

CNI2025 Lab04

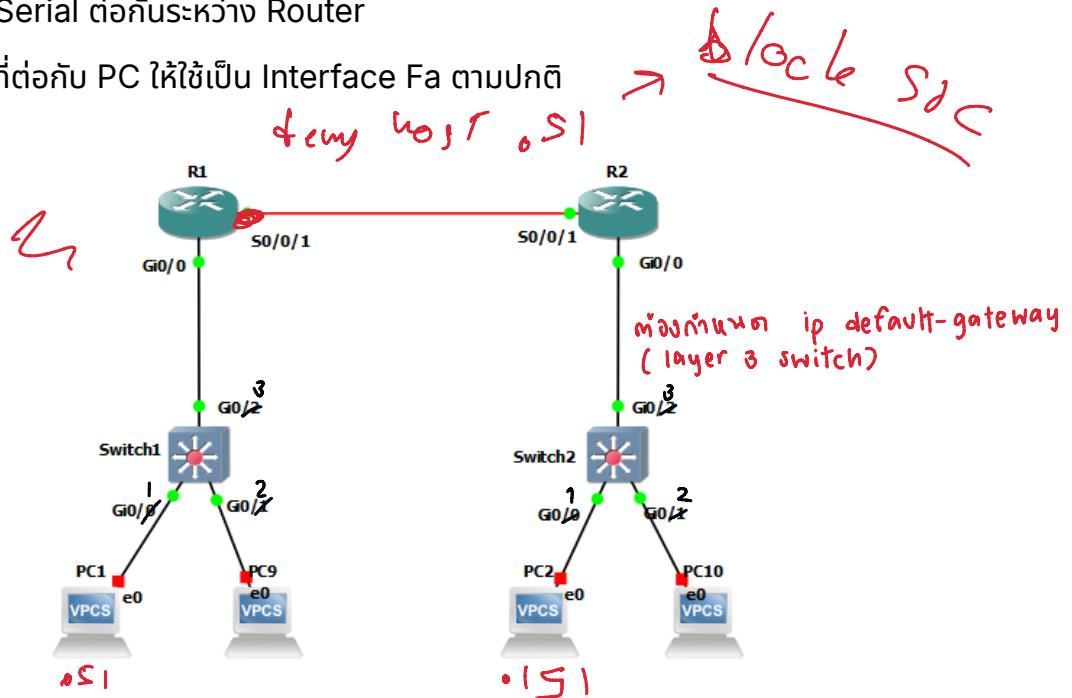
เลขกลุ่ม G =

เลขประจำตัว ชื่อ นามสกุล

Part 0

- ให้นักศึกษาแบ่งกลุ่ม ตามที่เคยแบ่งไว้ใน Lab01 โดยมีกึ่งหมดไม่เกิน 18 กลุ่ม กลุ่มละ 2-3 คน แต่ละกลุ่มจะมีค่ากลุ่ม G ตั้งแต่ 1-18 ให้ใส่เลขกลุ่ม G ที่ด้านบน
- อุปกรณ์ในห้อง Lab 306 มีกึ่งหมด 7 Rack ให้นักศึกษาใช้อุปกรณ์ตามที่ได้แบ่งไว้ใน Lab01
- แต่ละกลุ่ม (G) ให้ทำการเชื่อมต่อ Network Topology ดังรูป
 - โดยใช้ Switch 2 ตัว Router 2 ตัวและ PC 4 VM โดย PC1-2 จะเป็น Windows 11 และ PC9-10 จะเป็น Linux Ubuntu 24.04
 - Server ในแต่ละ Rack จะมี VM1-16 โดย VM1-8 เป็น Windows 11 และ VM9-16 เป็น Linux Ubuntu 24.04

- ในทุก VM ที่ใช้งาน ให้บันคึกษา เปิด (Disable) Network Adapter ที่เชื่อมต่อ กับ Internet (306) และให้เปิดใช้ (Enable) เอพะ Network Adapter ที่เชื่อมต่อ หมายัง อุปกรณ์เครือข่ายใน Rack เท่านั้น
- ให้ใช้สาย Serial ต่อ กับ ระหว่าง Router
- Switch ที่ต่อ กับ PC ให้ใช้เป็น Interface Fa ตามปกติ



4. ให้เข้าไปที่ Switch ทำการ Clear configuration ใน Switch และ reload Switch ก่อนเริ่ม กำ Lab

a. คำสั่ง `erase startup-config`

b. คำสั่ง `delete flash:vlan.dat`

c. คำสั่ง `reload`

5. ให้เข้าไปที่ Router ทำการ Clear configuration ใน Router และ reload Router ก่อนเริ่ม กำ Lab

a. คำสั่ง `erase startup-config`

b. คำสั่ง `reload`

6. ทำการตั้งค่า IP ให้กับ PC และ Switch

Device	IP Address
PC1	192.168.11.1/25
PC2	192.168.131.1/25
PC9	192.168.12.1/25
PC10	192.168.132.1/25

Switch1	192.168.0.126/25 (VLAN1)
Switch2	192.168.0.254/25 (VLAN1)

4. กำหนดการตั้งค่าให้ Switch สามารถที่จะ Telnet และ SSH ไปได้ผ่าน Line VTY โดยให้ตั้งชื่อ Hostname ว่า SG-1 โดย G คือ ลำดับกุ่บที่นักศึกษาได้ (เช่น G = 1 Hostname จะเป็น S1-1)

```
Switch>en
Switch#conf t
Switch(config)#host S1-1
S1-1(config)#
```

ทำการตั้งค่า RSA Key เพื่อเตรียมพร้อมสำหรับการ SSH

```
S1-1(config)#no ip domain lookup
S1-1(config)#ip domain name itkmitl.lab
S1-1(config)#ip ssh version 2
S1-1(config)#crypto key generate rsa modulus 2048
# ถ้าเป็น Switch C2950 Series ให้ใช้ modulus ที่น้อยที่สุด เพราะใช้เวลานาน
```

กำหนดการ + general-keygen

ทำการสร้าง User **admin** รหัสผ่าน **cisco** เพื่อ Login ผ่าน Line VTY

```
S1-1(config)#username admin privilege 15 secret cisco
S1-1(config)#line vty 0 8
S1-1(config-line)#login local
S1-1(config-line)#transport input telnet ssh
S1-1(config-line)#exec-timeout 0 0
S1-1(config-line)#logging synchronous
```

หากทำการตั้งค่าเสร็จสิ้นแล้วให้ทำการ Save Config ที่ได้ทำไป

```
S1-1#wr
```

และดำเนินการกับ **Switch 2** โดยใช้ชื่อเป็น **SG-2**

จากนั้นทำการทดสอบ Telnet SSH จาก PC ไปหา Switch

From	To	Result
PC1	Switch1	S

PC1	Switch2	F
PC2	Switch1	F
PC2	Switch2	S
PC9	Switch1	S
PC9	Switch2	F
PC10	Switch1	F
PC10	Switch2	S

8. ทำการตั้งค่าให้ Router สามารถที่จะ Telnet SSH ไปได้ผ่าน Line VTY โดยให้ตั้งชื่อ Hostname ว่า RG-1 โดย G คือ ลำดับกุ่มที่นักศึกษาได้ (เช่น G = 1 Hostname จะเป็น R1-1)

