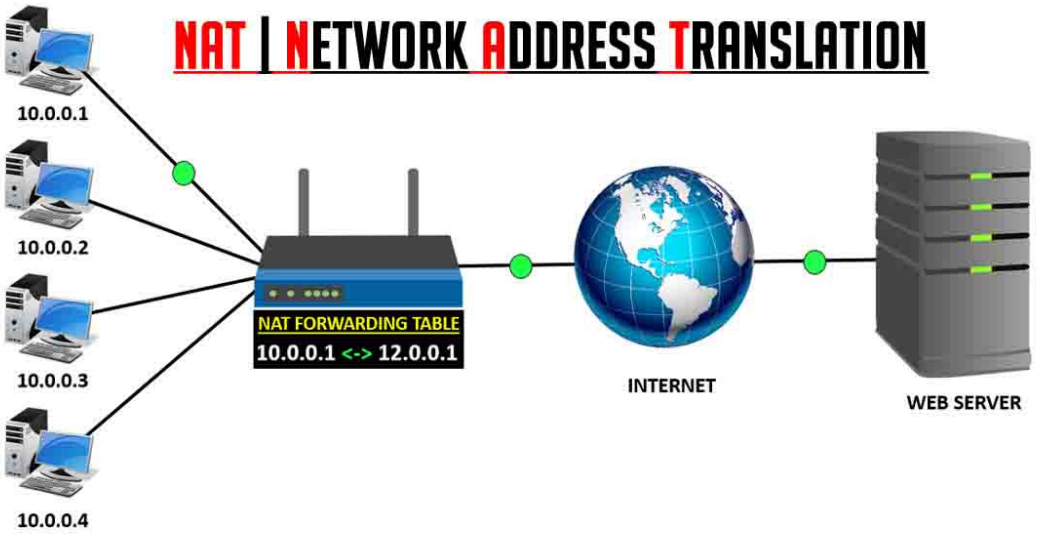
NAT

Network Address Translation

(NAT) Network Address Translation คือเทคโนโลยีที่ใช้แปลง IP Address ภายใน (Private IP) ของเครือข่ายส่วนตัวให้เป็น IP Address สาธารณะ (Public IP) เพื่อให้อุปกรณ์หลายเครื่องในเครือข่ายสามารถใช้ IP เดียวกันในการเชื่อมต่ออินเทอร์เน็ต ช่วยประหยัด IP และเพิ่มความปลอดภัย



หลักการทำงานของ NAT (Network Address Translation)

NAT (Network Address Translation) คือกระบวนการที่เราเตอร์หรืออุปกรณ์เครือข่ายใช้ในการปรับเปลี่ยนข้อมูลที่อยู่ IP ในส่วนหัวของแพ็กเก็ตข้อมูล เพื่อให้เครื่องคอมพิวเตอร์หลายเครื่องที่อยู่ในเครือข่ายส่วนตัว (private network) สามารถใช้ที่อยู่ IP สาธารณะ (public IP address) เดียวกันในการเชื่อมต่อกับอินเทอร์เน็ต ลองนึกภาพว่า NAT เป็นเหมือนพนักงานต้อนรับในออฟฟิศ ที่รับจดหมายจากภายนอกและส่งต่อให้กับพนักงานที่ถูกต้องภายในออฟฟิศ โดยที่คนส่งจดหมายไม่จำเป็นต้องรู้ว่าพนักงานคนนั้นนั่งอยู่ที่โต๊ะไหน

ขั้นตอนการทำงานของ NAT

1. อุปกรณ์ในเครือข่ายส่วนตัวส่งแพ็กเก็ตข้อมูล

เมื่อคอมพิวเตอร์หรืออุปกรณ์ใดๆ ในเครือข่ายส่วนตัวต้องการส่งข้อมูลออกไปยังอินเทอร์เน็ต (เช่น เข้าเว็บไซต์, ส่งอีเมล) อุปกรณ์นั้นจะส่งแพ็กเก็ตข้อมูลไปยังเราเตอร์ โดยในส่วนหัวของแพ็กเก็ตข้อมูลจะมีที่อยู่ IP ต้นทางเป็นที่อยู่ IP ส่วนตัวของอุปกรณ์นั้น และที่อยู่ IP ปลายทางเป็นที่อยู่ IP ของเซิร์ฟเวอร์ปลายทางบนอินเทอร์เน็ต

2. เราเตอร์ตรวจสอบแพ็กเก็ตข้อมูล

เมื่อเราเตอร์ได้รับแพ็กเก็ตข้อมูลจากอุปกรณ์ในเครือข่ายส่วนตัว เราเตอร์จะตรวจสอบที่อยู่ IP ต้นทางในส่วนหัวของแพ็กเก็ตข้อมูล หากพบว่าเป็นที่อยู่ IP ส่วนตัว เราเตอร์จะทำการแปลงที่อยู่ IP ต้นทางเป็นที่อยู่ IP สาธารณะของตัวเอง

3. เราเตอร์บันทึกข้อมูลการแปลงที่อยู่ IP

เราเตอร์จะบันทึกข้อมูลการแปลงที่อยู่ IP ไว้ในตาราง NAT table โดยจะเก็บข้อมูลคู่ของที่อยู่ IP ส่วนตัวและพอร์ต, ที่อยู่ IP สาธารณะและพอร์ต, รวมถึงข้อมูลอื่นๆ ที่เกี่ยวข้อง เช่น เวลาที่เริ่มต้นการเชื่อมต่อ

