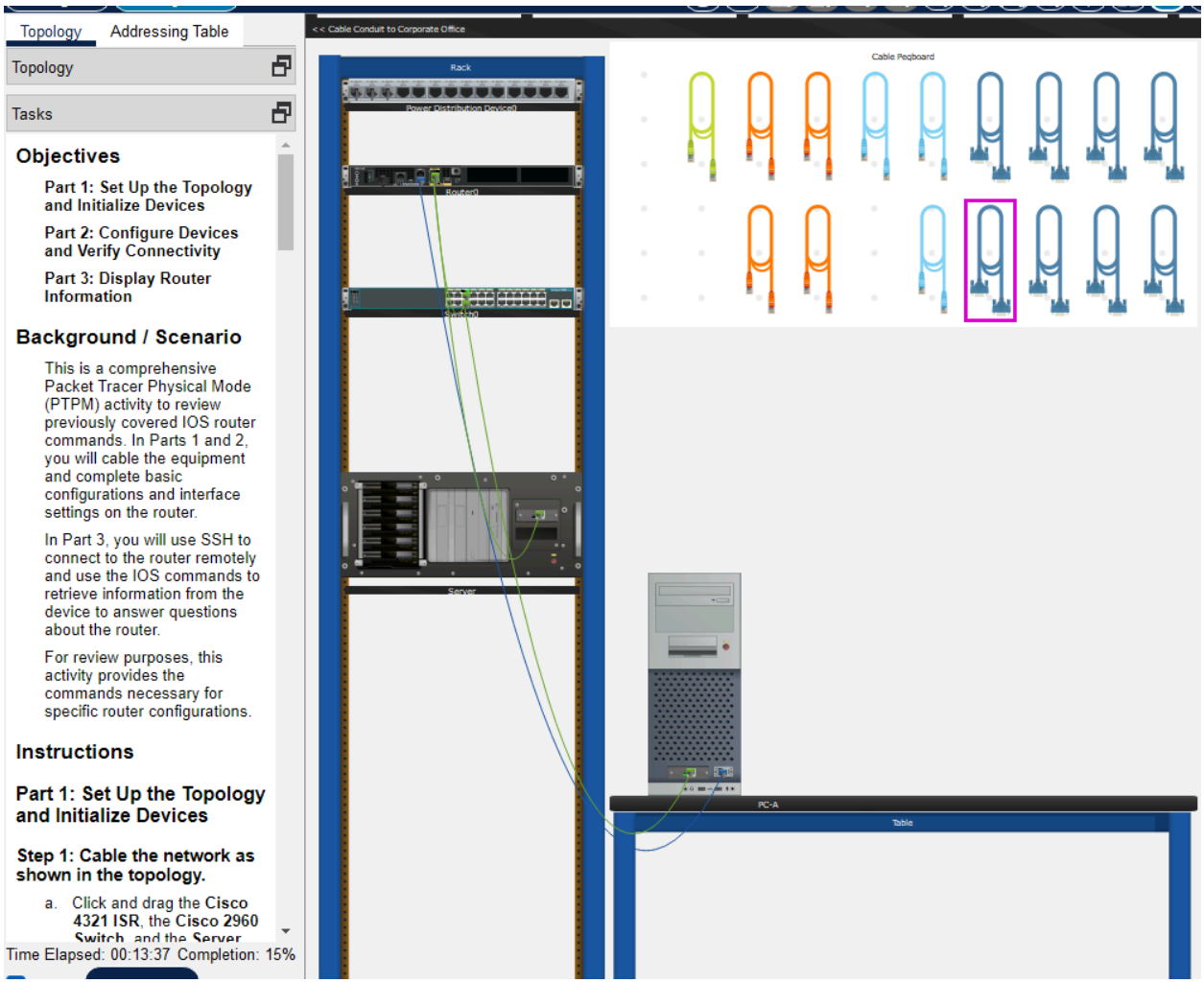
Part 1: ตั้งค่าแผนผังเครือข่าย (Topology) และเปิดใช้งานอุปกรณ์

