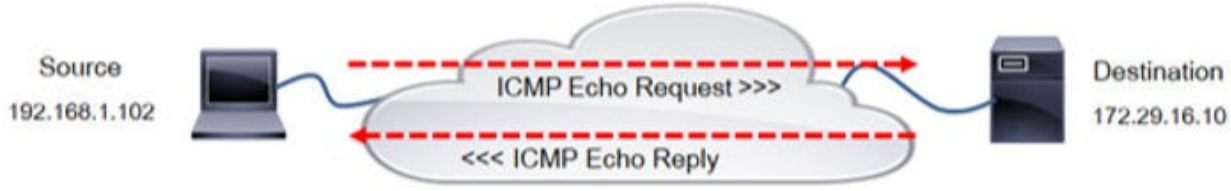
ICMP: Internet Control Message Protocol (Ping and Trace Route)



ICMP (Internet Control Message Protocol)

ICMP เป็นโปรโตคอลที่ใช้ในการรายงานข้อผิดพลาดต่างๆที่เกิดขึ้นในการทำงานของ Protocol TCP/IP และใช้แสดงข่าวสารเกี่ยวกับการเชื่อมต่อ รวมทั้งสามารถใช้เพื่อตรวจสอบและแก้ไขปัญหาในระบบเครือข่ายได้ เช่น การใช้คำสั่ง “ping” และ “trace route”

คำสั่ง Ping

เราใช้คำสั่ง ping เพื่อทดสอบการเชื่อมต่อจากเครื่อง Computer หรือ อาจจะเป็นอุปกรณ์ Network อื่นๆของเราไปยังอุปกรณ์ปลายทางกันอยู่บ่อยๆ เพื่อให้ทราบว่าปลายทางยังอยู่ปกติหรือไม่ เช่น ping ไปหา www.google.com เครื่อง Computer หรือ Router ของเราก็จะส่ง icmp echo request ซึ่งเป็น packet ที่มีขนาดเล็กๆไปยัง www.google.com หาก packet ไปถึงปลายทาง google ก็จะตอบ icmp echo reply กลับมาที่อุปกรณ์ของเรา เราก็จะทราบว่า www.google.com ยังอยู่มีการตอบสนองกลับมาหรือไม่

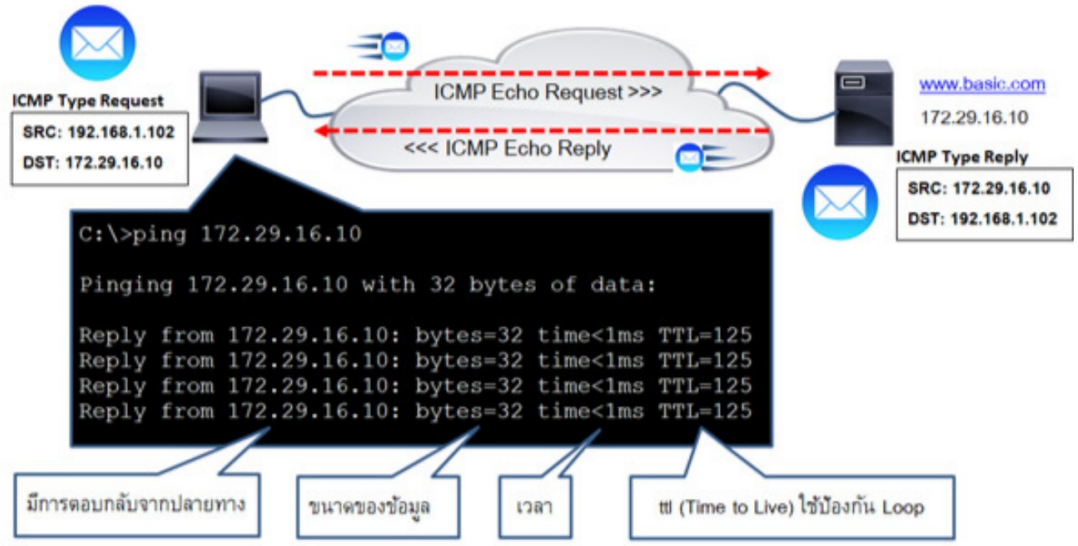
```
Frame 5: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src: c2:01:1a:18:00:00 (c2:01:1a:18:00:00), Dst: c2:02:09:58:00:00 (c2:02:09:58:00:00)
Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x6c78 [correct]
    Identifier (BE): 0 (0x0000)
    Identifier (LE): 0 (0x0000)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 6]
  Data (72 bytes)
      Data: 00000000000111d0abcdabcdabcdabcdabcdabcdabcdabcd...
      [Length: 72]
```