4. เราเตอร์ส่งแพ็กเก็ตข้อมูลออกไปยังอินเทอร์เน็ต

หลังจากแปลงที่อยู่ IP ต้นทางแล้ว เราเตอร์จะส่งแพ็กเก็ตข้อมูลออกไปยังอินเทอร์เน็ต โดยแพ็กเก็ตข้อมูลนี้จะมีที่อยู่ IP ต้นทางเป็นที่อยู่ IP สาธารณะของเราเตอร์

5. เซิร์ฟเวอร์ปลายทางตอบกลับแพ็คเกจข้อมูล

เมื่อเซิร์ฟเวอร์ปลายทางบนอินเทอร์เน็ตได้รับแพ็กเก็ตข้อมูล ก็จะประมวลผลและส่งข้อมูลตอบกลับมายังเราเตอร์ โดยในส่วนหัวของแพ็กเก็ตข้อมูลตอบกลับจะมีที่อยู่ IP ต้นทางเป็นที่อยู่ IP ของเซิร์ฟเวอร์ และที่อยู่ IP ปลายทางเป็นที่อยู่ IP สาธารณะของเราเตอร์

6. เราเตอร์แปลงที่อยู่ IP ปลายทาง

เมื่อเราเตอร์ได้รับแพ็กเก็ตข้อมูลตอบกลับจากอินเทอร์เน็ต เราเตอร์จะตรวจสอบ NAT table เพื่อค้นหาว่าแพ็กเก็ตข้อมูลนี้ควรจะส่งต่อไปยังอุปกรณ์ใดในเครือข่ายส่วนตัว โดยจะทำการแปลงที่อยู่ IP ปลายทางจากที่อยู่ IP สาธารณะกลับเป็นที่อยู่ IP ส่วนตัวของอุปกรณ์นั้น

7. เราเตอร์ส่งแพ็กเก็ตข้อมูลตอบกลับไปยังอุปกรณ์ในเครือข่ายส่วนตัว

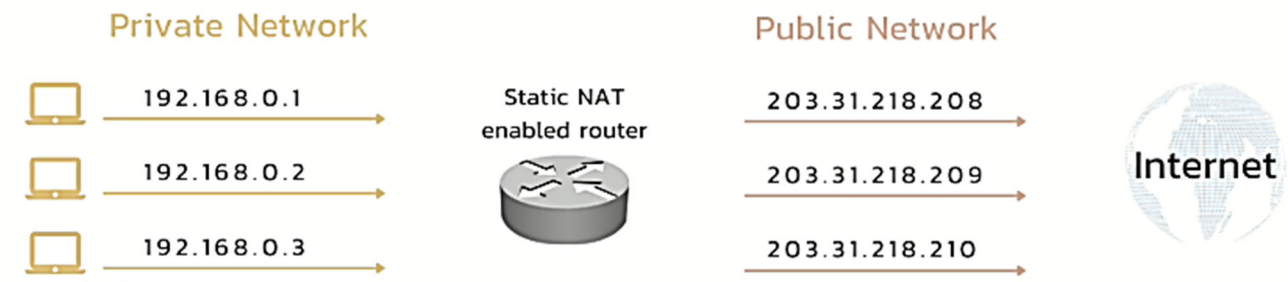
หลังจากแปลงที่อยู่ IP ปลายทางแล้ว เราเตอร์จะส่งแพ็กเก็ตข้อมูลตอบกลับไปยังอุปกรณ์ต้นทางในเครือข่ายส่วนตัว

ประเภทของ **NAT**

NAT (Network Address Translation) แบ่งออกเป็นประเภทหลักๆ ได้ 2 ประเภท ดังนี้

1. Static NAT
2. Dynamic NAT

1. Static NAT



Static NAT คือ รูปแบบหนึ่งของ Network Address Translation (NAT) ที่ทำหน้าที่ **แปลงที่อยู่ IP ส่วนตัว (Private IP Address) ไปเป็นที่อยู่ IP สาธารณะ (Public IP Address) แบบคงที่** นั่นหมายความว่า ที่อยู่ IP ส่วนตัวหนึ่งๆ จะถูกจับคู่กับที่อยู่ IP สาธารณะหนึ่งๆ แบบถาวร ไม่เปลี่ยนแปลงลองนึกภาพตามนะครับ Static NAT ก็เหมือนกับการมี **เบอร์โทรศัพท์บ้าน** ที่เมื่อมีคนโทรเข้ามาที่เบอร์นี้ ก็จะติดต่อกับบ้านหลังนี้หลังเดียวเสมอ ไม่ว่าใครจะเป็นคนโทรเข้ามาลักษณะสำคัญของ Static NAT

- **การจับคู่แบบหนึ่งต่อหนึ่ง (One-to-One Mapping):** ที่อยู่ IP ส่วนตัวหนึ่งอัน จะถูกแมปกับที่อยู่ IP สาธารณะหนึ่งอันแบบตายตัว
- **การเข้าถึงจากภายนอก:** อุปกรณ์ภายในเครือข่ายที่ใช้ Static NAT สามารถถูกเข้าถึงได้จากเครือข่ายภายนอก (อินเทอร์เน็ต) ผ่านที่อยู่ IP สาธารณะที่กำหนดไว้
- **เหมาะสำหรับเซิร์ฟเวอร์:** Static NAT เหมาะสำหรับการใช้งานกับเซิร์ฟเวอร์ภายในเครือข่ายที่ต้องการให้ผู้ใช้ภายนอกเข้าถึงบริการได้โดยตรง เช่น เว็บเซิร์ฟเวอร์, เมลเซิร์ฟเวอร์, เกมเซิร์ฟเวอร์

