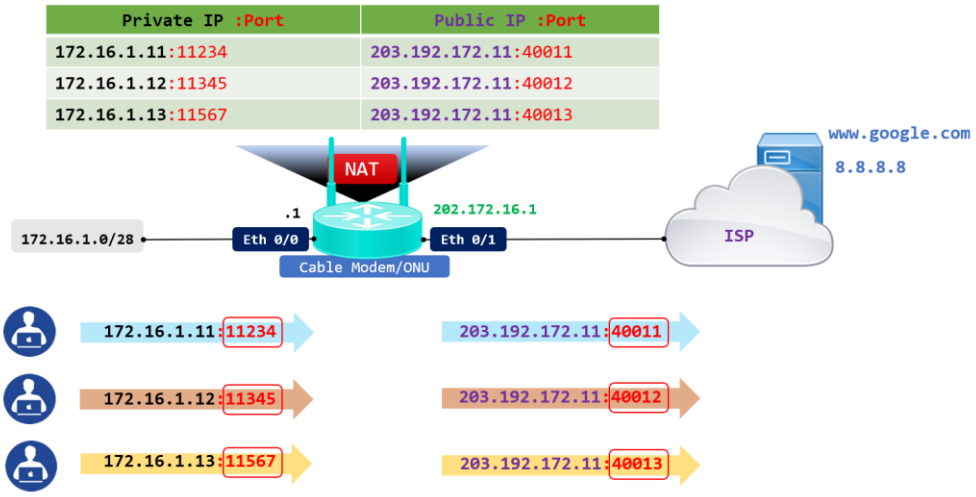
Port Address Translation - PAT

Port Address Translation - PAT หรือ NAT Overload เป็นการ NAT อีกรูปแบบหนึ่งโดยใช้หมายเลข Port ที่อยู่ใน Layer 4 คือ TCP/UDP Port เข้ามาเกี่ยวข้องด้วย ดัง Diagram ที่ได้แสดงด้านล่าง



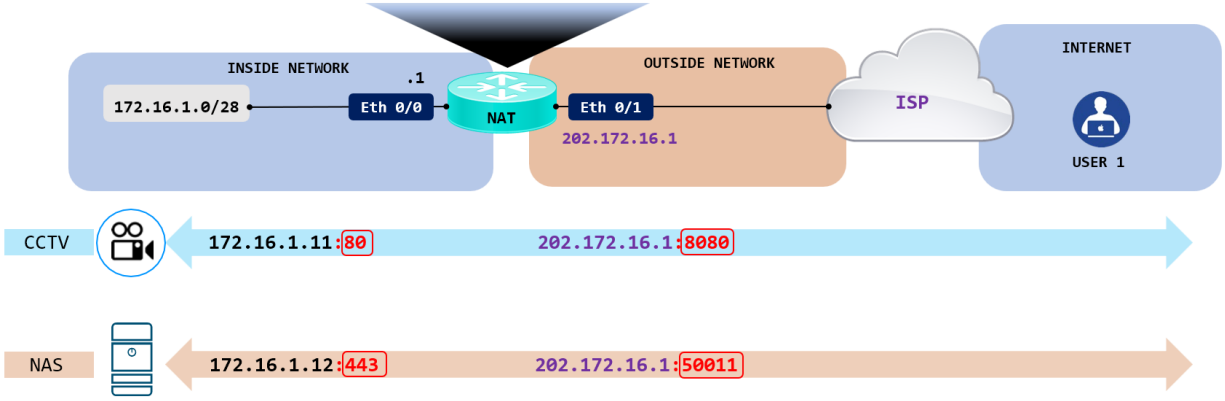
ข้อดีของ PAT คือสามารถใช้ Public IP เพียง 1 IP ก็สามารถรองรับการใช้งาน User/Client ได้จำนวนมาก ตัวอย่างที่มีการใช้ PAT ก็คือ Internet ที่ใช้กันตามบ้านเรือนทั่วไปหรือ Home Use ถ้าหากทำการตรวจสอบ IP Public จะเห็นได้ว่าอุปกรณ์ภายในบ้านที่เชื่อมต่อกับ Router ผู้ให้บริการ จะมี IP Public ที่เป็น IP เดียวกันทุกอุปกรณ์

PAT มีอยู่ด้วยกัน 2 แบบด้วยกัน คือ Static PAT และ Dynamic PAT สำหรับในบทความนี้จะขอกล่าวถึง PAT Static เป็นลำดับแรกก่อน

