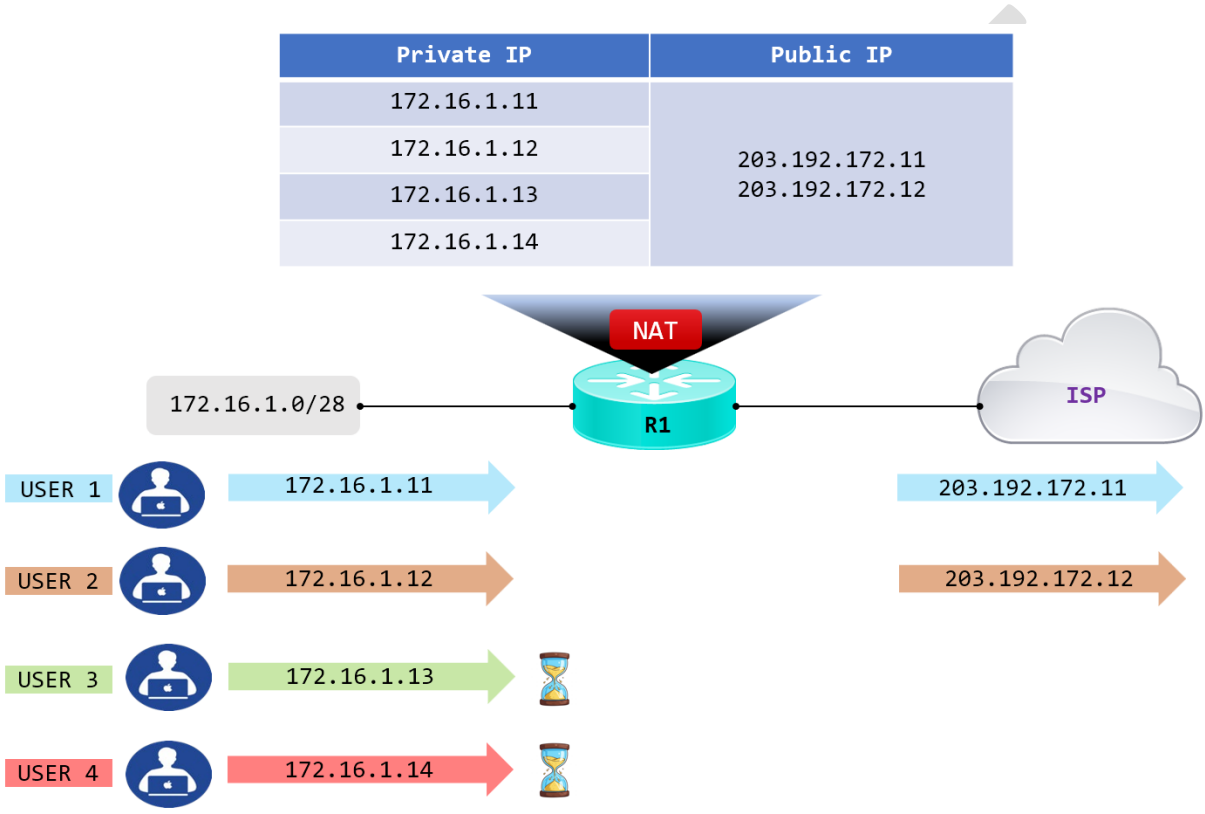
Dynamic NAT

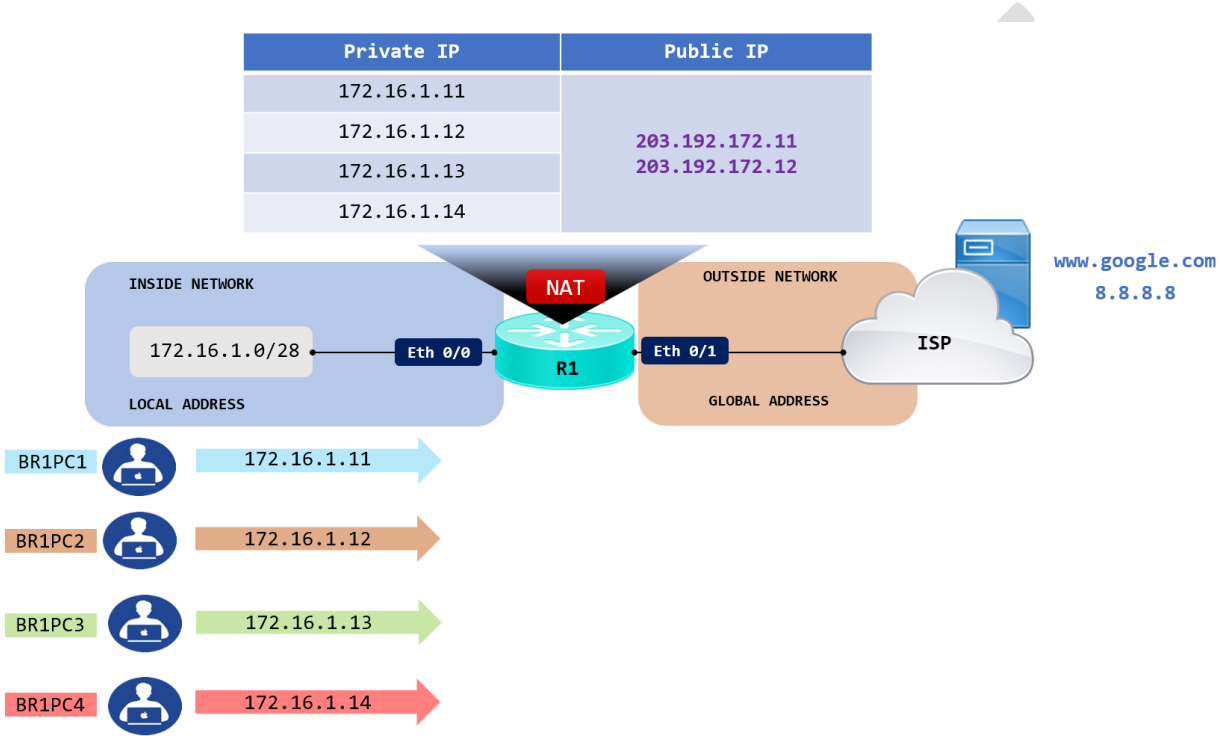
ในบทก่อนหน้านี้ได้กล่าวถึง Static NAT และการ Config ต้องจับคู่ระหว่าง IP Private กับ IP Public เพื่อแปลงหรือ Translate IP ไปมาระหว่างกัน แบบเจาะจงหรือ Fixed เอาไว้ แต่สำหรับ Dynamic NAT นั้น อุปกรณ์ที่ทำหน้าที่ NAT เช่น Router จะทำการแปลงระหว่าง IP Public และ IP Private ไปมา ให้อัตโนมัติ โดยจะมองไปยังที่ Pool ของ IP จริง ถ้าหากมี IP Public ที่เพียงพอก็จะสามารถใช้งานได้



ตามรูปที่ได้แสดงตัวอย่างด้านบน ในเครือข่ายภายในหรือ LAN มี User/Client ทั้งหมด 4 IP และมี IP Public ใน Pool เพียง 2 IP เมื่อ Client ต้องการใช้งาน Internet จะเห็นได้ว่าสามารถใช้งานพร้อมกันเพียงแค่ 2 User/Client เท่านั้น ตามจำนวนของ Public IP ที่มีอยู่ นั่นคือ Client ที่ 1 และ 2 ส่วน Client 3 และ 4 ต้องรอจนกว่า Client ที่ 1 และ 2 ใช้งานเสร็จ และมี IP Public เหลืออยู่ใน Pool จึงจะสามารถใช้งานได้