ตัวอย่างการใช้งาน Static NAT

สมมติว่าคุณมีเว็บเซิร์ฟเวอร์อยู่ในเครือข่ายภายในบ้าน ที่อยู่ IP ส่วนตัวคือ 192.168.1.100 และคุณต้องการให้ผู้ใช้บนอินเทอร์เน็ตเข้าถึงเว็บเซิร์ฟเวอร์นี้ได้ คุณสามารถตั้งค่า Static NAT บนเราเตอร์ โดยกำหนดให้ที่อยู่ IP ส่วนตัว 192.168.1.100 ถูกแปลงเป็นที่อยู่ IP สาธารณะของเราเตอร์ เช่น 203.0.113.10

เมื่อผู้ใช้บนอินเทอร์เน็ตพิมพ์ที่อยู่ IP สาธารณะ 203.0.113.10 ลงในเว็บเบราว์เซอร์ คำขอจะถูกส่งต่อไปยังเราเตอร์ เราเตอร์จะตรวจสอบ Static NAT configuration และส่งต่อคำขอไปยังเว็บเซิร์ฟเวอร์ที่อยู่ IP 192.168.1.100 ภายในเครือข่าย

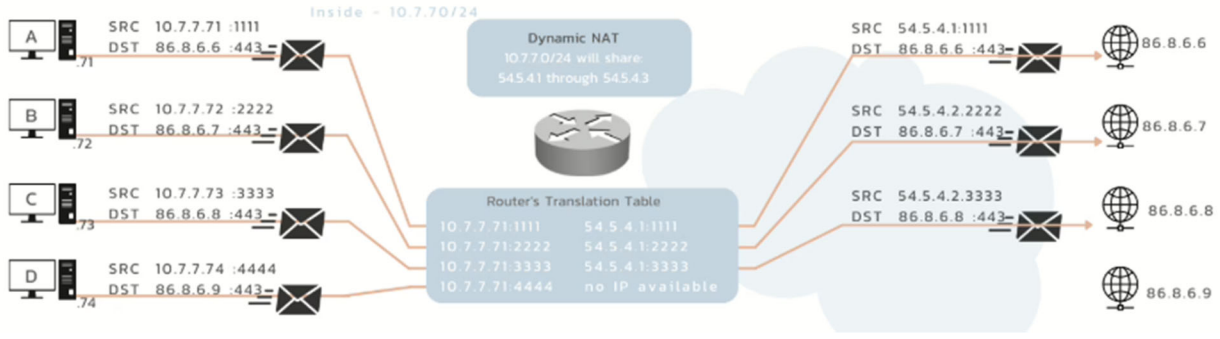
ข้อดีของ Static NAT

- **เข้าถึงอุปกรณ์ภายในได้ง่าย:** ผู้ใช้ภายนอกสามารถเข้าถึงอุปกรณ์ภายในเครือข่ายได้โดยตรงผ่านที่อยู่ IP สาธารณะ
- **ใช้งานง่าย:** การตั้งค่า Static NAT ค่อนข้างง่าย ไม่ซับซ้อน

ข้อเสียของ Static NAT

- **สิ้นเปลืองที่อยู่ IP สาธารณะ:** ต้องใช้ที่อยู่ IP สาธารณะจำนวนเท่ากับอุปกรณ์ที่ต้องการให้เข้าถึงจากภายนอก
- **ความปลอดภัย:** การเปิดให้เข้าถึงอุปกรณ์ภายในโดยตรง อาจมีความเสี่ยงด้านความปลอดภัย หากไม่ได้กำหนดค่า firewall อย่างเหมาะสม

2. Dynamic NAT



Dynamic NAT คือ อีกรูปแบบหนึ่งของ Network Address Translation (NAT) ที่ทำหน้าที่ **แปลงที่อยู่ IP ส่วนตัว (Private IP Address) ไปเป็นที่อยู่ IP สาธารณะ (Public IP Address) แบบไดนามิก** หมายความว่า ที่อยู่ IP ส่วนตัวจะถูกจับคู่กับที่อยู่ IP สาธารณะแบบไม่ตายตัว โดยระบบจะเลือกที่อยู่ IP สาธารณะจากกลุ่มที่กำหนดไว้ให้แบบสุ่ม ณ เวลาที่มีการเชื่อมต่อเปรียบเทียบง่ายๆ Dynamic NAT ก็เหมือนกับการใช้ **เบอร์โทรศัพท์สาธารณะ** ที่มีเบอร์โทรศัพท์หลายเบอร์ให้เลือกใช้ แต่ละครั้งที่เราโทรออก ระบบอาจจะสุ่มให้เราใช้เบอร์ใดเบอร์หนึ่งจากเบอร์ที่มีอยู่