Static PAT

Static PAT หรือที่เราเข้าใจและรู้จักกันก็คือการ Forward Port โดยทำการกำหนดหมายเลขของ TCP/UDP Port ของทั้งฝั่ง Private IP และ Public IP ตามรูปที่ได้แสดงด้านล่าง ตัวอย่างการใช้งาน Static PAT เช่น กล้องวงจรปิดหรือ IP CCTV ที่ติดตั้งภายในบ้านแล้วสามารถ Login เพื่อดูกล้องวงจรปิดภายในบ้านจากที่อื่นได้ ในรูปตัวอย่าง User 1 ต้องการดูกล้องวงจรปิด ก็อาจจะทำการ Access เข้า IP Public ผ่าน Web Browser แล้วตามด้วย TCP/UDP Port ซึ่งในที่นี้คือ 8080 จากนั้น Router ที่ทำหน้าที่ NAT เห็นว่า Port ที่เข้ามาคือ Port 8080 ก็จะทำการ Translate เป็น IP Private คือ 172.16.1.11 Port 80 จึงทำให้ User 1 สามารถดูกล้องวงจรปิดภายในบ้านได้

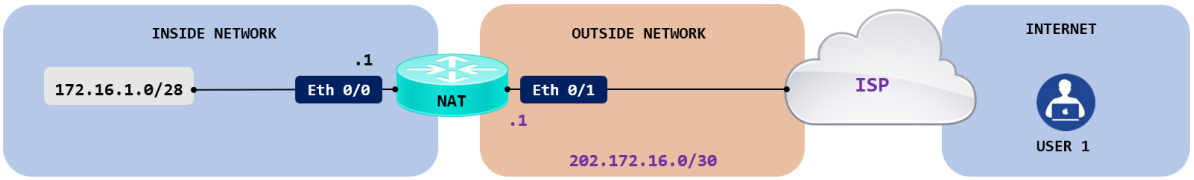
Private IP :Port	Public IP :Port
172.16.1.11:80	202.172.16.1:8080
172.16.1.12:443	202.172.16.1:50011



หรืออีก 1 ตัวอย่าง ถ้าหากมีการใช้ NAS (Network Attached Storage) ภายในบ้านหรือองค์กร ก็ต้องมีการ Forward Port เพื่อที่จะสามารถเข้าใช้งาน NAS จากที่อื่นได้

PAT And Static PAT Configuration

ในลำดับถัดไปเป็นตัวอย่างในการ Config PATและ Static PAT โดยจะกำหนดให้ Inside Network ที่ใช้งานมี Private IP เป็นเครือข่าย 172.16.1.0/28 และ Outside Network ใช้ IP Public 202.172.16.1/30 ซึ่งเป็น IP WAN (Wide Area Network) ที่ใช้เชื่อมต่อกับผู้ให้บริการ ดังรูป Diagram ที่ได้แสดงด้านล่าง



- สร้าง ACL แบบ Standard เพื่อเลือกกลุ่ม IP Private ที่ต้องการ สามารถใช้ ACL Standard แบบ Number หรือแบบ Name ก็ได้ ในตัวอย่างนี้จะแสดง ACL Standard แบบ Name

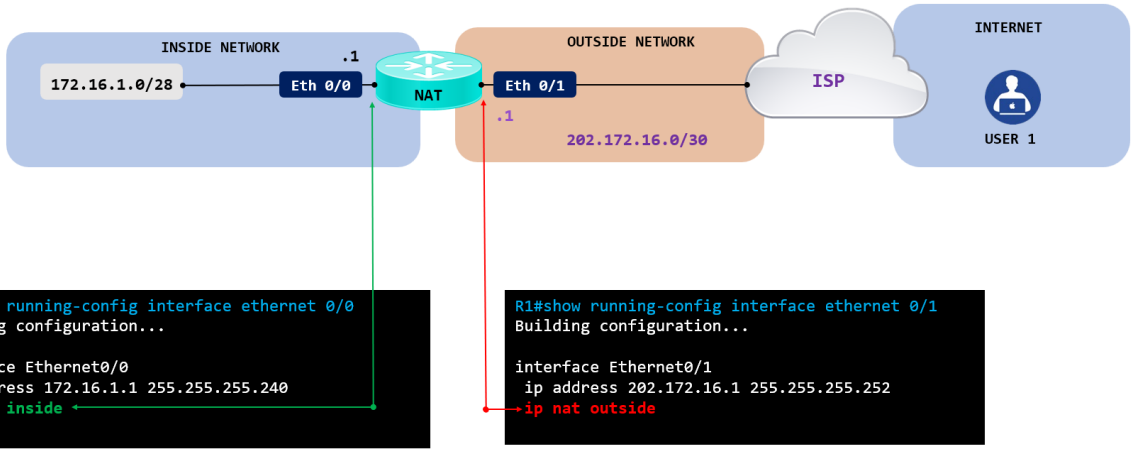
```
R1(config)#access-list [Number standard ACL] [permit/deny] [Source IP] [Wildcard Mask]
```