1. จากนั้นทำการตั้งค่า Interface ที่ต่อ กับ Switch ให้เป็น IP เมอร์แร์ของ Subnet ที่กำหนด ไป
2. ตั้งค่า RSA Key
3. ตั้งค่า Line VTY
4. สร้าง Username และ Save Config ที่กำไป
5. ทำแบบเดียวกันกับ Router ตัวที่ 2 โดยให้ตั้ง Hostname ว่า RG-2

จากนั้นทำการทดสอบ Telnet และ SSH จาก PC ไป Router

From	To	Result
PC1	Router1	S
PC1	Router2	F
PC2	Router1	F
PC2	Router2	S
PC9	Router1	S
PC9	Router2	F
PC10	Router1	F
PC10	Router2	S

Part 1 (DHCP)

- ทำการตั้งค่า IP ระหว่าง Router เป็น 30.6.0.0/30 โดยให้ Interface กี่ของ Router1 เป็น 30.6.0.1/30 และกี่ของ Router2 เป็น 30.6.0.2/30
- ทำการตั้งค่า Route เพื่อให้ Router ทั้ง 2 รู้จัก Network ทั้งหมด

```
R1-1(config)#ip route <Network ID> <Subnet Mask> 30.6.0.2
```

```
R1-2(config)#ip route <Network ID> <Subnet Mask> 30.6.0.1
```

- จากนั้นทำการทดสอบ Ping หา Device ทุกตัว

From	To	Expected Result	Result
PC1	PC9	Success	S
PC1	Switch1	Success	S
PC1	Router1	Success	S
PC1	Router1 (30.6.0.1)	Success	S
PC1	Router2 (30.6.0.2)	Success	S
PC1	Router2	Success	S
PC1	Switch2	Success	S
PC1	PC2	Success	S
PC1	PC10	Success	S
PC2	Switch1	Success	S
PC2	Router1	Success	S
PC2	Router1 (30.6.0.1)	Success	S
PC2	Router2 (30.6.0.2)	Success	S
PC2	Router2	Success	S
PC2	Switch2	Success	S
PC2	PC9	Success	S
PC2	PC10	Success	S
PC9	Switch1	Success	S
PC9	Router1	Success	S
PC9	Router1 (30.6.0.1)	Success	S
PC9	Router2 (30.6.0.2)	Success	S
PC9	Switch2	Success	S

PC9	PC10	Success	S
PC10	Switch1	Success	S
PC10	Router1	Success	S
PC10	Router1 (30.6.0.1)	Success	S
PC10	Router2 (30.6.0.2)	Success	S
PC10	Switch2	Success	S

หากไม่สามารถ Ping ได้ครบทั้งหมด ให้นักศึกษาทำการตรวจสอบ Firewall ของ End Device ว่าปิดแล้วหรือยัง และ Switch ทำการตั้งค่า Default Gateway แล้วหรือไม่

- ทำการตั้งค่า DHCP Server ที่ Router1 โดยชื่อว่า DHCP_LAN1

```
R1-1(config)#ip dhcp pool DHCP_LAN1
```

- ทำการกำหนดค่าต่าง ๆ ให้ DHCP

```
R1-1(dhcp-config)#domain-name itkmitl.lab
R1-1(dhcp-config)#network 192.168.1.0 255.255.255.128
R1-1(dhcp-config)#default-router 192.168.1.1
```

การกำหนด Domain Name คือ เมื่อมีการแจก DHCP PC ที่รับ DHCP จะได้รับ Domain ไปด้วย

คำสั่ง **network** หมายถึง การกำหนดว่า DHCP Pool นี้จะแจกถึงไหน

คำสั่ง **default-router** หมายถึง การกำหนดว่า Default Route ของ Network วงนี้คือ IP อะไร

- จากนั้นทำการ Exclude IP เพื่อให้แจกแค่ Range ที่กำหนดเท่านั้น โดยในที่นี้จะให้แจกแค่ เบอร์ที่ 50 ถึง 100 เท่านั้น

```
R1-1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.49
R1-1(config)#ip dhcp excluded-address 192.168.1.101 192.168.1.126
```

- จากนั้นทดสอบให้ PC ผ่าน Router1 รับ DHCP จาก Router

ตัวอย่างผลลัพธ์ที่ควรจะเป็น

Connection-specific DN...	itkmit.lab	2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP>
Description	Intel(R) PRO/1000 MT Network Conn	default qlen 1000
Physical Address	0C:CF:1B:D7:00:00	link/ether 0c:c4:57:a8:00:00 brd ff:ff:
DHCP Enabled	Yes	altname enp0s4
IPv4 Address	192.168.1.50	inet 192.168.1.51/25 brd 192.168.1.127
IPv4 Subnet Mask	255.255.255.128	s4
Lease Obtained	Thursday, December 4, 2025 4:24:49	
Lease Expires	Friday, December 5, 2025 4:24:48 PM	
IPv4 Default Gateway	192.168.1.1	
IPv4 DHCP Server	192.168.1.1	

8. จากนั้นทำการตั้งค่า DHCP Pool **DHCP_LAN2** สำหรับแจกให้กับ LAN ก่อตัว Router2 โดยให้แจกแค่ IP เบอร์ **150 - 200**

9. สังเกตผลลัพธ์ที่ได้ ก่อตัว Router2

10. คิดว่าเพราะเหตุใด PC ก่อตัว Router2 ยังไม่ได้รับ DHCP และมีวิธีแก้อย่างไร

11. ทดลอง Telnet และ SSH ทุก Device อีกครั้ง

12.	From	To	Result
	PC1	Switch1	失败
	PC1	Switch2	失败
	PC2	Switch1	失败
	PC2	Switch2	失败
	PC9	Switch1	失败
	PC9	Switch2	失败
	PC10	Switch1	失败
	PC10	Switch2	失败

From	To	Result
PC1	Router1	失败
PC1	Router2	失败
PC2	Router1	失败
PC2	Router2	失败
PC9	Router1	失败
PC9	Router2	失败
PC10	Router1	失败
PC10	Router2	失败

ต้อง Telnet, SSH ได้ทั้งหมดก่อน จึงจะเริ่มทำ Part 2

Part 2 (ACL)