ลักษณะสำคัญของ Dynamic NAT

- **การจับคู่แบบหลายต่อหลาย (Many-to-Many Mapping):** ที่อยู่ IP ส่วนตัวหลายๆ อัน สามารถถูกแปลงเป็นที่อยู่ IP สาธารณะหลายๆ อันได้ โดยไม่มีการกำหนดตายตัวว่า IP ส่วนตัวไหนจะใช้ IP สาธารณะอันไหน
- **การเข้าถึงจากภายนอก:** อุปกรณ์ภายในเครือข่ายที่ใช้ Dynamic NAT **ไม่สามารถ** ถูกเข้าถึงได้จากเครือข่ายภายนอก (อินเทอร์เน็ต) โดยตรง เพราะที่อยู่ IP สาธารณะที่ใช้ไม่ได้ถูกกำหนดไว้ตายตัว ทำให้ไม่รู้ว่าจะต้องใช้ IP สาธารณะอันไหนเพื่อเข้าถึงอุปกรณ์นั้นๆ
- **เหมาะสำหรับ:** ใช้งานกับเครือข่ายที่มีอุปกรณ์จำนวนมากที่ต้องการเชื่อมต่ออินเทอร์เน็ต แต่ไม่จำเป็นต้องให้ผู้ใช้ภายนอกเข้าถึงอุปกรณ์เหล่านั้นโดยตรง เช่น คอมพิวเตอร์พนักงานในบริษัท

ตัวอย่างการใช้งาน Dynamic NAT

สมมติว่าบริษัทมีคอมพิวเตอร์พนักงาน 100 เครื่อง และมีที่อยู่ IP สาธารณะ 10 อัน เมื่อพนักงานต้องการใช้งานอินเทอร์เน็ต เราเตอร์ที่ตั้งค่า Dynamic NAT ไว้จะทำการสุ่มเลือกที่อยู่ IP สาธารณะ 1 อันจาก 10 อันที่มีอยู่เพื่อให้คอมพิวเตอร์เครื่องนั้นใช้เชื่อมต่อ โดยที่อยู่ IP สาธารณะที่ถูกเลือกให้อาจจะเปลี่ยนไปเรื่อยๆ ในแต่ละครั้งที่เชื่อมต่อ

ข้อดีของ Dynamic NAT

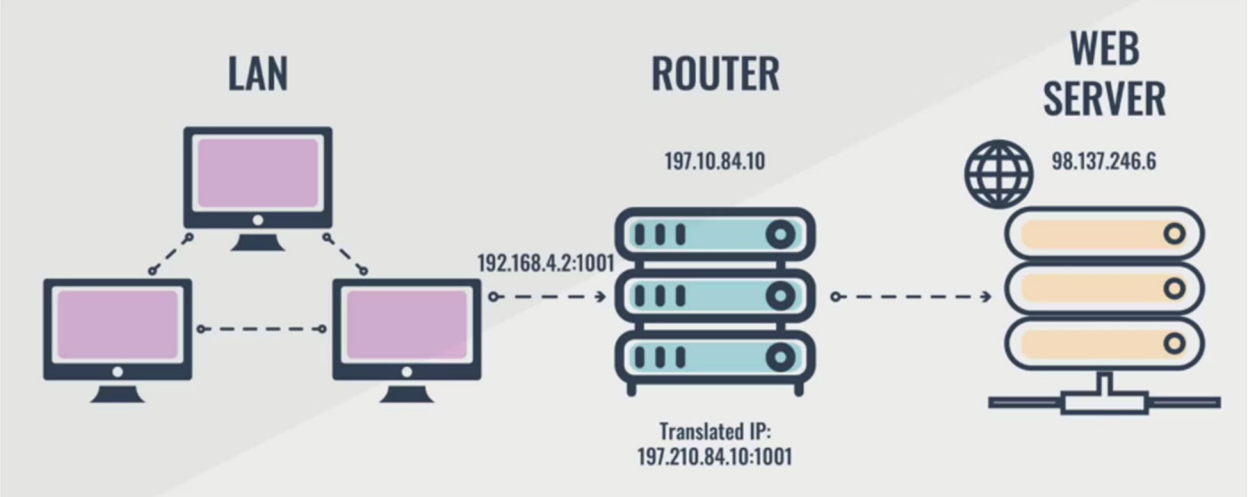
- **ประหยัดที่อยู่ IP สาธารณะ:** สามารถใช้อุปกรณ์หลายเครื่องร่วมกันใช้ที่อยู่ IP สาธารณะจำนวนน้อยกว่าได้ ช่วยลดปัญหาการขาดแคลนที่อยู่ IP
- **ความปลอดภัย:** เนื่องจากอุปกรณ์ภายในไม่สามารถถูกเข้าถึงจากภายนอกโดยตรง จึงช่วยเพิ่มความปลอดภัยให้กับเครือข่าย

ข้อเสียของ Dynamic NAT

- **ไม่สามารถเข้าถึงจากภายนอก:** ไม่เหมาะกับการใช้งานที่ต้องการให้ผู้ใช้ภายนอกเข้าถึงอุปกรณ์ภายในเครือข่ายโดยตรง

Dynamic NAT เป็นรูปแบบ NAT ที่ช่วยประหยัดที่อยู่ IP สาธารณะ และเพิ่มความปลอดภัยให้กับเครือข่าย เหมาะสำหรับเครือข่ายที่มีอุปกรณ์จำนวนมากที่ต้องการเชื่อมต่ออินเทอร์เน็ต แต่ไม่ต้องการให้เข้าถึงจากภายนอกโดยตรง