OR

```
R1(config)#ip access-list standard [Number or Name]
R1(config-std-nacl)#[permit/deny] [Source IP] [Wildcard Mask]
```

```
R1(config)#ip access-list standard PRIVATE_NET
R1(config-std-nacl)#permit 172.16.1.0 0.0.0.15
```

- กำหนด Interface สำหรับ Inside Network และ Outside Network



- ใช้คำสั่งตามรูปที่ได้แสดงด้านล่างเพื่อเป็นการใช้งาน NAT Overload หรือ PAT

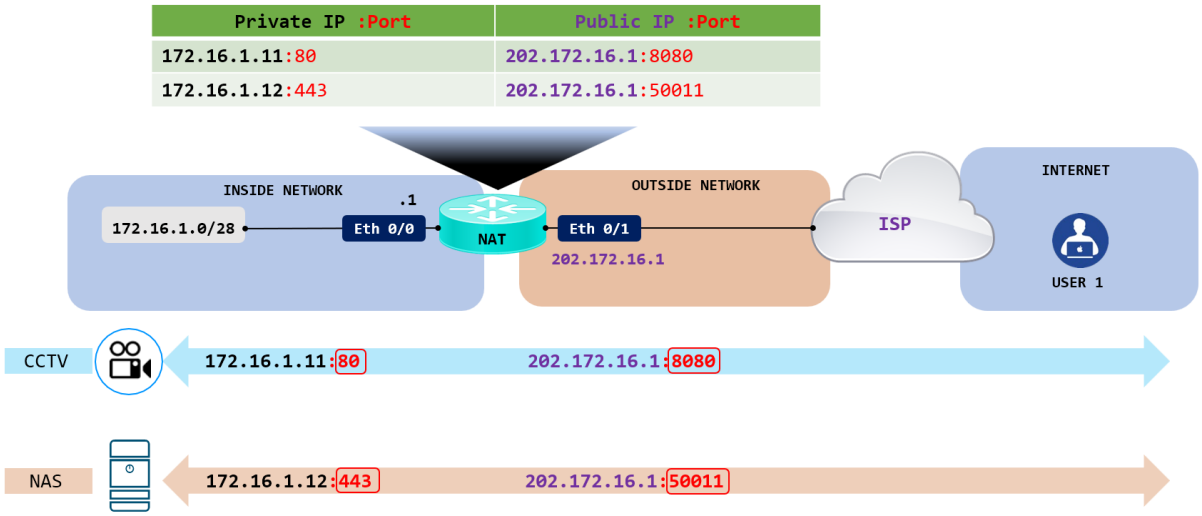
```
R1(config)#ip nat inside source list [ACL Number/Name] interface [Outside Interface] overload
```

```
R1(config)#ip nat inside source list PRIVATE_NET interface ethernet 0/1 overload
```

- ทำการตรวจสอบโดยใช้คำสั่ง “show ip nat translation” ที่ Router R1 ซึ่งทำหน้าที่ NAT เห็นได้ว่ามี IP Private 172.16.1.11 และ 172.16.1.12 สามารถเชื่อมต่อไปยัง Internet ได้ โดยใช้ IP Public เป็น IP เดียวกันคือ 202.172.16.1 แต่จะมีหมายเลข TCP/UDP Port ที่แตกต่างกันออกไปซึ่งอุปกรณ์ที่ทำหน้าที่ NAT จะเป็นผู้กำหนดให้ จึงทำให้เปรียบเสมือนว่าใช้คนละ IP Public นั่นเอง

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 202.172.16.1:0    172.16.1.11:0      8.8.8.8:0          8.8.8.8:0
icmp 202.172.16.1:1    172.16.1.11:1      8.8.8.8:1          8.8.8.8:1
icmp 202.172.16.1:2    172.16.1.12:1      8.8.8.8:1          8.8.8.8:2
icmp 202.172.16.1:3    172.16.1.12:2      8.8.8.8:2          8.8.8.8:3
```

- หลังจากที่ทำการตรวจสอบการเชื่อมต่อและสามารถใช้งาน Internet ได้แล้ว ในลำดับถัดไปจะเป็นการกำหนดหมายเลข Port TCP/UDP Port หรือการทำ Static PAT เพื่อที่จะจำลองให้สามารถดู CCTV และใช้งาน NAS จาก Internet ได้ โดยได้กำหนด TCP/UDP Port ตามรูป Diagram ที่ได้แสดงด้านล่าง



คำสั่งที่ใช้สำหรับในการ Config Static PAT ที่ Router R1 ที่ทำหน้าที่ NAT