1. ทำการตั้งค่า ACL (Access Control List) เพื่อให้เป็นไปตามข้อความต่อไปนี้

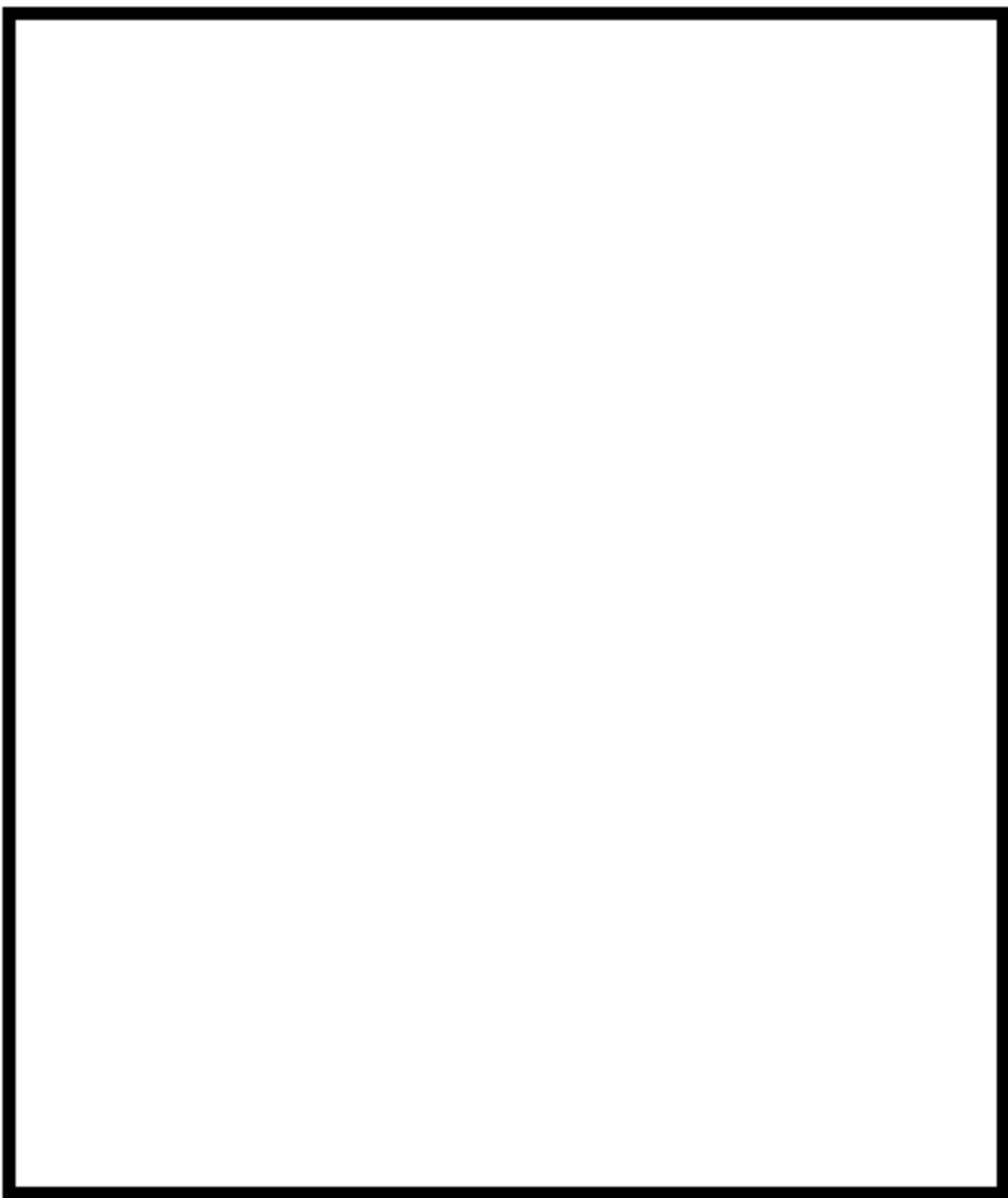
- a. **ไม่ให้** PC1 Ping ไปหา PC2 ได้
- b. ให้ PC2 Ping ไปหา PC1 ได้
- c. ให้ PC9 Ping ไปหา PC10 ได้
- d. **ไม่ให้** PC10 Ping ไปหา PC9 ได้
- e. ให้เฉพาะ PC1 PC9 สามารถ Telnet SSH ไปที่ Switch1 ได้เท่านั้น
- f. ให้เฉพาะ PC2 PC10 สามารถ Telnet SSH ไปที่ Switch2 ได้เท่านั้น
- g. ให้เฉพาะ PC2 PC10 สามารถ Telnet SSH ไปที่ Router1 ด้วย IP ที่อยู่ในวงเดียวกับ PC ได้เท่านั้น (IP 30.6.0.0/30 ไม่ควร Telnet SSH ไปได้)
- h. ให้เฉพาะ PC1 PC9 สามารถ Telnet SSH ไปที่ Router2 ด้วย IP ที่อยู่ในวงเดียวกับ PC ได้เท่านั้น (IP 30.6.0.0/30 ไม่ควร Telnet SSH ไปได้)

2. จากนั้นทำการบันทึกผลที่ได้ลงตาราง

From	To	Protocol	Result
PC1	PC2	ICMP	F
PC2	PC1	ICMP	S
PC9	PC10	ICMP	S
PC10	PC9	ICMP	F
PC1	Switch1	Telnet/SSH	S
PC9	Switch1	Telnet/SSH	S
PC2	Switch1	Telnet/SSH	F
PC10	Switch1	Telnet/SSH	F
PC2	Switch2	Telnet/SSH	S
PC10	Switch2	Telnet/SSH	S
PC1	Router1 (192.168.G.X/25)	Telnet/SSH	F

PC1	Router1	Telnet/SSH (30.6.0.1/30)	S
PC10	Router2	Telnet/SSH (192.168.G.X/25)	F
PC10	Router2	Telnet/SSH (30.6.0.2/30)	S

3. บันทึกคำสั่งที่ใช้ในการตั้งค่าให้ Switch และ Router ทำงานได้ตามที่กำหนด



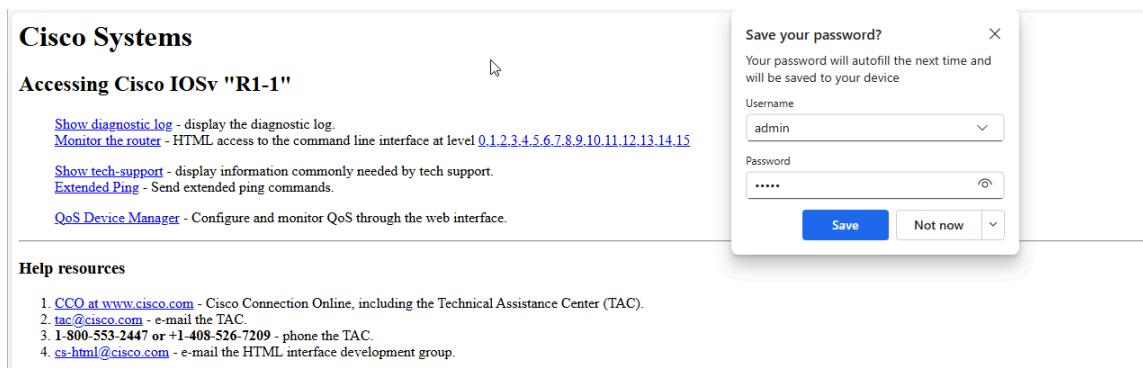
พื้นที่ขีดเขียนของไรก์ได้ (ແປກພາບ ເຂົ້າມຳອອັບຍາຍ)

4. ກຳການເປີດ HTTP Server ທີ່ Switch ແລະ Router

```
R1-1(config)#ip http server  
R1-1(config)#ip http authentication local  
---
```

```
S1-1(config)#ip http server  
S1-1(config)#ip http authentication local
```

การใช้คำสั่ง `ip http authentication local` หมายถึงให้ Login ด้วย Username ที่เราสร้างขึ้นมา เพื่อเข้าถึงเก่าบันจากนั้นกดลงเข้าด้วย IP ของ Router และ Switch เหล่านั้น ตัวอย่าง



Cisco Systems

Accessing Cisco IOSv "S1-1"

[Telnet](#) - to the router.
[Show interfaces](#) - display the status of the interfaces.
[Show diagnostic log](#) - display the diagnostic log.
[Monitor the router](#) - HTML access to the command line interface at level [0.1.2.3.4.5.6.7.8.9.10.11.12.13.14.15](#)
[Show tech-support](#) - display information commonly needed by tech support.
[Extended Ping](#) - Send extended ping commands.
[Web Console](#) - Manage the Switch through the web interface.