ตัวอย่างของ Message ICMP echo request

```
Frame 6: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src: c2:02:09:58:00:00 (c2:02:09:58:00:00), Dst: c2:01:1a:18:00:00 (c2:01:1a:18:00:00)
Internet Protocol Version 4, Src: 192.168.12.2 (192.168.12.2), Dst: 192.168.12.1 (192.168.12.1)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x7478 [correct]
    Identifier (BE): 0 (0x0000)
    Identifier (LE): 0 (0x0000)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 5]
    [Response time: 44,194 ms]
  Data (72 bytes)
      Data: 00000000000111d0abcdabcdabcdabcdabcdabcdabcdabcd...
      [Length: 72]
```

ตัวอย่างของ Message ICMP echo reply

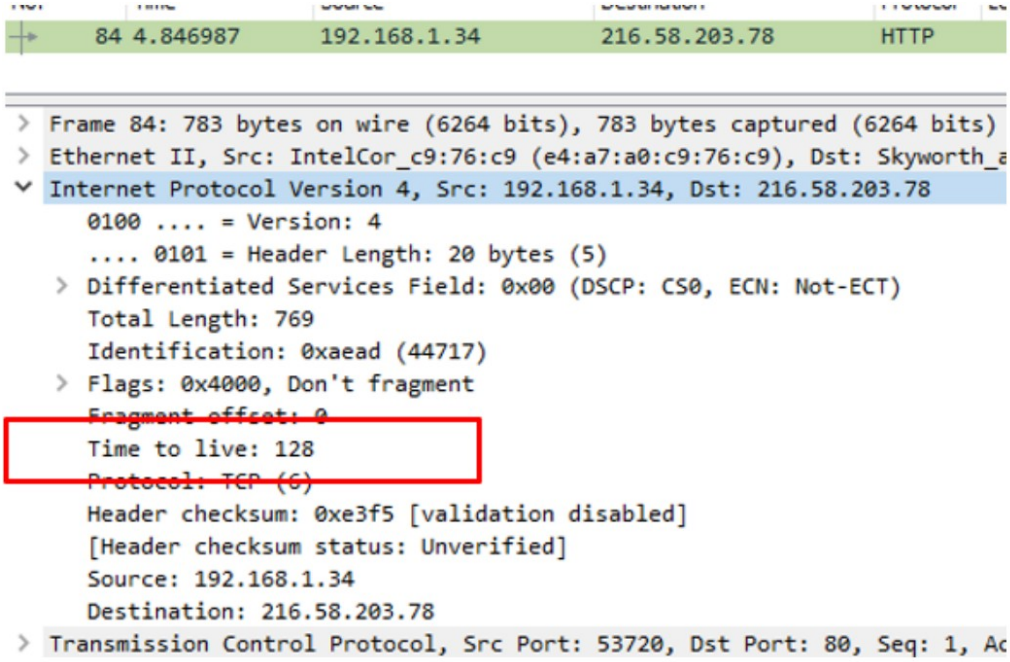
สำหรับระบบปฏิบัติการ Windows วิธีการ ping เราก็สามารถเปิด “Command Prompt” จาก Windows ของเรา แล้วก็เริ่มพิมพ์คำสั่ง ping เพื่อทดสอบกันได้เลย



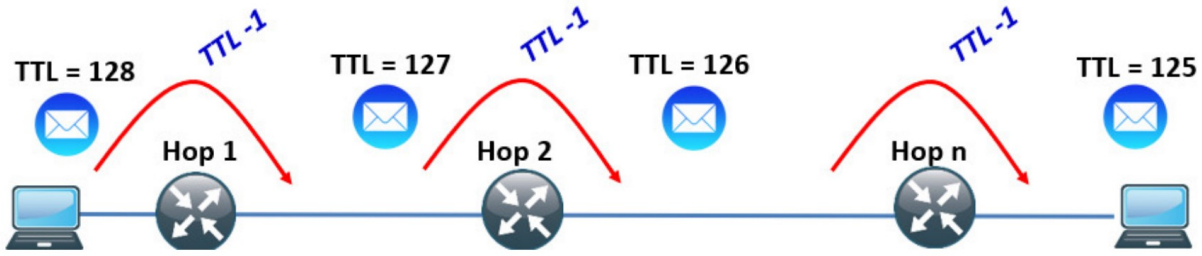
เมื่อทำการ ping แล้วมีการตอบกลับมาของข้อมูล เราจะเห็นได้ว่าตอบกลับมาจากปลายทาง IP Address อะไร ขนาดข้อมูลเท่าไหร่กี่ bytes เวลาในการไปและตอบกลับมาใช้เวลาไปเท่าไหร่ รวมถึงจะเห็นค่า TTL ด้วย