PAT (Port Address Translation) หรือ NAT Overload



PAT (Port Address Translation) หรือที่รู้จักกันในชื่อ NAT Overload คือ เทคนิคการแปลงที่อยู่เครือข่ายรูปแบบหนึ่งที่ช่วยให้อุปกรณ์หลายเครื่องภายในเครือข่ายส่วนตัว (private network) สามารถแชร์ที่อยู่ IP สาธารณะ (public IP address) เดียวกันในการเชื่อมต่อกับอินเทอร์เน็ตได้

วิธีการทำงานของ PAT

PAT ทำงานโดยการใช้หมายเลขพอร์ต (port number) เพื่อแยกแยะการเชื่อมต่อของอุปกรณ์แต่ละเครื่อง เมื่ออุปกรณ์ภายในเครือข่ายต้องการส่งข้อมูลออกไปยังอินเทอร์เน็ต PAT จะทำการแปลงที่อยู่ IP ต้นทางในส่วนหัวของแพ็กเก็ตข้อมูลจากที่อยู่ IP ส่วนตัวเป็นที่อยู่ IP สาธารณะ พร้อมกับกำหนดหมายเลขพอร์ตเฉพาะให้กับการเชื่อมต่อนั้นๆ

ตัวอย่างการทำงานของ PAT

สมมติว่ามีคอมพิวเตอร์ 2 เครื่องในเครือข่ายภายในบ้าน ต้องการเข้าถึงเว็บไซต์เดียวกันบนอินเทอร์เน็ต โดยใช้ที่อยู่ IP สาธารณะเดียวกัน PAT จะทำการแปลงที่อยู่ IP ส่วนตัวของคอมพิวเตอร์ทั้งสองเครื่องเป็นที่อยู่ IP สาธารณะเดียวกัน แต่จะกำหนดหมายเลขพอร์ตที่แตกต่างกันให้กับแต่ละเครื่อง เช่น

- คอมพิวเตอร์ A: ที่อยู่ IP ส่วนตัว 192.168.1.10 ถูกแปลงเป็นที่อยู่ IP สาธารณะ 203.0.113.1 พอร์ต 55000
- คอมพิวเตอร์ B: ที่อยู่ IP ส่วนตัว 192.168.1.11 ถูกแปลงเป็นที่อยู่ IP สาธารณะ 203.0.113.1 พอร์ต 55001

เมื่อเซิร์ฟเวอร์เว็บไซต์ตอบกลับข้อมูล PAT จะใช้หมายเลขพอร์ตเพื่อระบุว่าข้อมูลควรจะถูกส่งต่อไปยังคอมพิวเตอร์เครื่องใด

ข้อดีของ PAT

- **ประหยัดที่อยู่ IP สาธารณะ:** ช่วยให้สามารถใช้อุปกรณ์หลายเครื่องร่วมกันใช้ที่อยู่ IP สาธารณะเพียงอันเดียวได้ ซึ่งเป็นประโยชน์อย่างมากในยุคที่ที่อยู่ IPv4 ใกล้จะหมดลง
- **เพิ่มความปลอดภัย:** ช่วยซ่อนที่อยู่ IP ส่วนตัวของอุปกรณ์ภายในเครือข่ายจากเครือข่ายภายนอก ทำให้ยากต่อการโจมตีจากภายนอก
- **ใช้งานง่าย:** PAT มักจะถูกตั้งค่าโดยอัตโนมัติในเราเตอร์ ทำให้ผู้ใช้ไม่ต้องกำหนดค่าเอง

ข้อเสียของ PAT

- **ปัญหาการเชื่อมต่อแบบ peer-to-peer:** PAT อาจทำให้เกิดปัญหาในการเชื่อมต่อแบบ peer-to-peer เนื่องจากอุปกรณ์ที่อยู่เบื้องหลัง PAT ไม่สามารถถูกเข้าถึงได้โดยตรงจากอุปกรณ์ภายนอก
- **ความซับซ้อนในการแก้ไขปัญหา:** PAT อาจทำให้การแก้ไขปัญหาเครือข่ายทำได้ยากขึ้น เนื่องจากต้องพิจารณาหมายเลขพอร์ตด้วย

PAT เป็นเทคนิค NAT ที่ได้รับความนิยมอย่างมาก เนื่องจากช่วยประหยัดที่อยู่ IP สาธารณะ และเพิ่มความปลอดภัยให้กับเครือข่าย แม้จะมีข้อจำกัดบ้าง แต่ก็เป็นเทคโนโลยีที่สำคัญที่ช่วยให้เราสามารถใช้งานอินเทอร์เน็ตได้อย่างมีประสิทธิภาพ

การเลือกใช้ NAT ประเภทใดขึ้นอยู่กับความต้องการและลักษณะการใช้งานของเครือข่าย โดย PAT (NAT Overload) เป็นประเภทที่นิยมใช้มากที่สุดในปัจจุบัน เนื่องจากประหยัดที่อยู่ IP สาธารณะได้มากที่สุด

