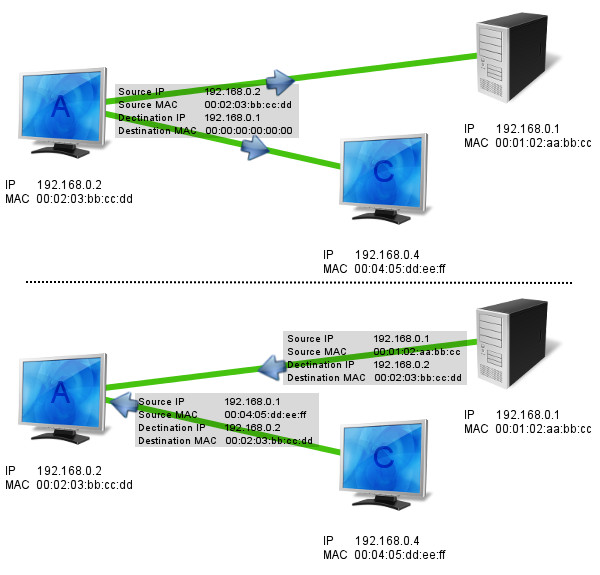
**การปลอมตัว (Spoofing)**

หมายถึง การทำให้อีกฝ่ายหนึ่งเข้าใจว่าเป็นตัวเองเป็นอีกบุคลหนึ่ง การโจมตีแบบนี้จัดอยู่ในประเภทหลอกลวงและควบคุมระบบ การสปูฟิงเป็นการหลอกให้คู่สนทนาเชื่อว่าตนกำลังสนทนากับฝ่ายหรือบุคคลที่ต้องการสนทนาจริงๆ ดังนั้นการรักษาความคงสภาพก็โดยการพิสูจน์ทราบตัวตน(Authentication) ซึ่งจะเป็นวิธีการป้องกันการโจมตีในลักษณะนี้ได้

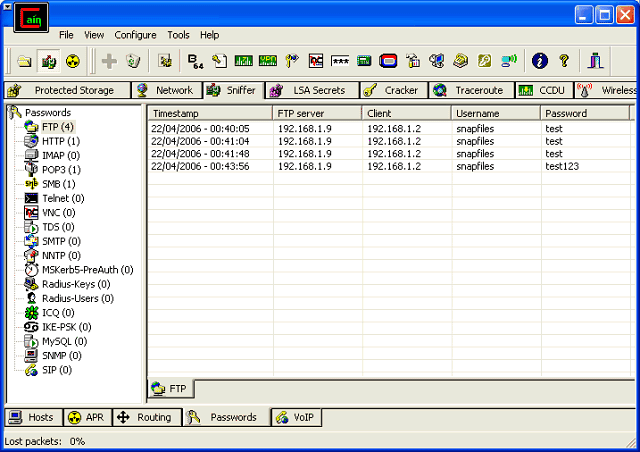
ไอพีสปูฟิง (IP Spoofing) หมายถึง การที่ผู้บุกรุกอยู่นอกเครือข่าย แล้วแสร้งทำเป็นว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้ โดยอาจใช้ไอพีแอดเดรสเหมือนกับที่ใช้ในเครือข่าย หรืออาจใช้ไอพีอแดเดรสข้างนอก ที่เครือข่ายเชื่อว่าเป็นคอมพิวเตอร์ที่เชื่อได้หรืออนุญาตให้เข้าใช้ทรัพยากรในเครือข่ายได้ การโจมตีแบบนี้โดยมากมักเป็นการเปลี่ยนแปลง หรือเพื่มข้อมูลเข้าไปในแพ็กเก็ตที่รับส่งระหว่างไคลเอนท์และเซิร์ฟเวอร์ หรือคอมพิวเตอร์ที่สื่อสารกันในเครือข่าย

**ARP Spoof**

เนื่องจากการทำงานของ ARP จะมีการส่ง ARP Request ออกไป แล้วรอให้มี ARP Reply ตอบกลับมา ถ้าหากว่าระหว่างที่กำลังรอคำตอบอยู่นั้นมีผู้ไม่หวังดีตอบ ARP Reply ปลอมๆ ส่งไปให้ ผู้ที่ได้รับก็จะไม่สามารถทราบได้ว่า ARP Reply นั้นไม่ได้มาจากตัวจริง และจะบันทึกข้อมูล MAC Address ที่ไม่ถูกต้องนั้นไว้ใน ARP Table การส่ง ARP Reply ปลอมออกไปนั้นเรียกว่า ARP Spoof หรือ ARP Cache Poison [[6]](https://www.thaicert.or.th/papers/general/2012/pa2012ge012.html#6) [[7]](https://www.thaicert.or.th/papers/general/2012/pa2012ge012.html#7)  
  