ค่า TTL คืออะไร

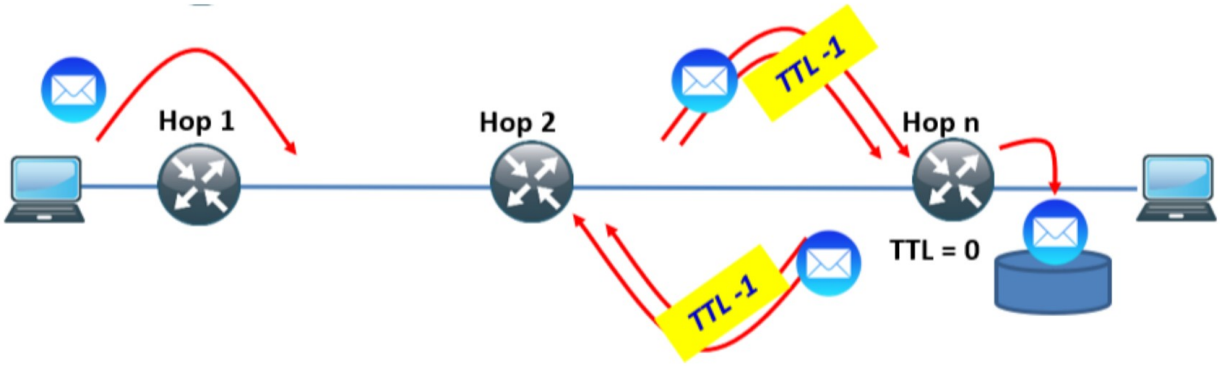
ค่า TTL หรือ Time to Live จะใช้ในการป้องกัน Loop ที่เกิดขึ้นในระดับ Layer 3 โดยถ้าหากทำการส่ง Packet จากต้นทางไปยังปลายทาง สำหรับในข้อมูลระดับ Layer 3 จะมีค่า TTL อยู่ ซึ่งถ้าหากใช้โปรแกรม Wireshark ดักจับข้อมูล ก็จะเห็นค่า TTL แสดงตามภาพ



ถ้าหาก Packet ผ่านอุปกรณ์ Layer 3 ออกไปค่า TTL จะลดลงที่ละ 1 จากภาพหากคอมพิวเตอร์ส่ง Packet ผ่าน Router จำนวน 3 ตัวค่า TTL ที่เริ่มจาก 128 (ค่าตั้งต้นของ Windows) จะลดลง 3 เมื่อ Packet ไปถึงยังปลายทางก็จะเหลือเท่ากับ 128-3= 125



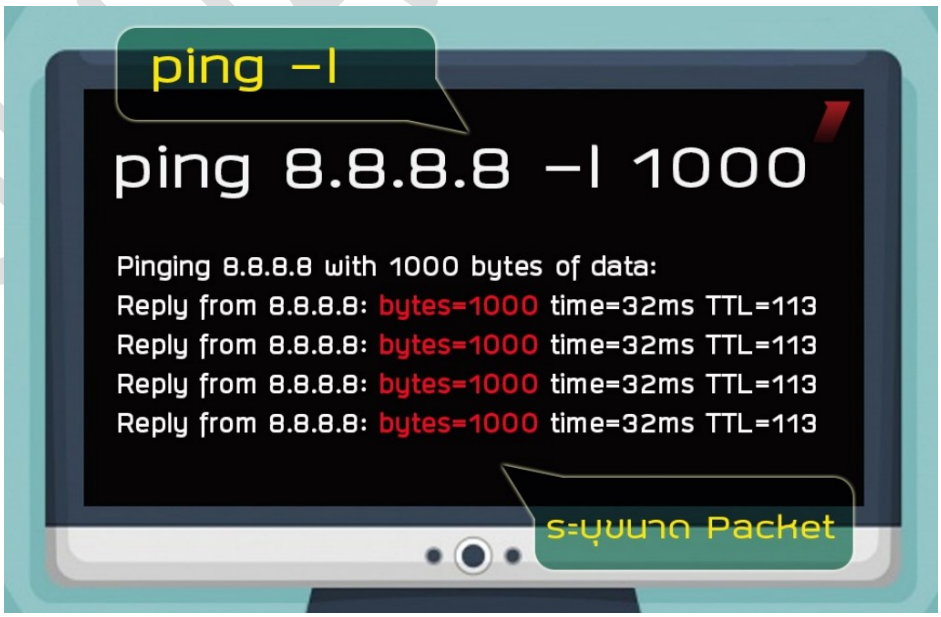
แต่ถ้าหาก Packet มีการวน loop เกิดขึ้น เมื่อ TTL ลดลงเหลือเท่ากับ 0 ก็ถือว่า packet นั้นจะ Expire หรือหมดอายุ จะถูก drop ทิ้ง แล้วอุปกรณ์จะส่งข้อความ ICMP message กลับไปบอกต้นทาง