ตารางเปรียบเทียบ NAT แต่ละประเภท

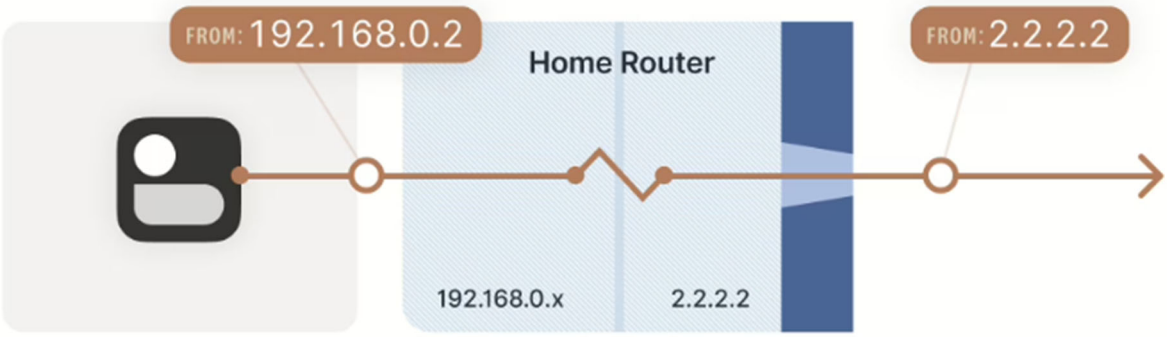
คุณสมบัติ	**Static NAT**	**Dynamic NAT**	**PAT (NAT Overload)**
วิธีการแปลง IP	**จับคู่ IP ส่วนตัวกับ IP สาธารณะแบบคงที่ (1:1)**	**จับคู่ IP ส่วนตัวกับ IP สาธารณะแบบสุ่มจาก pool (หลาย:หลาย)**	**หลาย IP ส่วนตัวใช้ IP สาธารณะเดียวกัน โดยใช้ Port แยกแยะ**
การเข้าถึงจากภายนอก	**เข้าถึงอุปกรณ์ภายในได้โดยตรง ผ่าน IP สาธารณะที่กำหนด**	**ไม่สามารถเข้าถึงอุปกรณ์ภายในโดยตรง**	**ไม่สามารถเข้าถึงอุปกรณ์ภายในโดยตรง**
การใช้ IP สาธารณะ	**สิ้นเปลือง ต้องใช้ IP สาธารณะเท่ากับจำนวนอุปกรณ์ที่ต้องการให้เข้าถึง**	**ประหยัดกว่า Static NAT**	**ประหยัดที่สุด ใช้ IP สาธารณะเพียง 1 อัน**

ความปลอดภัย	เสี่ยงกว่า หากไม่ได้กำหนดค่า Firewall ให้ดี	ปลอดภัยกว่า Static NAT	ปลอดภัยกว่า Static NAT
ความซับซ้อนในการตั้งค่า	ง่าย	ปานกลาง	ง่าย (มักตั้งค่าอัตโนมัติในเราเตอร์)
เหมาะกับ	เซิร์ฟเวอร์ที่ต้องการให้เข้าถึงจากภายนอก เช่น เว็บเซิร์ฟเวอร์, เกมเซิร์ฟเวอร์	เครือข่ายที่มีอุปกรณ์จำนวนมากที่ต้องเชื่อมต่ออินเทอร์เน็ต แต่ไม่ต้องการให้เข้าถึงจากภายนอก	เครือข่ายทั่วไป เช่น เครือข่ายภายในบ้าน, สำนักงานขนาดเล็ก

หมายเหตุ:

- ตารางนี้แสดงการเปรียบเทียบ NAT แต่ละประเภทในภาพรวม
- การเลือกใช้ NAT ประเภทใด ขึ้นอยู่กับความต้องการและลักษณะการใช้งานของแต่ละเครือข่าย

การตรวจสอบ **NAT (NAT traversal)**



การตรวจสอบ NAT (NAT traversal) คือ เทคนิคที่ใช้ในการ **แก้ปัญหาการเชื่อมต่อ** ระหว่างอุปกรณ์ที่อยู่เบื้องหลัง NAT (Network Address Translation)

อย่างที่เราทราบกันดีว่า NAT ช่วยแปลงที่อยู่ IP ส่วนตัวเป็นที่อยู่ IP สาธารณะ เพื่อให้อุปกรณ์ในเครือข่ายส่วนตัวสามารถเชื่อมต่ออินเทอร์เน็ตได้ แต่ NAT ก็สร้างปัญหาให้กับการเชื่อมต่อบางประเภท เช่น การเชื่อมต่อแบบ peer-to-peer เนื่องจากอุปกรณ์ที่อยู่หลัง NAT จะไม่สามารถถูกเข้าถึงโดยตรงจากอุปกรณ์ภายนอกได้

เทคนิคการตรวจสอบ NAT

มีเทคนิคหลากหลายที่ใช้ในการตรวจสอบ NAT ซึ่งแต่ละเทคนิคก็มีข้อดีข้อเสียแตกต่างกันไป ตัวอย่างเทคนิคที่นิยมใช้ เช่น

