข่ายห้องปฏิบัติการลงในกรอบด้านล่างด้วยมือ ให้มีอย่างน้อย เครื่องของกลุ่มเรา เครื่องกลุ่มข้างเคียง 2 เครื่อง สวิตช์ เราเตอร์ (default gateway) และกลุ่มเมฆแทน อินเทอร์เน็ต กำกับที่อยู่ IP ทุกอุปกรณ์ที่ทราบ
2. เปิด Cisco Packet Tracer สร้างผังเดียวกันโดยใช้ End Devices → PC จำนวน 3 เครื่อง Network Devices → Switches → 2960 หนึ่งตัว Routers → 1941 หนึ่งตัว เชื่อมด้วยสาย Copper Straight-Through
3. คลิกที่ PC แต่ละเครื่อง → Desktop → IP Configuration ตั้งค่า IP, mask และ gateway ให้ตรงกับที่สำรวจได้จริง (ตัวเลข IP ของเราเตอร์ตั้งที่ Router → Config → GigabitEthernet0/0 และเปิด Port Status เป็น On)
4. ใช้ Desktop → Command Prompt ของ PC ตัวใดตัวหนึ่ง ping ไปยังอีก 2 เครื่องและ gateway ผลต้องเป็น Reply ทั้งหมด จับภาพหน้าจอ
5. บันทึกไฟล์เป็น **lab01_<รหัสนักศึกษา>.pkt**

6. บันทึกผลและวิเคราะห์

1. จากตารางที่ 1.2 ค่า RTT ไปยัง loopback, gateway และเว็บภายนอกต่างกันอย่างไร อธิบายว่าอะไร ทำให้เวลาต่างกัน
2. ค่า TTL ที่ได้จาก ping loopback กับจาก www.ssru.ac.th ต่างกันหรือไม่ ค่า TTL ลดลงเมื่อไร และ บอกอะไรเราได้เกี่ยวกับจำนวนเราเตอร์ระหว่างทาง
3. จากตารางที่ 1.4 เรียงลำดับส่วนหัวจากนอกสุดไปในสุดตามที่เห็นในแพ็กเก็ตจริง แล้วเทียบกับลำดับชั้น ในรูปที่ 1.1 ตรงกันหรือไม่
4. ขนาดของแพ็กเก็ต ping ทั้งเฟรม (ดูที่บรรทัด Frame) เป็นกี่ไบต์ ในจำนวนนั้นเป็นส่วนหัว Ethernet + IPv4 + ICMP รวมกี่ไบต์ และเป็นข้อมูล (payload) จริงกี่ไบต์

7. คำถามท้ายการทดลอง

1. เหตุใดเครื่อง 3 เครื่องในตารางที่ 1.1 จึงมี default gateway เดียวกัน แต่มีที่อยู่ MAC ไม่ซ้ำกันเลย

2. ถ้าถอดสาย LAN ออกแล้ว ping 127.0.0.1 จะยังได้ Reply หรือไม่ เพราะเหตุใด และการทดสอบนี้บอกอะไรเรา
3. ใน tracert บาง hop ตอบด้วย * แปลว่าเส้นทางขาดหรือไม่ อธิบาย
4. หุ่นยนต์เคลื่อนที่ตัวหนึ่งเชื่อม Wi-Fi ในโรงงานและต้องส่งตำแหน่งไปเซิร์ฟเวอร์ทุก 100 ms ค่า RTT ที่วัดได้จาก ping เกี่ยวข้องกับข้อกำหนดนี้อย่างไร และควรวัดอะไรเพิ่ม
5. Wireshark เห็นเนื้อหาของหน้าเว็บ neverssl.com ได้ทั้งหมด แต่ถ้าเปิด <https://www.ssru.ac.th> จะเห็นอะไร และเหตุใดจึงต่างกัน (ตอบจากความรู้เบื้องต้น จะเรียนละเอียดในสัปดาห์ที่ 14)

8. งานที่ต้องส่งและเกณฑ์การให้คะแนน

สิ่งที่ต้องส่งผ่านระบบ LMS ภายในสัปดาห์ถัดไป

1. ใบงานฉบับนี้ที่กรอกตารางที่ 1.1–1.4 และตอบคำถามครบทุกข้อ (สแกนหรือกรอกในไฟล์)
2. ภาพหน้าจอ Follow HTTP Stream และภาพหน้าจอผล ping ใน Packet Tracer
3. ไฟล์ lab01_<รหัสนักศึกษา>.pcapng และ lab01_<รหัสนักศึกษา>.pkt

เกณฑ์การให้คะแนน (10 คะแนน)

หัวข้อประเมิน	คะแนน	เกณฑ์ระดับดี
ความถูกต้องของผลการปฏิบัติ	4	ตารางที่ 1.1–1.4 กรอกครบและค่าสอดคล้องกับเครือข่ายจริง ผัง Packet Tracer ping ได้ทั้งหมด
การบันทึกผลและหลักฐาน	2	ภาพหน้าจอครบ ไฟล์ .pcapng และ .pkt เปิดได้
การวิเคราะห์และคำตอบคำถามท้ายการทดลอง	3	อธิบายเชื่อมโยง RTT/TTL/การท่อกับทฤษฎีได้ถูกต้อง
การส่งงานตรงเวลาและการทำงานเป็นทีม	1	ส่งภายในกำหนด สมาชิกทั้งสองคนมีส่วนร่วม

9. เอกสารอ้างอิง

1. Kurose, J.F. & Ross, K.W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson. Chapter 1.
2. Cisco Networking Academy. (2020). *Introduction to Networks Companion Guide* (CCNAv7). Cisco Press. Modules 1–3.
3. Sanders, C. (2017). *Practical Packet Analysis* (3rd ed.). No Starch Press. Chapters 1–4.
4. Wireshark Foundation. (2025). *Wireshark User's Guide*. https://www.wireshark.org/docs/wsug_html_chunked/

5. Cisco Systems. (2025). *Cisco Packet Tracer Resources*. <https://www.netacad.com/cisco-packet-tracer>