ลักษณะการใช้คำสั่ง ping ก็จะพิมพ์ว่า ping แล้วตามด้วย ip หรือ url ปลายทางที่เราต้องการทดสอบ ยกตัวอย่าง ping 8.8.8.8 เป็นต้น และเรายังสามาร ping แบบใส่ Option เพิ่มเติมได้ ซึ่งจะขอยกตัวอย่างการใช้คำสั่ง ping บน Windows บาง Option เช่น

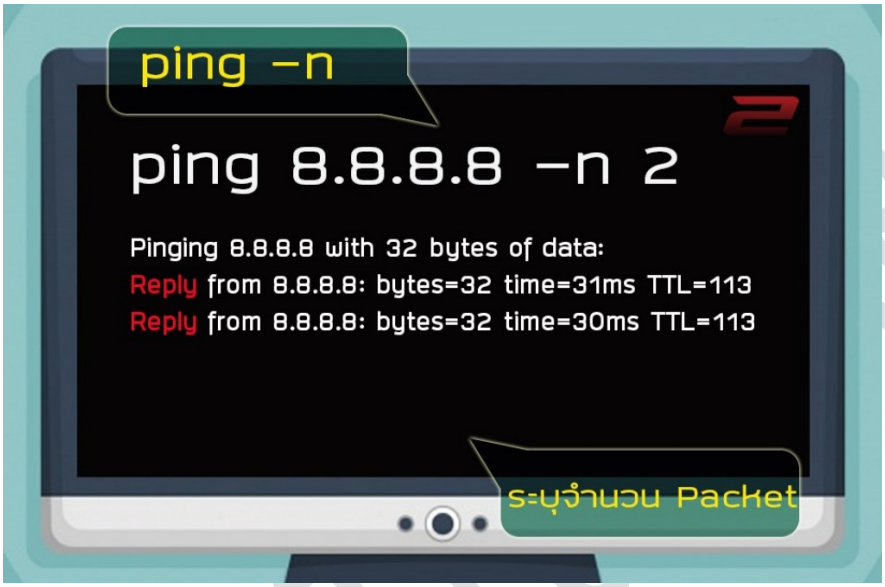
1. ping -l

เป็นการระบุขนาดของ Packet icmp ที่จะส่งออกไป ถ้าหากเราไม่ได้กำหนดก็จะมีขนาด 32 bytes ครับ เช่นหากเราต้องการจะ ping ไปหา dns ของ google(8.8.8.8) โดยมีขนาด size สัก 1000 bytes ก็ใช้คำสั่งนี้ได้



2. ping -n

การ ping จาก Computer ที่เป็น Windows ปกติจะมีการส่ง icmp echo request ไปหาปลายทาง 4 packets แต่ในบางครั้ง เช่น เราอยากส่งออกไปหา dns ของ google(8.8.8.8)แค่ 2 packets ก็สามารถกำหนดได้ดังนี้

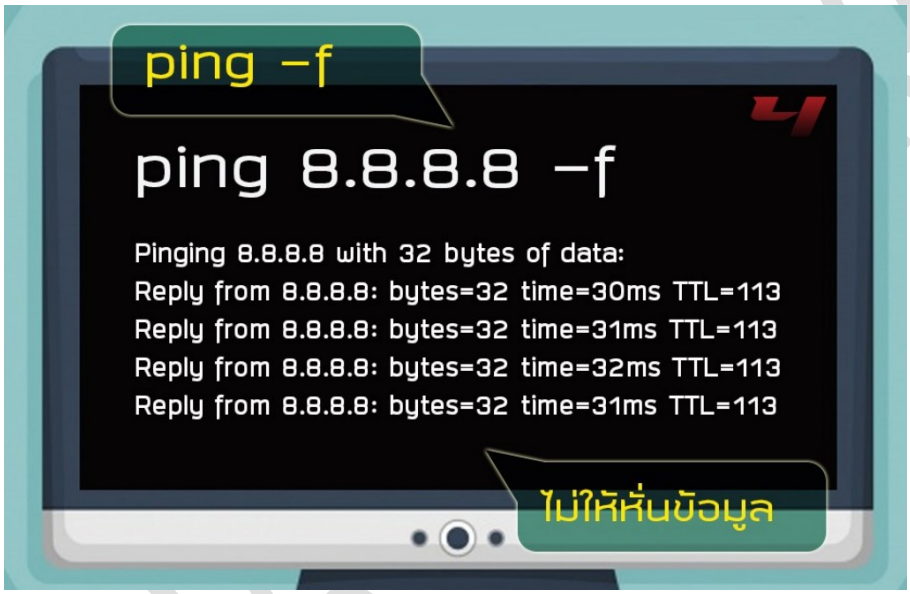


3. ping -t

การ ping จาก Computer ที่เป็น Windows ปกติจะมีการส่ง icmp echo request ไปหาปลายทางโดย Default 4 packets แต่ในบางครั้ง เช่น เราอยากส่งออกไปหา dns ของ google(8.8.8.8) ยาวๆไปเลย เพื่อดูว่ามีบาง packet หายไปบ้างหรือเปล่าในกรณีส่งเยอะๆก็สามารถกำหนดได้ดังนี้