- **STUN (Session Traversal Utilities for NAT):** เป็นเทคนิคที่ใช้ในการค้นหาประเภทของ NAT และที่อยู่ IP สาธารณะของตัวเอง โดยการส่งคำขอไปยังเซิร์ฟเวอร์ STUN บนอินเทอร์เน็ต
- **TURN (Traversal Using Relays around NAT):** เป็นเทคนิคที่ใช้เซิร์ฟเวอร์ TURN เป็นตัวกลางในการถ่ายทอดข้อมูลระหว่างอุปกรณ์ที่อยู่หลัง NAT โดยข้อมูลจะถูกส่งไปยังเซิร์ฟเวอร์ TURN ก่อน แล้วเซิร์ฟเวอร์ TURN จะส่งต่อข้อมูลไปยังอุปกรณ์ปลายทาง
- **Hole punching:** เป็นเทคนิคที่ใช้ในการเจาะรู (hole) บน NAT เพื่อให้อุปกรณ์ภายนอกสามารถเชื่อมต่อเข้ามาได้ โดยอุปกรณ์ทั้งสองฝั่งจะต้องส่งข้อมูลออกไปยังเซิร์ฟเวอร์ภายนอกพร้อมกัน เพื่อให้ NAT เปิดพอร์ตสำหรับการเชื่อมต่อ
- **Application-level gateways (ALG):** เป็นเทคนิคที่ใช้ gateway ในการตรวจสอบและปรับเปลี่ยนข้อมูลในแพ็กเก็ตข้อมูล เพื่อให้การเชื่อมต่อผ่าน NAT ทำงานได้อย่างถูกต้อง

การใช้งานการตรวจสอบ NAT

การตรวจสอบ NAT ถูกนำมาใช้ในแอปพลิเคชันและบริการต่างๆ ที่ต้องการการเชื่อมต่อแบบ peer-to-peer เช่น

- **VoIP (Voice over IP):** เช่น โปรแกรมโทรศัพท์ผ่านอินเทอร์เน็ต
- **Video conferencing:** เช่น โปรแกรมประชุมทางไกล
- **Online gaming:** เช่น เกมออนไลน์
- **File sharing:** เช่น โปรแกรมแชร์ไฟล์

ข้อจำกัดของการตรวจสอบ NAT

- **ความซับซ้อน:** การตรวจสอบ NAT อาจมีความซับซ้อนในการติดตั้งและกำหนดค่า
- **ประสิทธิภาพ:** การใช้เทคนิคการตรวจสอบ NAT อาจส่งผลกระทบต่อประสิทธิภาพของเครือข่าย
- **ความเข้ากันได้:** เทคนิคการตรวจสอบ NAT บางอย่าง อาจไม่สามารถใช้งานได้กับ NAT ทุกประเภท

สรุปการตรวจสอบ NAT (NAT traversal)

การตรวจสอบ NAT เป็นเทคนิคที่สำคัญที่ช่วยให้แอปพลิเคชันและบริการต่างๆ สามารถทำงานได้อย่างถูกต้อง แม้ว่าอุปกรณ์จะอยู่เบื้องหลัง NAT แม้จะมีข้อจำกัดบ้าง แต่ก็เป็นเทคโนโลยีที่ช่วยให้เราสามารถใช้งานอินเทอร์เน็ตได้อย่างเต็มประสิทธิภาพ

NAT IP คือ

NAT IP หมายถึง Public IP Address ที่ Router ใช้งานในการเชื่อมต่ออินเทอร์เน็ต ซึ่งเป็น IP Address ที่อุปกรณ์ภายนอกมองเห็นเมื่อมีการติดต่อจากเครือข่ายของคุณ

1. ที่อยู่ IP สาธารณะ (Public IP Address) ที่ใช้ในการแปลงที่อยู่

- ในกระบวนการ NAT เราเตอร์หรืออุปกรณ์ NAT จะแปลงที่อยู่ IP ส่วนตัวของอุปกรณ์ภายในเครือข่าย เป็นที่อยู่ IP สาธารณะ เพื่อให้สามารถสื่อสารกับอินเทอร์เน็ตได้
- ที่อยู่ IP สาธารณะนี้ เรียกได้ว่าเป็น “NAT IP” เพราะเป็น IP ที่ถูกใช้ในกระบวนการ NAT
- โดยทั่วไปแล้ว NAT IP จะเป็นที่อยู่ IP สาธารณะที่ผู้ให้บริการอินเทอร์เน็ต (ISP) กำหนดให้กับเราเตอร์ของคุณ

2. ที่อยู่ IP ของอุปกรณ์ NAT เอง

- อุปกรณ์ที่ทำหน้าที่ NAT เช่น เราเตอร์ จะมีที่อยู่ IP ของตัวเอง ซึ่งอาจจะเป็นได้ทั้งที่อยู่ IP ส่วนตัวหรือที่อยู่ IP สาธารณะ
- ที่อยู่ IP ของอุปกรณ์ NAT นี้ ก็สามารถเรียกได้ว่าเป็น “NAT IP” เช่นกัน เพราะเป็น IP ของอุปกรณ์ที่ทำหน้าที่ NAT

ตัวอย่าง

สมมติว่าคุณมีคอมพิวเตอร์ที่เชื่อมต่อกับเราเตอร์ภายในบ้าน และต้องการเข้าถึงเว็บไซต์บนอินเทอร์เน็ต

- คอมพิวเตอร์ของคุณมีที่อยู่ IP ส่วนตัว เช่น 192.168.1.100
- เราเตอร์ของคุณมีที่อยู่ IP สาธารณะ เช่น 203.0.113.1 และทำหน้าที่ NAT
- เมื่อคอมพิวเตอร์ของคุณส่งข้อมูลไปยังเว็บไซต์ เราเตอร์จะแปลงที่อยู่ IP ต้นทางจาก 192.168.1.100 เป็น 203.0.113.1