Help resources

- [CCO at www.cisco.com](#) - Cisco Connection Online, including the Technical Assistance Center (TAC).
- [tac@cisco.com](#) - e-mail the TAC.
- 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
- [cs-html@cisco.com](#) - e-mail the HTML interface development group.

5. ทำการเปิด HTTPS Server ที่ Switch และ Router

```
R1-1(config)#ip http secure-server  
---  
S1-1(config)#ip http secure-server
```

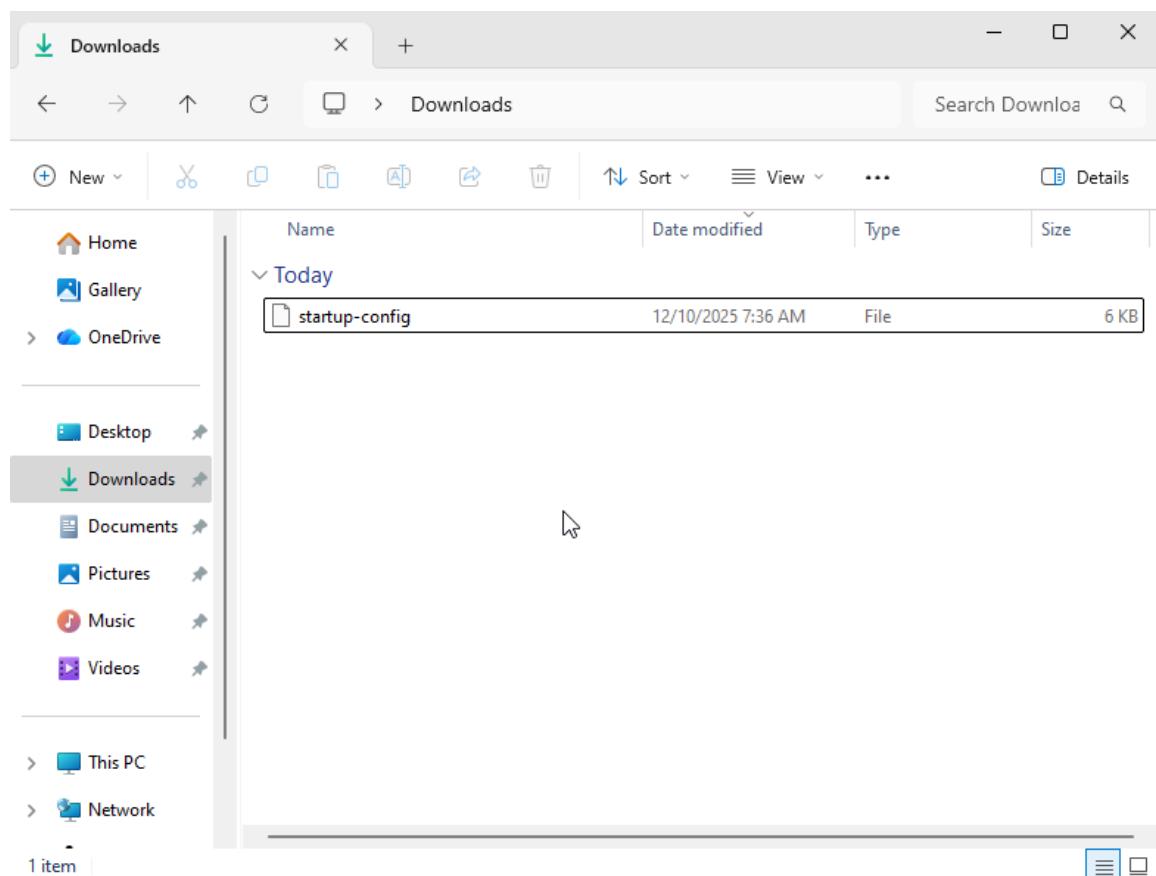
* **หมายเหตุ** หากกลุ่มได้ที่ได้ Switch Cisco C2950 Series จะมีข้อจำกัดอยู่ว่าจะไม่สามารถเปิด HTTPS Server ได้ ให้ข้ามไป

6. ทำการเปิด TFTP Server ที่ Switch และ Router เพื่อให้ Download startup-config ของอุปกรณ์ไปเก็บที่ Device ได้

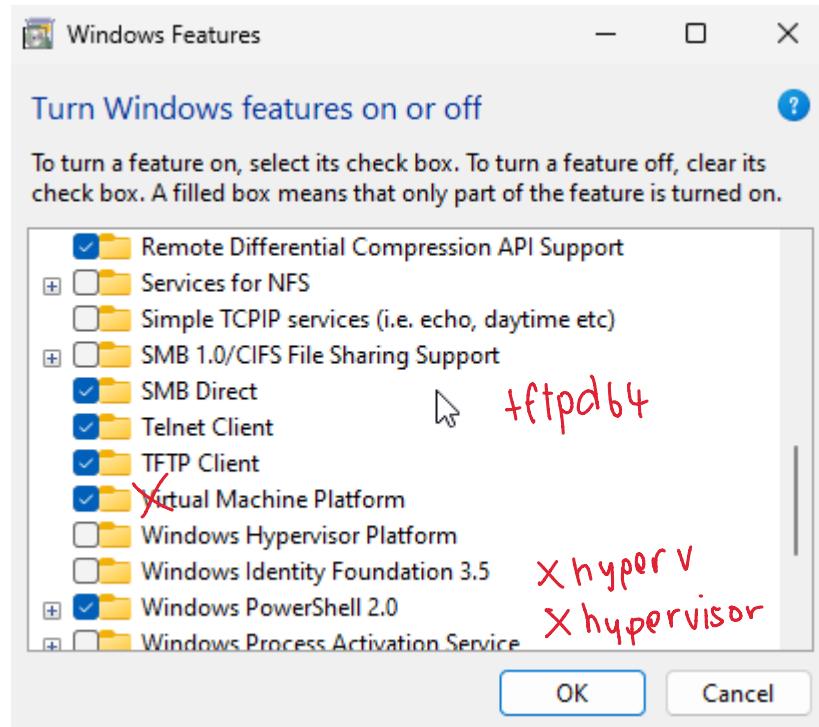
```
R1-1(config)#tftp-server nvram:startup-config
```

```
S1-1(config)#tftp-server nvram:startup-config
```