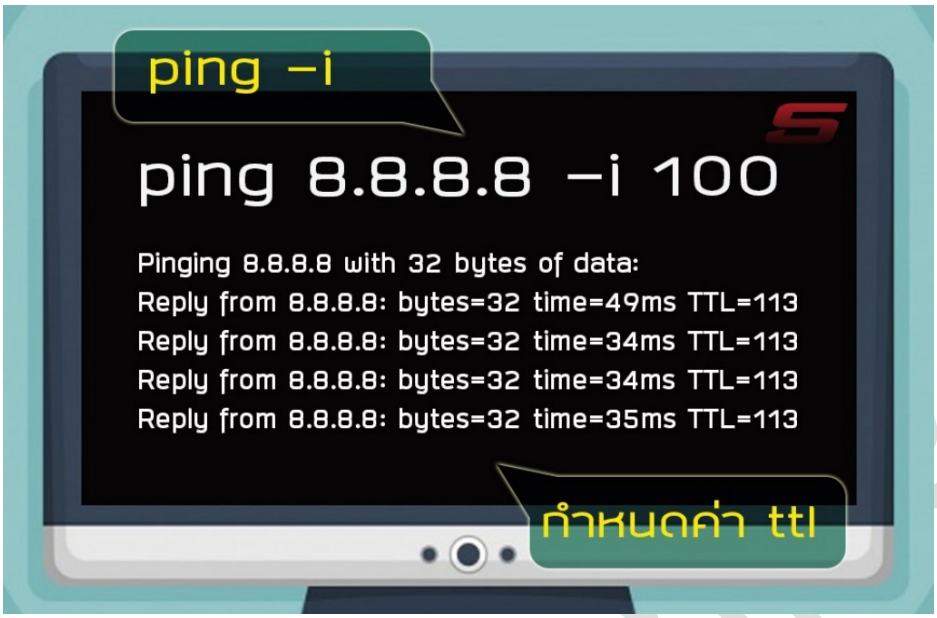
4. ping -f

ในการส่ง packet ออกไป หาก packet มีขนาดใหญ่เกินค่า MTU(maximum transmission unit) ของพวกอุปกรณ์ Router, Switch ที่อยู่ระหว่างทาง ตัว Packet ของเราก็จะโดนหั่น หรือที่เรียกว่าการทำ Fragment เพื่อให้ส่งต่อไปได้ยังปลายทาง หากเราต้องการบอกว่าอย่าหั่น Packet icmp ของฉันนะ!! (Don,t Fragment) เราก็สามารถใส่ Option "-f" ในการ ping ได้ เช่น เราต้องการส่ง icmp request ไปหา dns ของ google และห้ามทำ Fragment กับ Packet นี้(-f) ก็สามารถใช้คำสั่งนี้ได้



5. ping -i

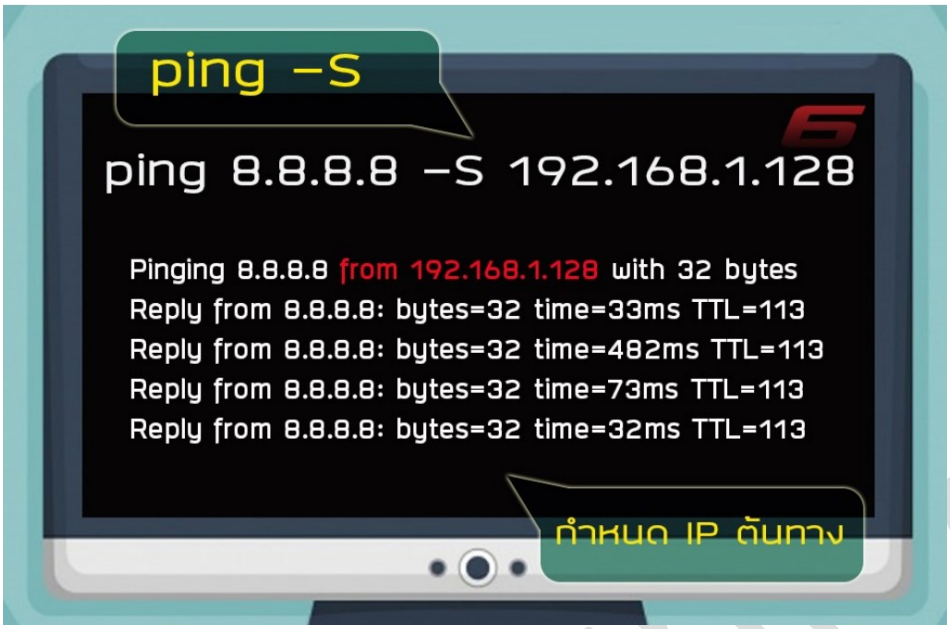
การ ping จะมีค่า TTL (Time To Live) ตั้งต้นอยู่แล้ว ขึ้นอยู่กับอุปกรณ์และ OS ของอุปกรณ์ที่เรา ping ค่า TTL จะบอกว่า Packet เราจะไปได้ไกลกี่ Hop ซึ่งมีเอาไว้สำหรับการป้องกัน Loop ที่จะเกิดขึ้น ถ้าหากเราต้องการกำหนดค่า TTL ตั้งต้นขึ้นมาเองไม่ต้องการใช้ค่า Default ก็สามารถทำได้ครับ เช่น เราต้องการส่ง icmp request ไปหา dns ของ google ให้มีค่า TTL = 100 (Default = 128) ก็สามารถใช้คำสั่งนี้ได้