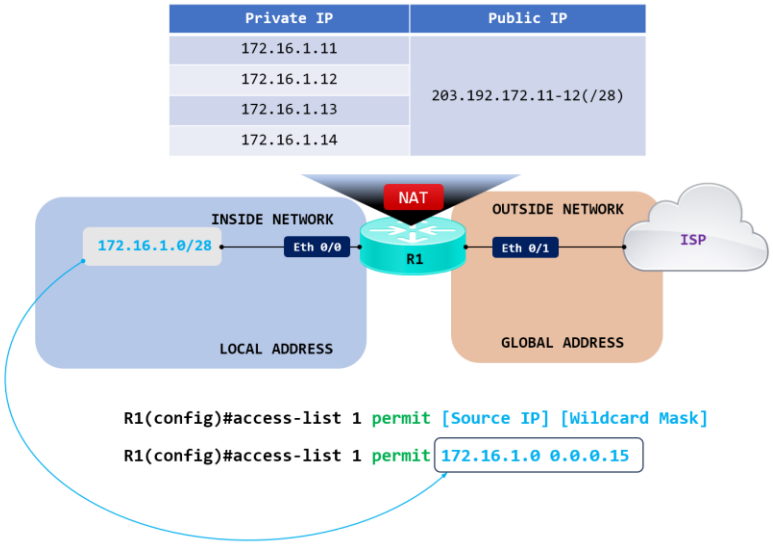
Dynamic NAT Configuration

การ Config Dynamic NAT จะแตกต่างออกไปจาก Static NAT ที่เป็นการจับคู่ IP Private และ IP Public กันโดยตรง ในส่วนของ Dynamic NAT นั้น ต้องมีการสร้าง Access Control List (ACL) เพื่อเป็นการเลือกกลุ่มของ Private IP หรือ IP ภายในองค์กรที่ต้องการใช้งาน Internet หรือต้องการให้มีการ NAT จากนั้นจึงกำหนด Pool ของ Public IP เพื่อที่จะให้ Private IP ได้ใช้งาน Translation IP

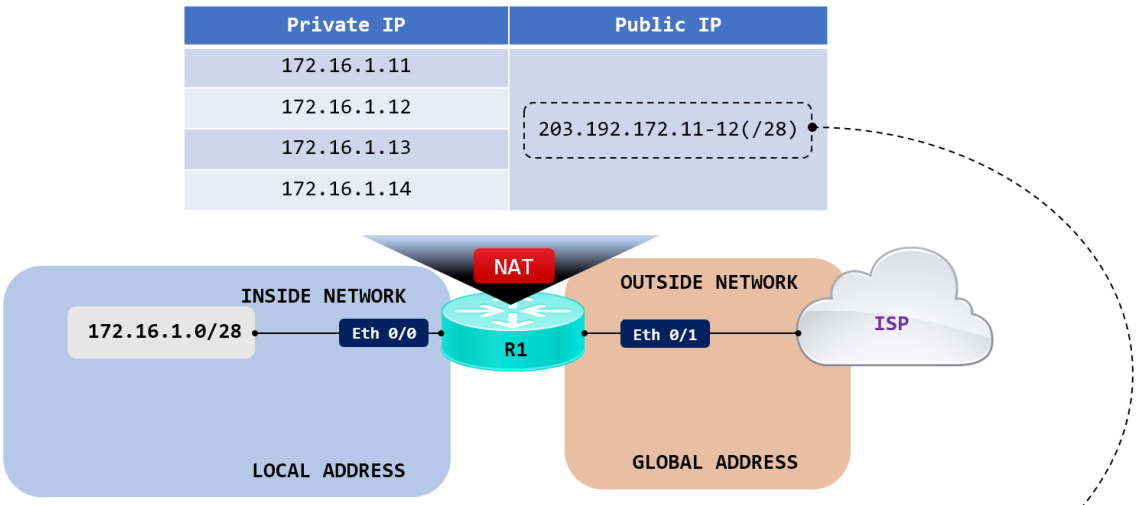


อ้างอิงจาก Diagram ด้านบน เราจะสามารถ Config Dynamic NAT ได้อย่างไร?