ตัวอย่าง



ที่ Windows สามารถ เปิด TFTP Client ได้โดยไม่ต้องโหลดอะไรเพิ่ม

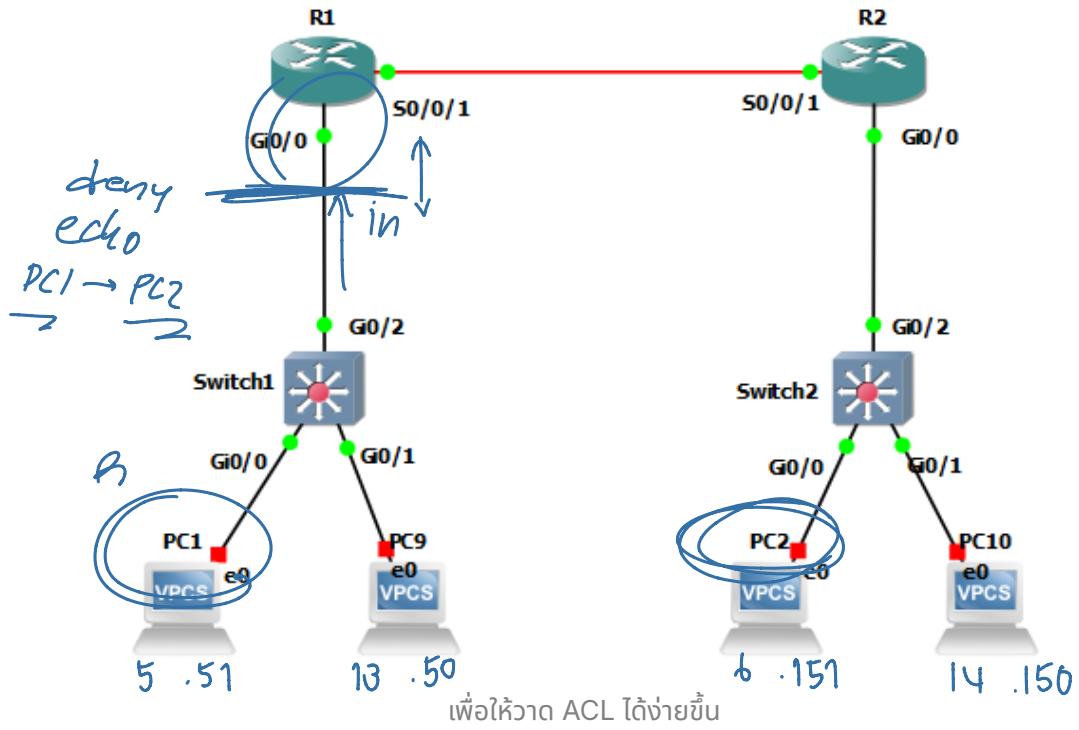


ให้ติ๊กแค่เฉพาะ TFTP Client เท่านั้น

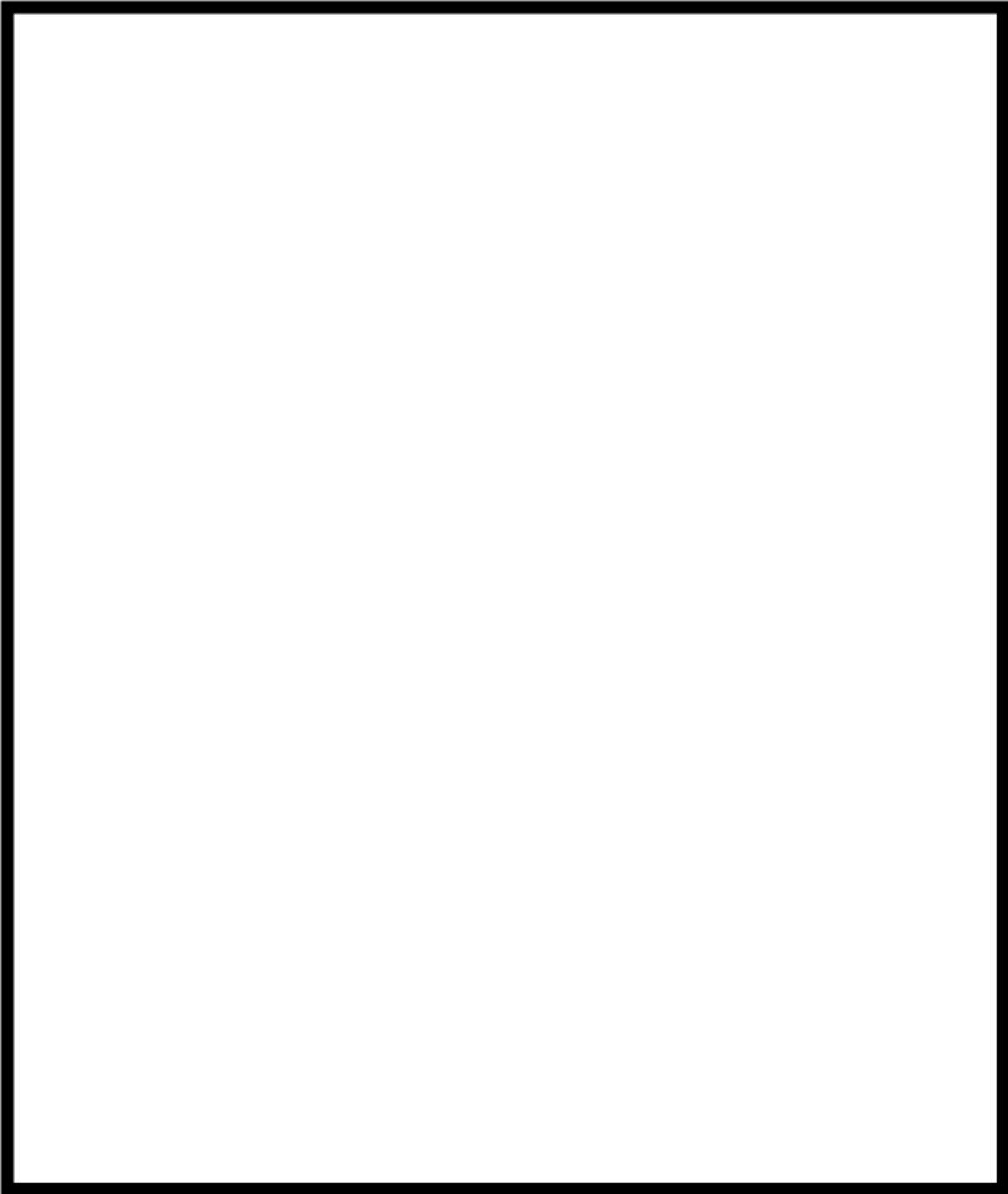
และในส่วนของ Linux Ubuntu จำเป็นต้องโหลด Client เพิ่มเติม

```
sudo apt update  
sudo apt install tftp-hpa
```

```
nat@nat:~$ ls  
Desktop  Downloads  Pictures  snap          Templates  
Documents  Music      Public    startup-config  Videos
```