6. ping -s

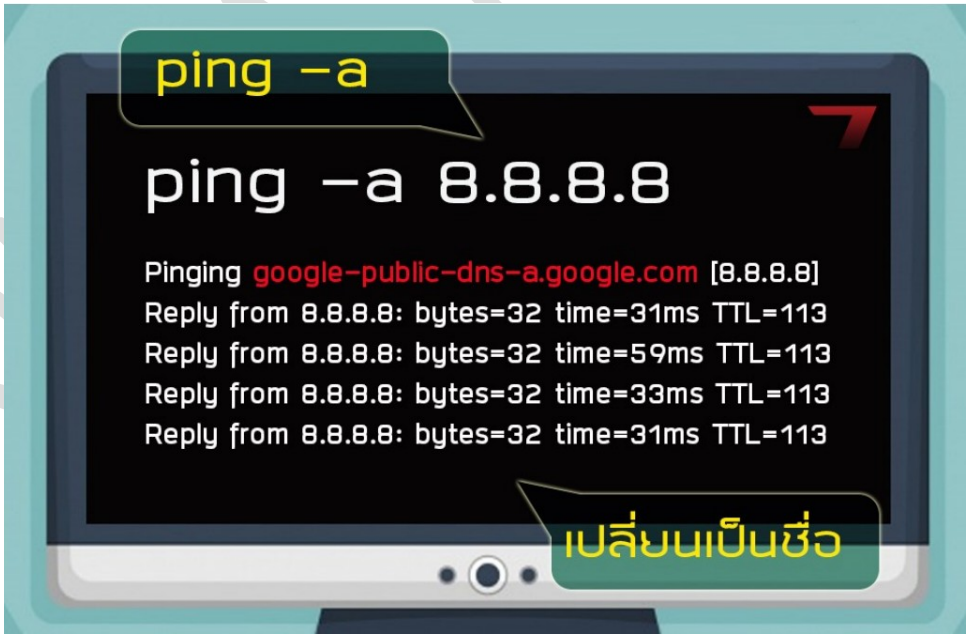
บางครั้งเครื่อง Computer ของเราอาจจะมีหลาย IP Address เช่น ตัวอย่าง card wireless = IP 10.10.10.100, card lan IP 192.168.1.128 ถ้าหากเราต้องการ ping ส่ง icmp request ออกไปจาก card lan ที่เป็น ip 192.168.1.128 ไปหา dns ของ google ก็สามารถใช้คำสั่งนี้ได้

หมายเหตุ: หากท่านไหนนึกภาพการ ping ใส่ source ไม่ออก ให้ลองนึกว่าการ ping ก็เหมือนการส่งจดหมายจากบ้านหลังที่ 1 ไปหาบ้านหลังที่ 2 บ้านหลังที่ 1 มีคนอยู่หลายๆคน มีพ่อ แม่ ลูก (ก็เหมือน Computer 1 เครื่องมีหลายๆ IP) หากบนซองจดหมายอยากให้เป็นชื่อลูกเป็นคนส่ง ก็เปลี่ยนชื่อผู้ส่งเป็นชื่อลูกแทน หรือ อยากให้แม่เป็นผู้ส่งจดหมายก็เปลี่ยนชื่อผู้ส่งเป็นชื่อแม่แทน ส่วนปลายทางผู้รับก็ยังคงเดิม อันนี้ก็เปรียบได้กับการ ping ใส่ source บน Computer ครับ เราสามาถเปลี่ยน source เป็นเบอร์ IP ไหนก็ได้ที่อยู่บน Computer เรานั่นเอง