- สร้าง ACL แบบ Standard เพื่อระบุ Source IP ที่ต้องการจะให้มีการ NAT ซึ่งเป็นในส่วนของ Private IP หรือ IP ที่ใช้งานในองค์กร



- ทำการสร้าง Pool ของ IP Public ในตัวอย่างนี้มี 2 IP คือ 203.192.172.11-12 (/28)




```
R1(config)#ip nat pool [Pool Name] [Start IP And Stop IP] [Netmask or Prefix-length]

R1(config)#ip nat pool DYN_NAT 203.192.172.11 203.192.172.12 netmask 255.255.255.240
                                        OR
R1(config)#ip nat pool DYN_NAT 203.192.172.11 203.192.172.12 prefix-length 28
```

Pool Name: ตั้งชื่อ Pool ของ Public IP

Start IP And Stop IP: ชุด IP Public ที่ใช้ จากตัวอย่างได้ใช้ 2 IP เริ่มที่ 203.192.172.11 และ จบที่ IP 203.192.172.12

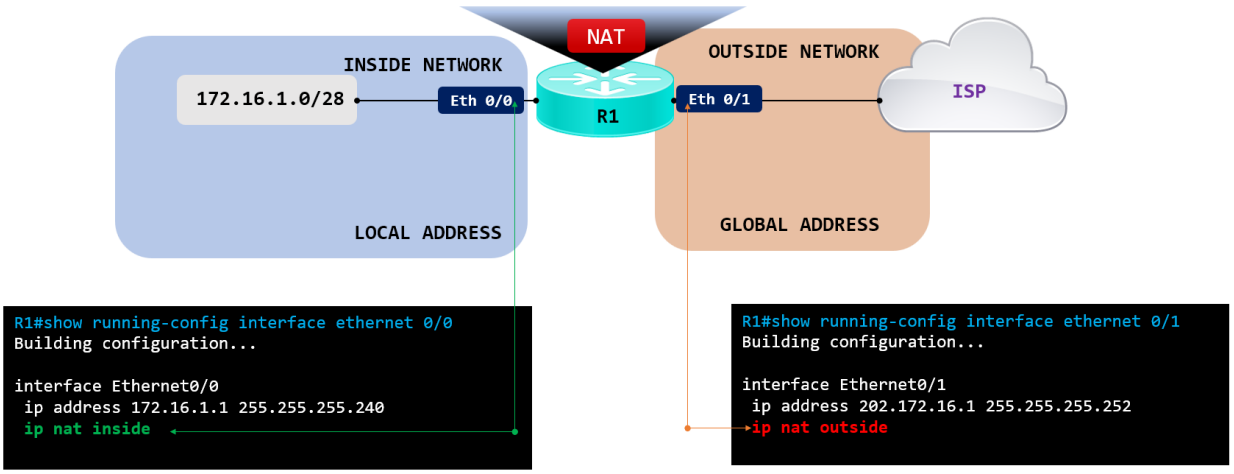
Netmask or Prefix-length: Netmask ของ IP Public ซึ่งทางผู้ให้บริการหรือหน่วยงานที่ทำการจัดสรร IP Public ได้กำหนดไว้ให้ จากในตัวอย่างคือ 255.255.255.240 ถ้าหากเขียนอยู่ในรูปของ Prefix-length คือ /28 นั่นเอง

- ทำการผูก ACL และ IP Pool เข้าด้วยกัน เพื่อให้ IP Private ได้เข้ามาหยิบใช้ IP Public ใน Pool ที่ได้ทำการสร้างก่อนหน้านี้ โดยใช้คำสั่งที่ได้แสดงด้านล่าง

```
R1(config)#ip nat inside source list [ACL Number or Name] Pool [Pool Name]
R1(config)#ip nat inside source list 1 pool DYN_NAT
```

- กำหนด Interface ที่เป็น Inside Network และ Outside Network

Private IP	Public IP
172.16.1.11	203.192.172.11-12(/28)
172.16.1.12	
172.16.1.13	
172.16.1.14	



ทำการทดสอบหลังจากที่ได้ Config Dynamic NAT แล้ว โดยการ Ping จาก User BR1PC1-4 ไปยัง 8.8.8.8 พร้อมกัน เห็นได้ว่ามีเพียง 2 User/Client เท่านั้น คือ BR1PC1 และ BRPC2 ที่สามารถ Ping ไปยัง 8.8.8.8 ได้ เนื่องจาก IP Public มีเพียง 2 IP และ Client BR1PC3 และ BR1PC4 ไม่สามารถ Ping ไปยัง 8.8.8.8 ได้ เพราะ Public IP ถูกใช้งานไปจนหมดแล้วต้องรอให้มี IP Public ว่างจึงจะสามารถใช้งานได้อีกครั้ง

```
BR1PC1> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=1.199 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=1.026 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=253 time=0.703 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=253 time=1.285 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=253 time=1.088 ms
```