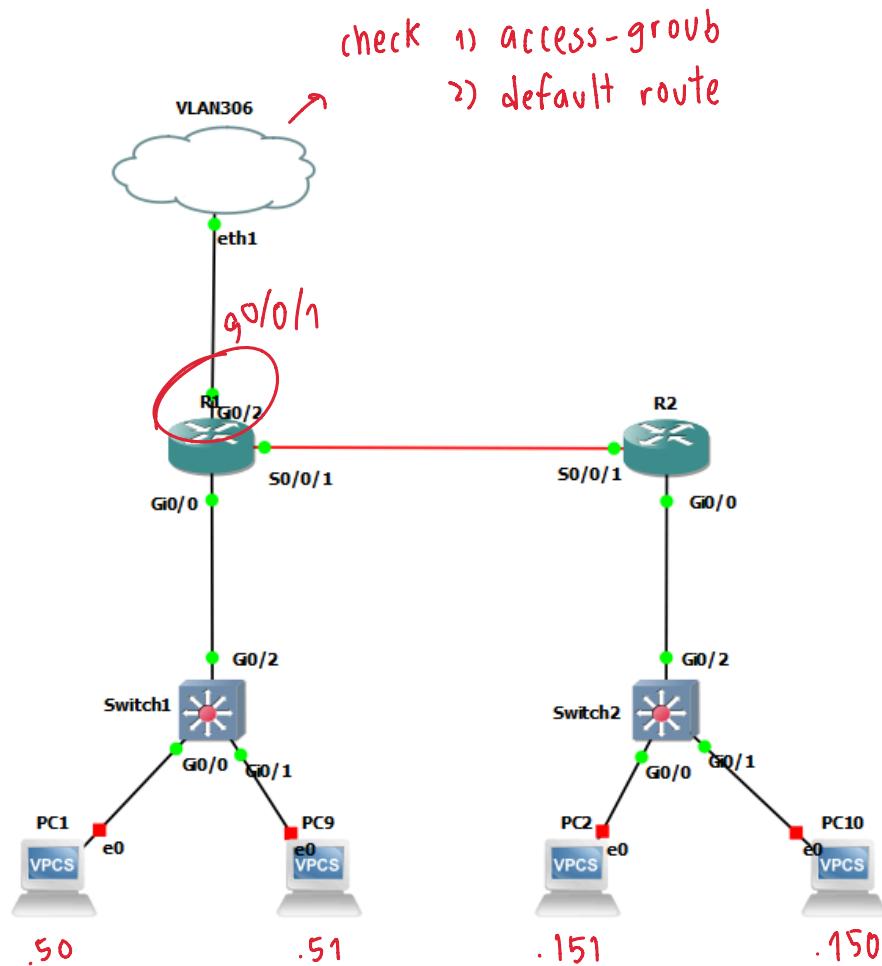
7. เมื่อเปิด HTTP HTTPS TFTP Server ที่ Switch และ Router และทุกตัวสามารถใช้งานได้ครบแล้ว ให้ตั้งค่า ACL ต่อไปนี้ (**กำต่อจากเดิม**)
 - a. ให้ PC1 สามารถเข้าถึงหน้าเว็บ (HTTP) ของ Router1 ได้เท่านั้น
 - b. ให้ PC2 สามารถเข้าถึงหน้าเว็บ (HTTPS) ของ Router2 ได้เท่านั้น
 - c. ให้ PC9 สามารถ TFTP ไปที่ Switch1 Router1 ได้เท่านั้น
 - d. ให้ PC10 สามารถ TFTP ไปที่ Switch2 Router2 ได้เท่านั้น
8. บันทึกภาพที่ได้จากการตั้งค่า ACL (ให้มีผลลัพธ์อันที่ไม่สำเร็จด้วย เช่น ข้อ a ให้กดลงใช้ PC2 หรืออื่น ๆ เพื่อทดสอบว่ามีแค่ PC1 จริง ๆ เท่านั้นที่ทำได้)



พื้นที่ขึ้นเขียนอะไร์ก์ได้ (ແປກພາບ ເຂົ້າມຳອອົງບາຍ)

Part 3 (NAT ແລະ Static NAT)

1. ກໍາການຕ່ວ Topology ເພີ່ມເຕີມ



Interface G0/2 ให้เปลี่ยนเป็น Interface กี่บักศึกษาใช้ต่อเข้ากับ VLAN306 จริง

2. ทำการตั้งค่า NAT Inside และ Outside

```
# Interface G0/0 and S0/0/1
R1-1(config-if)#ip nat inside
# Interface G0/2
R1-1(config-if)#ip nat outside
```

3. ตั้งค่าให้เข้ากับ VLAN306 รับ IP มาแบบ DHCP

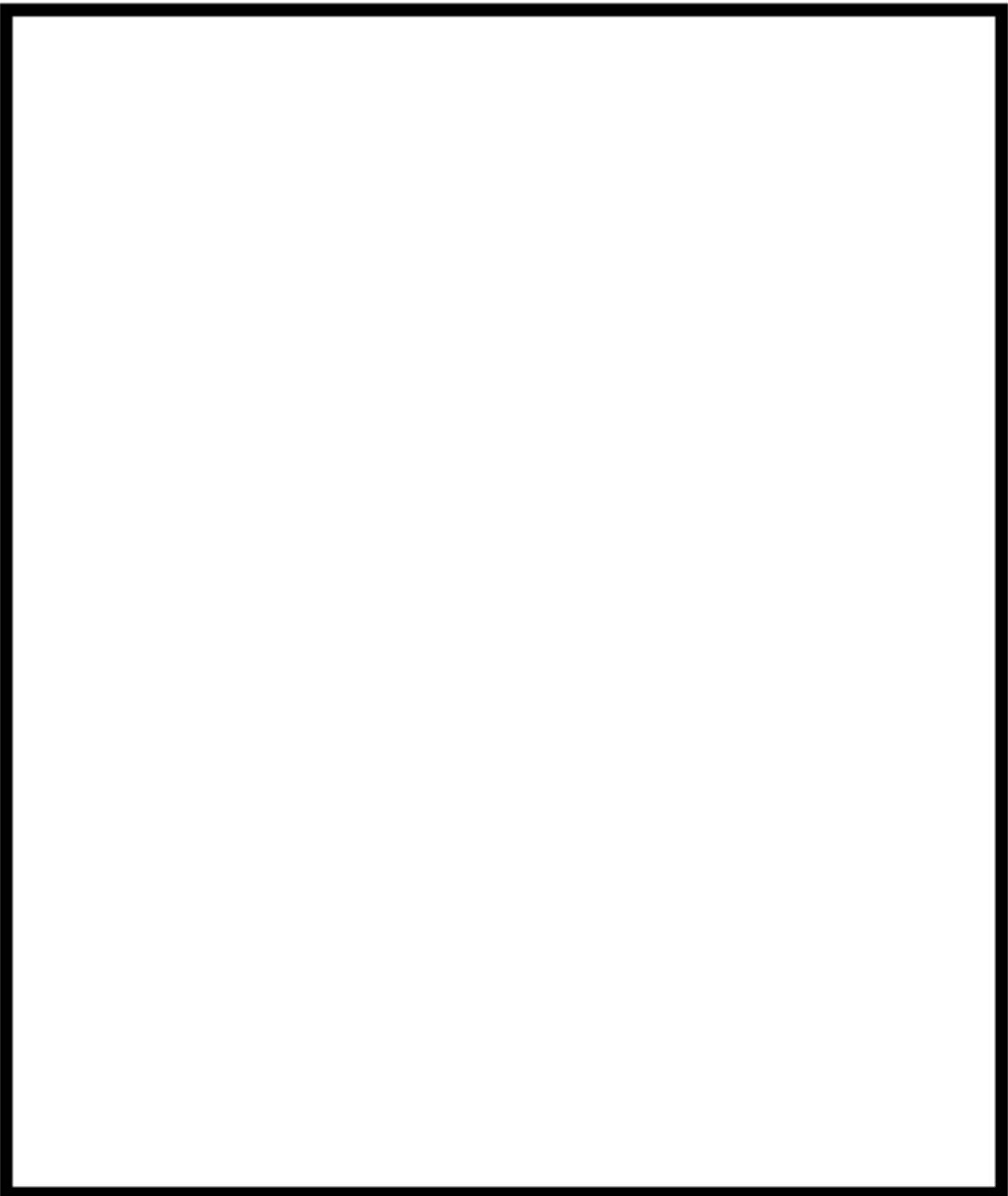
```
R1-1(config-if)#int g0/2
R1-1(config-if)#no shut
R1-1(config-if)#ip add dhcp 10.30.7.18
gateway 10.30.6.1
```