ตัวอย่างการทำ ARP Spoof เครื่องคอมพิวเตอร์ A ส่ง ARP Request ออกไปถามว่าเครื่องที่มี IP Address 192.168.0.1 มี MAC Address เป็นเท่าไหร่ แต่ถูกเครื่องคอมพิวเตอร์ C แย่งส่ง ARP Reply ตอบ MAC Address ของตัวเองมาให้ก่อนที่เครื่องตัวจริงจะตอบ ARP Reply กลับมาได้ทัน ดังนั้นเมื่อเครื่องคอมพิวเตอร์ A ได้รับ ARP Reply ดังกล่าวก็จะเข้าใจว่าเครื่องคอมพิวเตอร์ C เป็นเครื่องที่ต้องการติดต่อด้วยจริง ดังรูปที่ 5

  
รูปที่ 5 การทำ ARP Spoof

ตัวอย่างโปรแกรมที่สามารถทำ APR Spoof ได้ เช่น ARPspoof, , Ettercap, Dsniff เป็นต้น



ที่มารูปภาพ : http://www.securitylab.ru/upload/iblock/f52/f52dbf59554f73f90cd700db1d1e438a.gif

จุดประสงค์ของการทำ ARP Spoof มีได้หลากหลาย เช่น อาจจะทำ Man-in-the-Middle เพื่อดักรับข้อมูล หรือบล็อกไม่ให้เครื่องคอมพิวเตอร์ในระบบเครือข่ายเชื่อมต่อกับอินเทอร์เน็ตได้ โดยการส่ง ARP Reply บอก Gateway ปลอมออกไป เป็นต้น ซึ่งวิธีการดังกล่าวนี้ถูกใช้ในโปรแกรมชื่อ NetCut [[8]](https://www.thaicert.or.th/papers/general/2012/pa2012ge012.html#8)

**การตรวจสอบและป้องกัน ARP Spoof**

การทำ ARP Spoof จะทำได้ก็ต่อเมื่อเครื่องของผู้โจมตีและเครื่องของเหยื่ออยู่ในเครือข่ายเดียวกัน แต่การตรวจสอบ ARP Spoof ในระบบเครือข่ายนั้นทำได้ยาก เนื่องจากโพรโทคอล ARP ไม่ได้ถูกออกแบบมาเพื่อให้ตรวจสอบความถูกต้องของผู้รับและผู้ส่งตั้งแต่แรก อย่างไรก็ตาม ได้มีผู้พัฒนาเครื่องมือเพื่อช่วยวิเคราะห์ความผิดปกติในระบบเครือข่ายซึ่งอาจเกิดจาก ARP Spoof ได้ เช่น โปรแกรม [arpwatch](http://ee.lbl.gov/) หรือ [ArpON](http://arpon.sourceforge.net/) เป็นต้น ซึ่งทั้ง 2 โปรแกรมนี้เป็นซอฟต์แวร์ Open Source  
  
การป้องกันตัวเบื้องต้นจาก ARP Spoof สามารถทำได้โดยการทำ Static ARP ซึ่งเป็นการระบุค่า IP Address และ MAC Address ลงไปใน ARP Table ด้วยตนเอง [[9]](https://www.thaicert.or.th/papers/general/2012/pa2012ge012.html#9) ซึ่งสามารถทำได้โดยใช้คำสั่ง

*arp -s <IP ADDRESS> <MAC ADDRESS>*

เช่น เครื่องคอมพิวเตอร์ A สามารถเพิ่มเครื่องคอมพิวเตอร์ B ลงใน ARP Table ด้วยการใช้คำสั่งด้านล่าง

*arp -s 192.168.0.3 00:03:04:cc:dd:ee*

อย่างไรก็ตาม การทำ Static ARP อาจไม่สะดวกในการใช้งานกับระบบเครือข่ายขนาดใหญ่ เพราะหากมีเครื่องคอมพิวเตอร์อยู่ในระบบจำนวนมากก็ต้องเพิ่ม Static ARP ให้กับเครื่องเหล่านั้นในทุกครั้งที่เปิดเครื่อง รวมถึงผู้ที่ใช้งานอินเทอร์เน็ตสาธารณะหรือผู้ที่เชื่อมต่อผ่านบริการอินเทอร์เน็ตของที่พัก (ที่ไม่ใช่ Broadband ส่วนตัว) ก็อาจไม่สามารถทราบข้อมูล IP Address หรือ MAC Address ของเครื่องที่สำคัญในระบบเครือข่าย เช่น Gateway หรือ DNS Server ได้