Step 1: เชื่อมต่อสายตามที่กำหนด

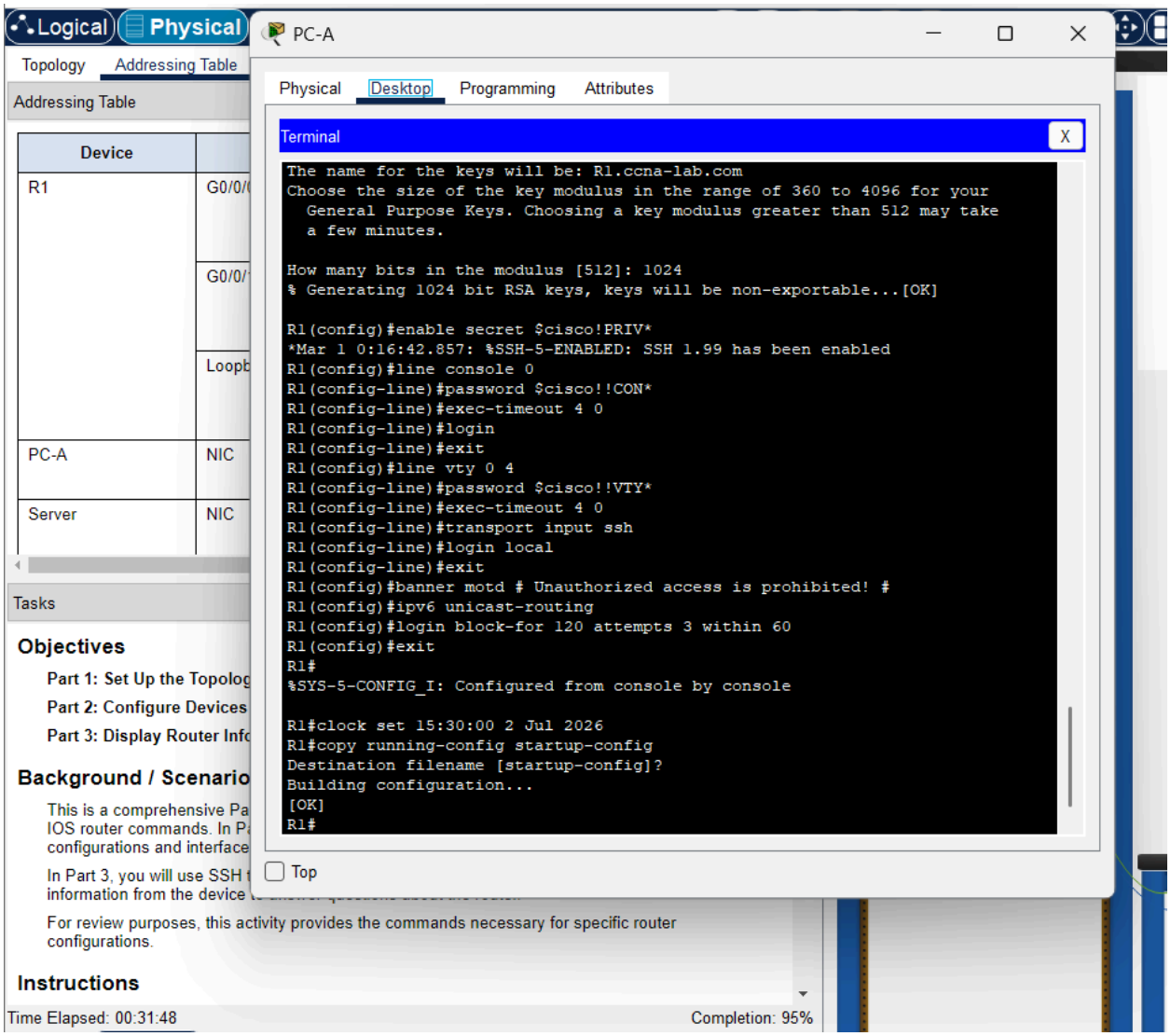


Part 2: กำหนดค่าอุปกรณ์ (Configuration) และทดสอบการเชื่อมต่อ

Step 1: ตั้งค่าอินเทอร์เฟซของคอมพิวเตอร์

- **a.** ตั้งค่า IP address, subnet mask และ default gateway ให้กับ **PC-A**
- **b.** ตั้งค่า IP address, subnet mask และ default gateway ให้กับ **Server** *(หมายเหตุ: ดูค่าต่าง ๆ ได้จากตาราง Addressing Table ในใบงานหลักของคุณ)*

Step 2: ตั้งค่าเร้าเตอร์ (Router)