ในกรณีนี้ “NAT IP” สามารถหมายถึง 203.0.113.1 (ที่อยู่ IP สาธารณะที่ใช้ในการแปลง) หรืออาจหมายถึงที่อยู่ IP ของเราเตอร์เอง ซึ่งก็คือ 203.0.113.1 เช่นกัน

NAT Network คือ

NAT Network หมายถึง เครือข่ายที่ใช้วิธี NAT ในการเชื่อมต่ออินเทอร์เน็ต ซึ่งเป็นเครือข่ายที่พบเห็นได้ทั่วไป เช่น เครือข่ายภายในบ้าน หรือเครือข่ายองค์กรขนาดเล็ก

ซึ่งหมายความว่า อุปกรณ์ต่างๆ ภายในเครือข่ายนี้ จะมีที่อยู่ IP ส่วนตัว และใช้ NAT ในการแปลงที่อยู่ IP ส่วนตัวเหล่านี้ เป็นที่อยู่ IP สาธารณะ เพื่อเชื่อมต่อกับอินเทอร์เน็ต

ลักษณะเด่นของ NAT Network

- **ใช้ที่อยู่ IP ส่วนตัว:** อุปกรณ์ภายในเครือข่ายจะใช้ที่อยู่ IP ส่วนตัว เช่น 192.168.1.x หรือ 10.0.0.x

- **มีอุปกรณ์ NAT:** จะมีอุปกรณ์ที่ทำหน้าที่ NAT เช่น เราเตอร์ ซึ่งจะทำหน้าที่แปลงที่อยู่ IP ส่วนตัวเป็นที่อยู่ IP สาธารณะ
- **เข้าถึงอินเทอร์เน็ตได้:** อุปกรณ์ภายในเครือข่ายสามารถเข้าถึงอินเทอร์เน็ตได้ แม้จะใช้ที่อยู่ IP ส่วนตัว
- **อาจถูกจำกัดการเข้าถึงจากภายนอก:** อุปกรณ์ภายในเครือข่ายอาจถูกจำกัดการเข้าถึงจากภายนอก ขึ้นอยู่กับการตั้งค่า NAT

ตัวอย่าง NAT Network

- **เครือข่ายภายในบ้าน:** เราเตอร์ Wi-Fi ในบ้านของคุณ มักจะทำหน้าที่ NAT โดยแปลงที่อยู่ IP ส่วนตัวของอุปกรณ์ต่างๆ ในบ้าน (เช่น สมาร์ทโฟน, คอมพิวเตอร์, Smart TV) เป็นที่อยู่ IP สาธารณะ เพื่อเชื่อมต่ออินเทอร์เน็ต
- **เครือข่ายองค์กร:** บริษัทหรือองค์กร มักจะใช้ NAT เพื่อให้คอมพิวเตอร์พนักงานจำนวนมาก สามารถเชื่อมต่ออินเทอร์เน็ตได้โดยใช้ที่อยู่ IP สาธารณะเพียงไม่กี่อัน
- **เครือข่ายเสมือน (Virtual Network):** ในระบบ Cloud Computing เครือข่ายเสมือนต่างๆ มักจะใช้ NAT เพื่อเชื่อมต่อกับอินเทอร์เน็ต

ประโยชน์ของ NAT Network

- **ประหยัดที่อยู่ IP สาธารณะ:** ช่วยลดปัญหาการขาดแคลนที่อยู่ IP
- **เพิ่มความปลอดภัย:** ช่วยซ่อนที่อยู่ IP ส่วนตัวของอุปกรณ์ภายใน ป้องกันการโจมตีจากภายนอก
- **ความยืดหยุ่น:** ช่วยให้สามารถจัดการเครือข่ายภายในได้อย่างยืดหยุ่น

NAT Network คือ เครือข่ายที่ใช้ NAT ในการแปลงที่อยู่ IP เป็นเทคโนโลยีที่สำคัญที่ช่วยให้เราสามารถใช้งานอินเทอร์เน็ตได้อย่างมีประสิทธิภาพ ปลอดภัย และประหยัด

ตัวอย่างคำสั่ง **NAT**

1. สร้าง access list สำหรับเครือข่ายที่คุณต้องการ NAT (เช่น เครือข่ายส่วนตัวของคุณที่ PC0 อยู่)

   Router(config)#access-list 2 permit 192.168.1.0 0.0.0.255

2. สร้างคำสั่ง NAT - ip nat inside source list [access-list name] interface [เช่น serial 0/1] overload

   นำ nat inside & nat outside ไปใช้กับอินเทอร์เฟซภายในและภายนอก

   Router(config)#ip nat inside source list 2 interface f0/0 overload

3. Enable NAT ที่ Interface ให้ถูกต้อง interface ขานอกใช้ nat outside , interface ขาในใช้ nat inside

   Router(config)#interface f0/1

   Router(config-if)#ip nat inside

   Router(config-if)#exit

   Router(config)#interface f1/1

   Router(config-if)#ip nat outside

   Router(config-if)#exit

4. ทดสอบ - ping และใช้คำสั่ง show ip nat translation

   Router#show ip nat translations

   Pro Inside global Inside local Outside local Outside global
   icmp 33.33.33.33:62855 192.168.1.1:62855 2.2.2.2:62855 2.2.2.2:62855
   icmp 33.33.33.33:63111 192.168.1.1:63111 2.2.2.2:63111 2.2.2.2:63111
   icmp 33.33.33.33:63623 192.168.1.1:63623 2.2.2.2:63623 2.2.2.2:63623