ผล Ping ไปยัง 8.8.8.8 จาก BR1PC1

```
BR1PC2> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=1.359 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=1.324 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=253 time=1.454 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=253 time=1.203 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=253 time=0.893 ms
```

ผล Ping ไปยัง 8.8.8.8 จาก BR1PC2

```
BR1PC3> ping 8.8.8.8

*172.16.1.1 icmp_seq=1 ttl=255 time=0.811 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.1 icmp_seq=2 ttl=255 time=0.569 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.1 icmp_seq=3 ttl=255 time=0.934 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.1 icmp_seq=4 ttl=255 time=0.634 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.1 icmp_seq=5 ttl=255 time=0.614 ms (ICMP type:3, code:1, Destination host unreachable)
```

ผล Ping ไปยัง 8.8.8.8 จาก BR1PC3

```
BR1PC4> ping 8.8.8.8

*172.16.1.1 icmp_seq=1 ttl=255 time=1.559 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.1 icmp_seq=2 ttl=255 time=1.625 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.1 icmp_seq=3 ttl=255 time=0.748 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.1 icmp_seq=4 ttl=255 time=0.691 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.1 icmp_seq=5 ttl=255 time=0.801 ms (ICMP type:3, code:1, Destination host unreachable)
```

ผล Ping ไปยัง 8.8.8.8 จาก BR1PC4

หลังจากที่ทดสอบ Ping แล้ว จากนั้นใช้คำสั่ง “show ip nat translation” เพื่อดู NAT Table เห็นได้ว่า IP ของ BR1PC1 และ BR1PC2 ได้ถูก Translation ตามรูปด้านล่าง

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 203.192.172.12:60762 172.16.1.11:60762 8.8.8.8:60762    8.8.8.8:60762
icmp 203.192.172.12:61018 172.16.1.11:61018 8.8.8.8:61018    8.8.8.8:61018
icmp 203.192.172.12:61274 172.16.1.11:61274 8.8.8.8:61274    8.8.8.8:61274
icmp 203.192.172.12:61530 172.16.1.11:61530 8.8.8.8:61530    8.8.8.8:61530
icmp 203.192.172.12:61786 172.16.1.11:61786 8.8.8.8:61786    8.8.8.8:61786
--- 203.192.172.12     172.16.1.11        ---                ---
icmp 203.192.172.11:61274 172.16.1.12:61274 8.8.8.8:61274    8.8.8.8:61274
icmp 203.192.172.11:61530 172.16.1.12:61530 8.8.8.8:61530    8.8.8.8:61530
icmp 203.192.172.11:61786 172.16.1.12:61786 8.8.8.8:61786    8.8.8.8:61786
icmp 203.192.172.11:62042 172.16.1.12:62042 8.8.8.8:62042    8.8.8.8:62042
icmp 203.192.172.11:62298 172.16.1.12:62298 8.8.8.8:62298    8.8.8.8:62298
--- 203.192.172.11     172.16.1.12        ---                ---
```

ส่วน IP ของ BR1PC3 และ BR1PC4 จะไม่เห็นในตาราง NAT Table เนื่องจากไม่มีการ Translate IP เกิดขึ้น เนื่องจาก IP Public ไม่เพียงพอที่จะนำมาใช้งาน

Dynamic NAT จะมีข้อดีคืออุปกรณ์ที่ทำ NAT เช่น Router จะทำหน้าที่ Translate IP ให้อัตโนมัติ แต่ก็ยังคงมีข้อเสียอยู่ ถ้าหากเกิดกรณีเหมือนกันกับในตัวอย่างคือมี IP Public ที่ไม่เพียงพอหรือไม่ครอบคลุมกับ Private IP ที่จะใช้งานจริง จะเกิดปัญหา เช่น บาง User/Client ไม่สามารถใช้งาน Internet ได้

9HUA Train