7. ping -a

ในกรณีที่เราทราบหมายเลข IP address ของอุปกรณ์ปลายทาง แต่เราอยากรู้ชื่อของอุปกรณ์ปลายทาง ก็สามารถใช้ ping -a ช่วยได้ครับ ตัวอย่างเช่น เราอยากทราบว่า IP 8.8.8.8 มีชื่อว่าอะไร ก็สามารถใช้คำสั่ง ping ดังนี้

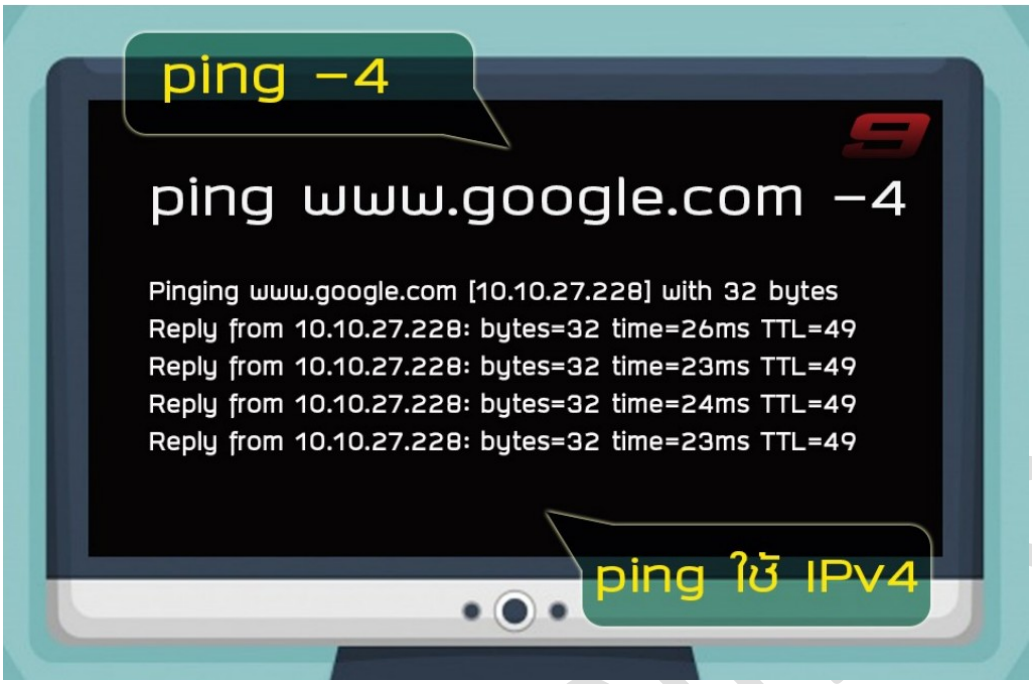


8. ping -r

หากเราต้องการทราบว่า packet icmp ที่เรา ping ไปผ่านเส้นทางที่เป็น IP Address อะไรบ้าง เราก็สามารถใช้ ping -r เข้ามาช่วยได้ครับ เช่นต้องการทราบเส้นทางไปยัง 10.10.10.1 และให้บันทึกเส้นทางมาสัก 4 IP ก็สามารถใช้คำสั่งนี้ได้