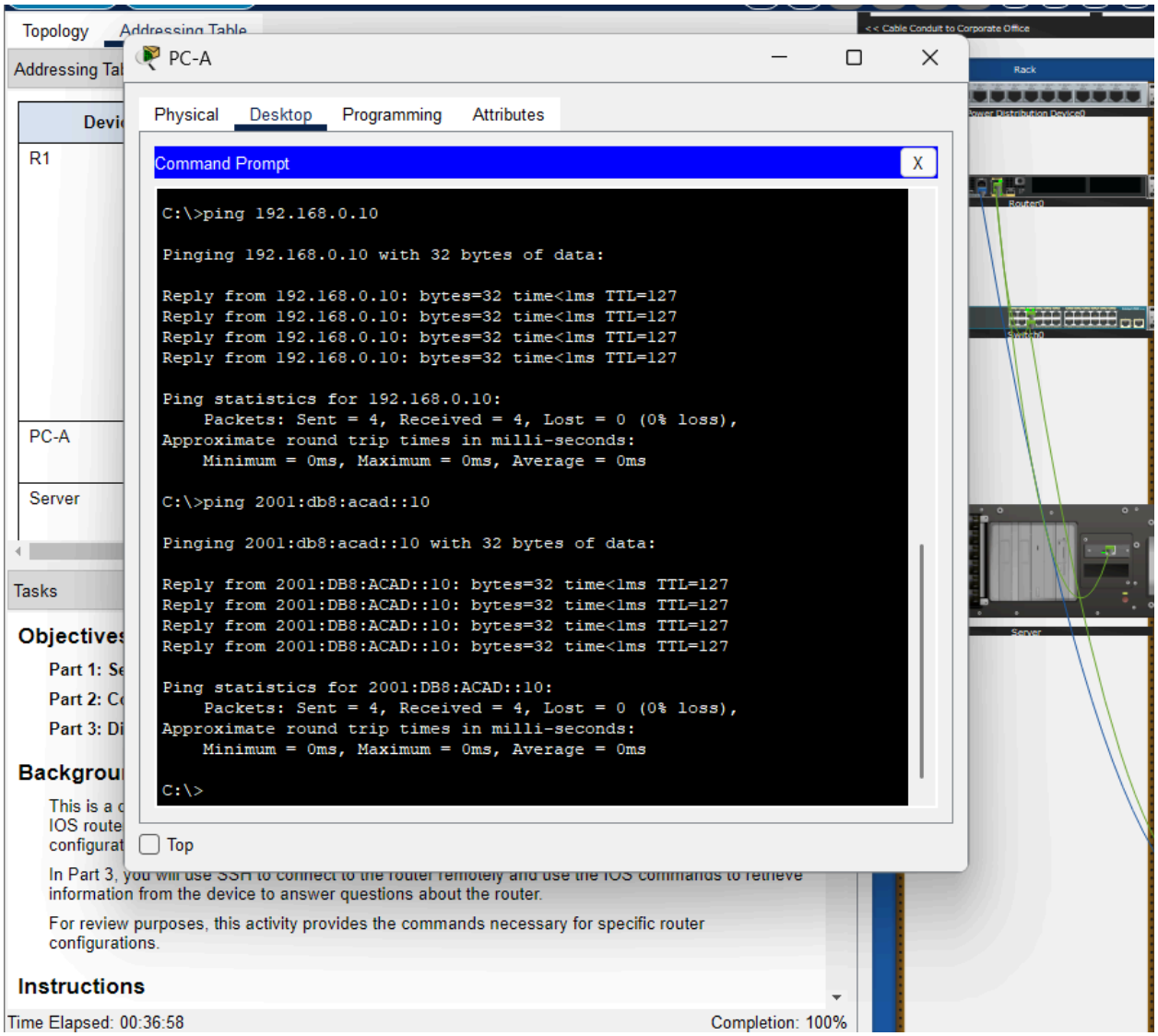


คำถามท้ายหัวข้อ: จะเกิดอะไรขึ้นหากสั่งรีโหลด (Restart) เร้าเตอร์ก่อนที่จะทำคำสั่งบันทึก `copy running-config startup-config`?