4. ทำการผูก Local IP ของ PC เข้ากับ IP ของห้อง 306 โดยในที่นี้ใช้ 4 เบอร์ 10.30.7.G, 10.30.7.50+G, 10.30.7.100+G, 10.30.7.150+G

```
R1-1(config)#ip nat inside source static <IP_PC1> <10.30.7.G>
R1-1(config)#ip nat inside source static <IP_PC2> <10.30.7.50+G>
```

```
R1-1(config)#ip nat inside source static <IP_PC9> <10.30.7.100+G>
R1-1(config)#ip nat inside source static <IP_PC10> <10.30.7.150+G>
```

5. ทดสอบ PC1 Ping → 8.8.8.8
6. ทดสอบ PC2 Ping → 1.1.1.1
7. ทดสอบ PC9 Ping → 8.8.4.4
8. ทดสอบ PC10 Ping → 208.67.222.222
9. ระหว่างที่กำลัง Ping ให้ใช้คำสั่ง `show ip nat translation` และ `show ip nat statistic`
10. บันทึกผลลัพธ์ที่สังเกตได้



พื้นที่ขดเดียบจะต้องได้ (ແປກພ ເຊຍນຄາວອິບາຍ)

Part 4 (NAT ແລະ Dynamic NAT)

1. ກໍາກາລບຄາສັ່ງທີ່ເປັນ Static NAT

```
R1-1(config)#no ip nat inside source static <IP_PC1> <10.30.7.G>
R1-1(config)#no ip nat inside source static <IP_PC2> <10.30.7.50+G>
R1-1(config)#no ip nat inside source static <IP_PC9> <10.30.7.100+G>
R1-1(config)#no ip nat inside source static <IP_PC10> <10.30.7.150+G>
```

2. ทำการตั้งค่า NAT Inside และ Outside

```
# Interface G0/0 and S0/0/1
R1-1(config-if)#ip nat inside
# Interface G0/2
R1-1(config-if)#ip nat outside
```

190-
192

3. ตั้งค่าให้ขาที่ต่อ กับ VLAN306

```
R1-1(config-if)#int g0/2
R1-1(config-if)#no shut
R1-1(config-if)#ip add 10.30.7.G 255.255.254.0
```

4. ทำการตั้งค่า Standard ACL สำหรับทั้ง 3 Network ที่ Router1

```
R1-1(config)#ip access-list standard ALLOW_NETWORK
R1-1(config-std-nacl)#permit 192.168.G.0 0.0.0.127
R1-1(config-std-nacl)#permit 192.168.G.128 0.0.0.127
R1-1(config-std-nacl)#permit 30.6.0.0 0.0.0.3
R1-1(config-std-nacl)#exit
```

5. ทำการสร้าง NAT Pool เป็น IP กี่ขา G0/2

```
R1-1(config)#ip nat pool DNAT 10.30.7.G 10.30.7.0 netmask 255.255.
254.0
```

27

6. ทำการผูก ACL กับ Pool เข้าด้วยกัน

```
R1-1(config)#ip nat inside source list ALLOW_NETWORK pool DNAT
```

7. ทำการตั้งค่า Default ออกไปที่ขา Interface G0/2 (จำกัด Router2 มา Router1 ด้วย)

```
R1-1(config)#ip route 0.0.0.0 0.0.0.0 10.30.6.1
```

8. ทดลองให้ PC1 Ping → 8.8.8.8 ค้างไว้

9. ทดลองให้ PC10 Ping → 1.1.1.1

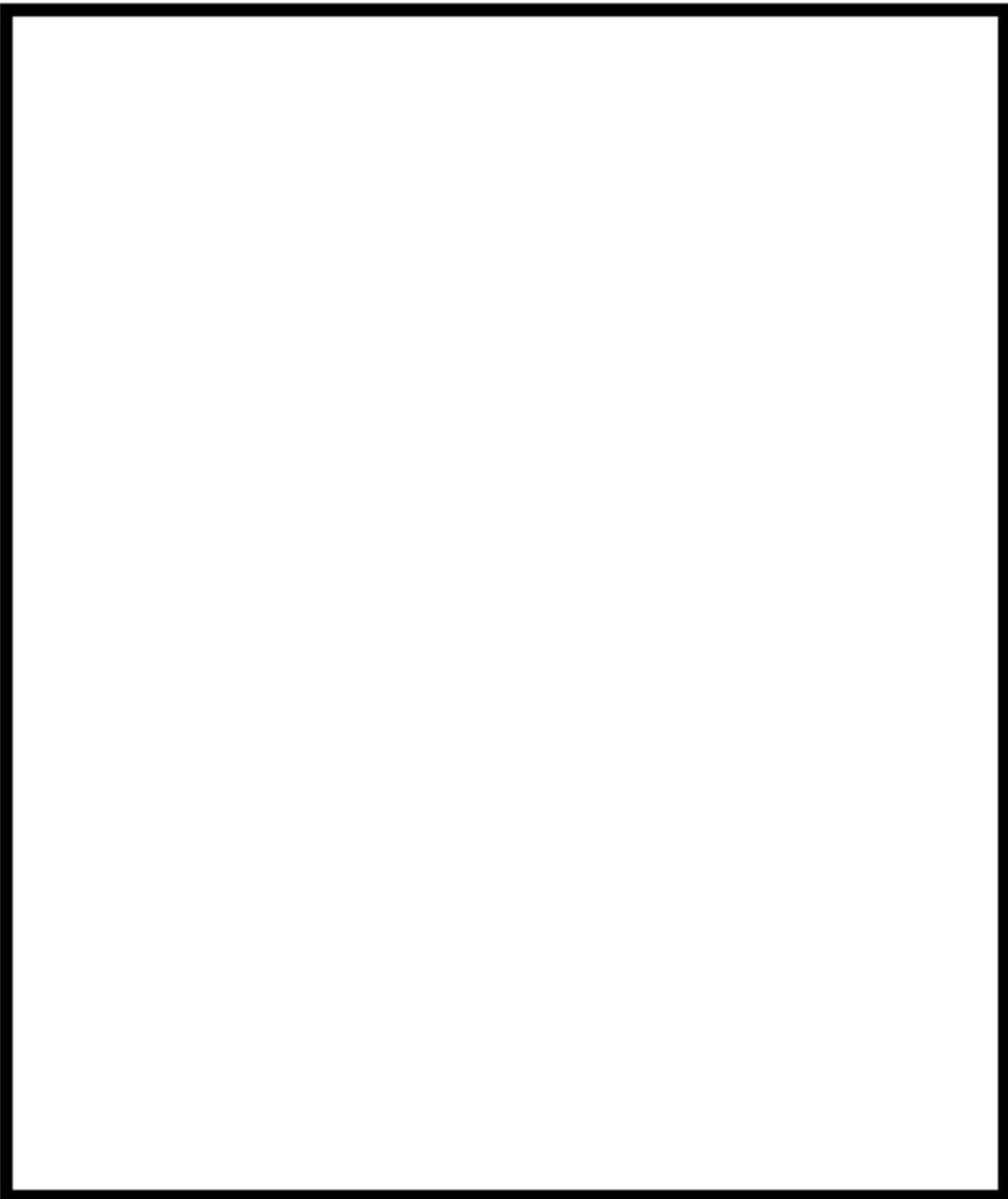
10. ทำการ Clear address translation

```
R1-1(config)#do clear ip nat translation *
```