```
R1(config)#ip nat inside source static [TCP/UDP] [IP PRVATE] [Local Port] interface [INSIDE GLOBAL IP] [Global TCP/UDP Port]

R1(config)#ip nat inside source static tcp 172.16.1.11 80 202.172.16.1 8080
                                           CCTV

R1(config)#ip nat inside source static tcp 172.16.1.12 443 202.172.16.1 50011
                                           NAS
```

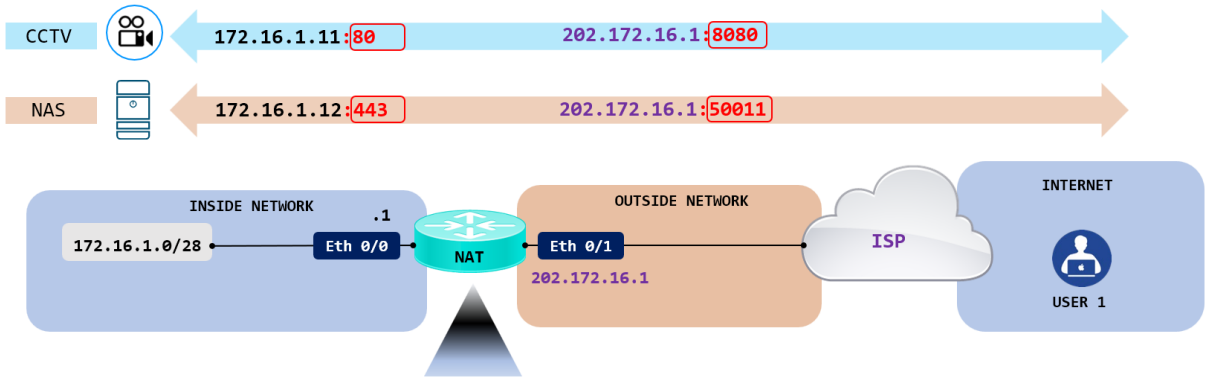
- ตรวจสอบ NAT Table “show ip nat translation” หลังจากที่ทำการ Config Static PAT แล้ว จะเห็นได้ว่ามี Private IP และ Public IP ได้ถูกจับคู่กันไว้แล้วและมี TCP/UDP Port ที่กำหนดไว้ด้วย ตามรูปที่ได้แสดงด้านล่าง

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 202.172.16.1:8080  172.16.1.11:80     ---                ---
tcp 202.172.16.1:50011 172.16.1.12:443    ---                ---
```

- ทดสอบการใช้งาน CCTV และ NAS จาก Internet เพื่อตรวจสอบการ Translate Port โดยการ Telnet จาก Router ที่จำลองเป็น Internet USER 1 เห็นได้ว่าสามารถใช้งาน CCTV และ NAS ได้ตาม TCP/UDP Port ที่ได้กำหนดไว้ และทำการตรวจสอบ NAT Table ที่ Router R1 ก็จะเห็นได้ว่ามีการ Translate TCP/UDP Port เกิดขึ้นเพื่อเข้าไปใช้งาน CCTV และ NAS ที่อยู่ใน Inside Network

```
USER_INTERNET#telnet 202.172.16.1 8080
Trying 202.172.16.1, 8080 ... Open


USER_INTERNET#telnet 202.172.16.1 50011
Trying 202.172.16.1, 50011 ... Open
```




```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 202.172.16.1:8080  172.16.1.11:80     202.172.16.5:11909 202.172.16.5:11909
tcp 202.172.16.1:8080  172.16.1.11:80     ---                ---
tcp 202.172.16.1:50011 172.16.1.12:443    202.172.16.5:59044 202.172.16.5:59044
tcp 202.172.16.1:50011 172.16.1.12:443    ---                ---
```

NAT ในรูปแบบ PAT มีประโยชน์ในการประหยัดใช้ IP Public ซึ่งสามารถใช้เพียง 1 Public IP ก็สามารถรองรับการใช้งาน User/Client ได้จำนวนมากในเวลาเดียวพร้อมๆ กัน โดยที่ PAT ได้นำ TCP/UDP Port ที่ทำงานใน Layer 4 มาแยกแยะ Session ด้วยการนำ TCP/UDP Port มาใช้งานนี้เองจึงมีประโยชน์ในการทำ Static PAT ด้วย อย่างเช่น ถ้าหากภายในบ้านมี CCTV หรือ NAS ก็เรียกใช้งานจากภายนอกได้ โดยที่ไม่ต้องเข้าไปหน้างาน หรือที่ตัวอุปกรณ์โดยตรง ถือเป็นการอำนวยความสะดวกสบายไปด้วย