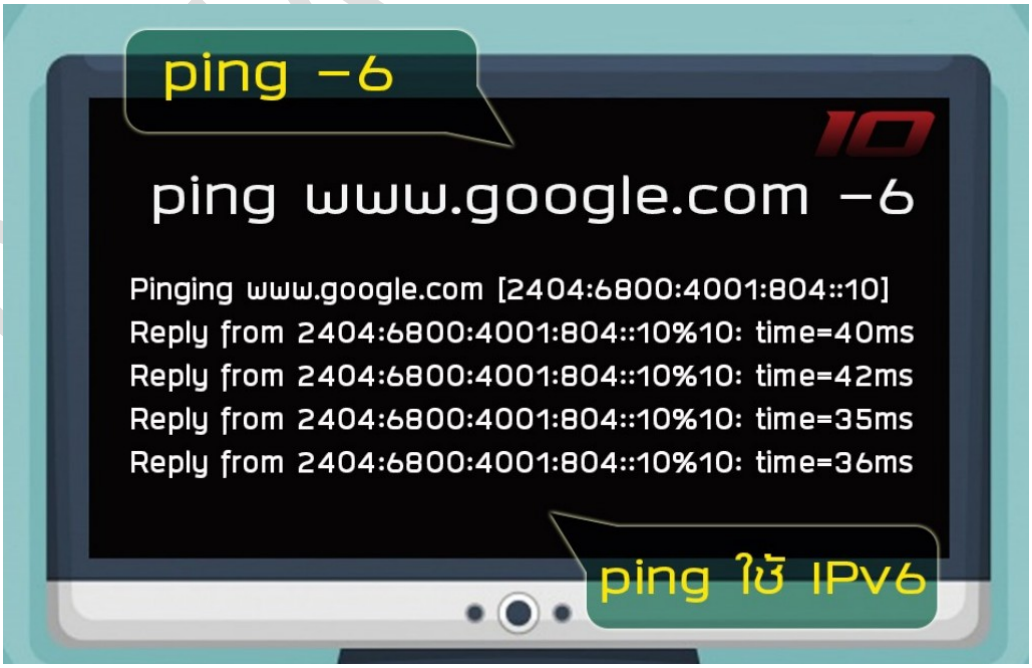
9. ping -4

ในกรณีเครื่อง Computer ของเรามีการตั้งค่าทั้ง IPv4 และ IPv6 อยู่ใน card lan และเราต้องการทดสอบการเชื่อมต่อด้วยการ ping ไปยัง www.google.com โดยบังคับใช้ IPv4 จากเครื่องเรา ก็สามารถใช้คำสั่งนี้ได้

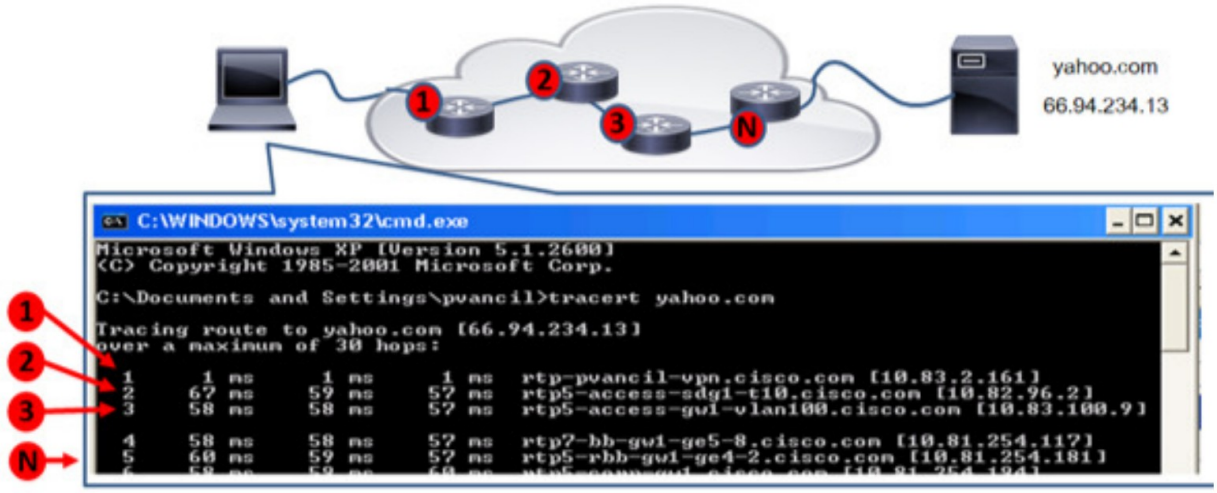


10. ping -6

ในกรณีเครื่อง Computer ของเรามีการตั้งค่าทั้ง IPv4 และ IPv6 อยู่ใน card lan และเราต้องการทดสอบการเชื่อมต่อด้วยการ ping ไปยัง www.google.com โดยบังคับใช้ IPv6 จากเครื่องเรา ก็สามารถใช้คำสั่งนี้ได้



คำสั่ง Tracert (Trace Route)



คำสั่ง Tracert (Trace Route) จะใช้ทดสอบการเชื่อมต่อแบบ end-to-end โดยมีการแสดงผลแต่ละจุดบน router หรืออุปกรณ์ Layer 3 ขึ้นมาในเส้นทางที่มีข้อมูลวิ่งผ่าน ซึ่งจะทำให้เราสามารถวิเคราะห์บริเวณจุดที่ระบบ Network มีปัญหาได้เบื้องต้น

ตัวอย่างการ trace route ไปยังปลายทาง yahoo.com เราก็จะเห็นเส้นทางว่าผ่านอุปกรณ์ layer3 อะไรบ้าง จุดที่ 1 จุดที่ 2-3 จนไปถึงจุดที่ N และถึงปลายทางในที่สุด หากข้อมูลที่แสดงไปถึงจุดที่ 3 แล้วไม่มีข้อมูล IP หรือ name อื่นๆแสดงแล้ว ก็จะทำให้เราทราบว่าปัญหาที่ติดต่อปลายทางไม่ได้ น่าจะอยู่ที่บริเวณจุดที่ 3 นั่นเอง