จากนั้นทดลอง PC10 Ping → 1.1.1.1 อีกครั้ง

จากนั้นที่ Router1 ให้ใช้คำสั่ง `show ip nat translations`

11. บันทึกผลลัพธ์ที่ได้จากข้อ 8 9 และ 10 และอธิบายสิ่งที่สังเกตได้จากการทำ



พื้นที่ขดเขียนบนอะโกร์กิโต้ (ແປກພ ເຂັ້ມງານຄໍາອອິບາຍ)

Part 5 (PAT)

1. จาก Part ก່າວທີ່ໄດ້ກົດລອງ ດ້ວຍ DNAT ໃນ Part ນີ້ຈະລອງດ້ວຍ PAT (Port Address Translation)
ຢູ່ຈະ shut ຖຸກວຸນທີ່ config ກ່ອນໜີ້
2. ກໍາກາຣລບກງູກທີ່ຕັ້ງຄ່າໃນ Part ກ່າວອອກ

```
R1-1(config)#no ip nat inside source list ALLOW_NETWORK pool DNAT
```

3. เปลี่ยนการผูก ACL จาก Pool เป็น Interface แทน

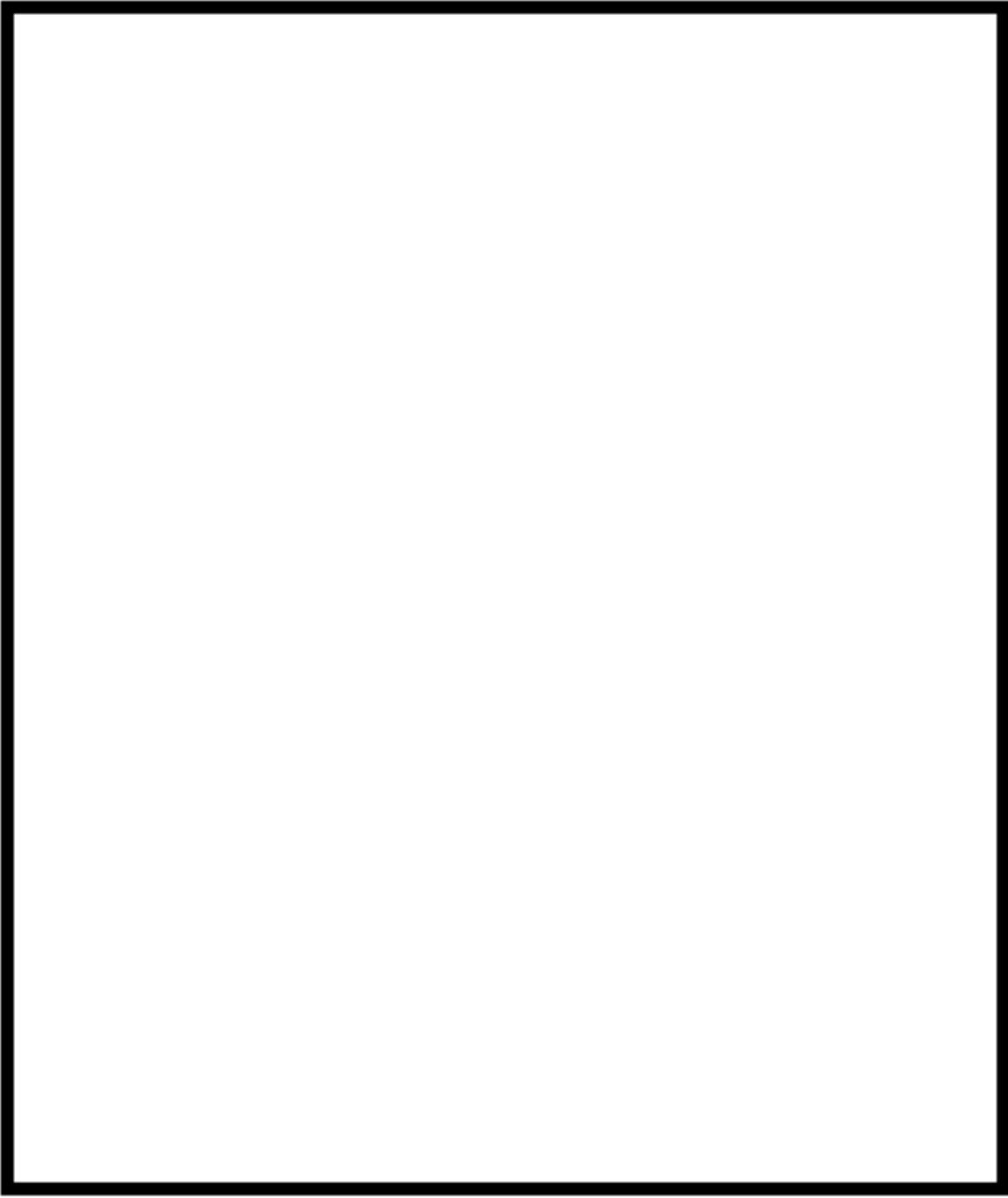
```
R1-1(config)#ip nat inside source list ALLOW_NETWORK interface g0/2  
overload
```

4. ทดสอบ PC1 Ping → 8.8.8.8 ค้างไว้

5. ทดสอบ PC10 Ping → 1.1.1.1

6. ใช้คำสั่ง `show ip nat translations`

7. บันทึกผลลัพธ์ที่ลังเกตได้และอธิบายความต่างระหว่าง Static NAT, DNAT และ PAT



พื้นที่ขีดเขียนของไรก์ได้ (แปะภาพ เขียนคำอธิบาย)

Part 6

- เมื่อทำ Lab เสร็จแล้ว ก่อนออกจากห้อง Lab ให้เก็บอุปกรณ์ เช่นสาย LAN และสายอื่นๆ ให้เรียบร้อย
- Shutdown VM ของตนเองใน Server และอย่าลืมปิดเครื่องคอมพิวเตอร์ก่อตัวของตนเอง

3. หากเป็นกลุ่มสุดท้ายที่ใช้ Rack ให้ปิด Server ที่ Rack ปิดอุปกรณ์เครือข่ายใน Rack ให้หมด และปิด UPS ที่ Rack ตามลำดับ
4. โดยปกติจะมี TA อยู่ด้วย แต่หากใช้ห้อง Lab เป็นคนสุดท้ายให้ปิดไฟ เครื่องปรับอากาศ ปิด UPS ที่ตู้ Rack ด้านหลังห้อง และปิด Breaker ที่หลังห้อง และ Lock ห้องกั้งประตูด้านหน้า และประตูด้านหลังให้เรียบร้อยด้วย