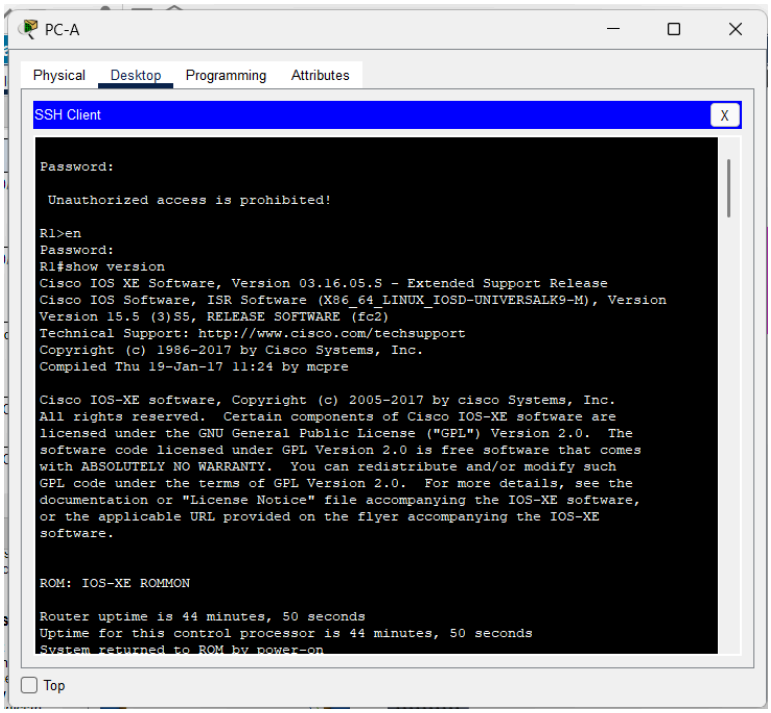
คำตอบ: ค่าคอนฟิกทั้งหมดที่เราพิมพ์ตั้งค่าไว้ก่อนหน้านี้จะหายไปทั้งหมด และเร้าเตอร์จะกลับไปเป็นสถานะว่างเปล่าเหมือนตอนเปิดเครื่องครั้งแรก เพราะค่าที่ตั้งไว้ยังอยู่ใน RAM (Running-config) ไม่ถูกย้ายไปเก็บใน NVRAM (Startup-config)

Step 3: ตรวจสอบการเชื่อมต่อเครือข่าย

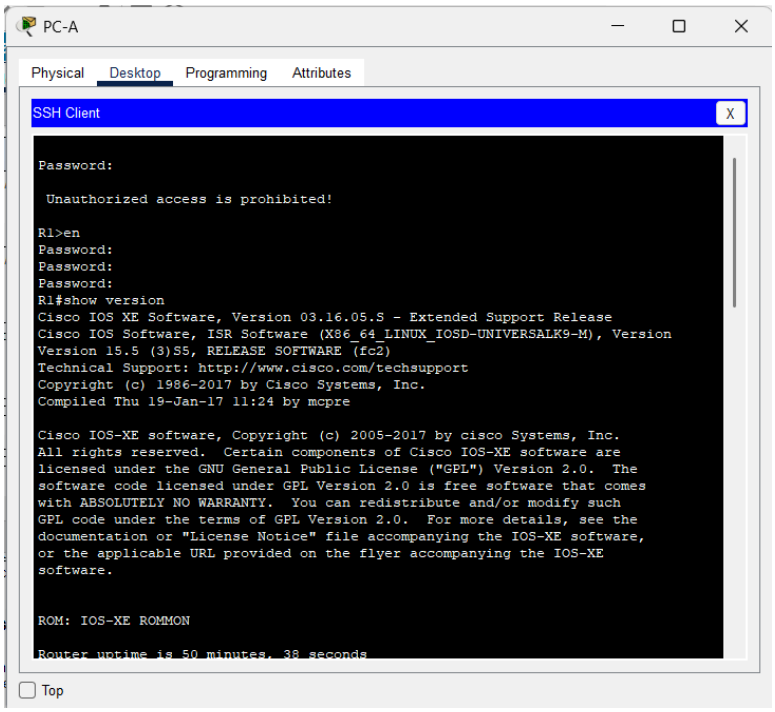
- **a.** ใช้ Command Prompt ที่ PC-A ลอง **ping** ไปยังหมายเลข IPv4 และ IPv6 ของ Server (บันทึกผลว่าสำเร็จหรือไม่)



- **b.** ใช้โปรแกรม Telnet / SSH client บน PC-A เชื่อมต่อ SSH ไปยังหมายเลข IPv4 ของอินเทอร์เฟซ Loopback บนเร้าเตอร์ R1 โดยใช้ Username: `SSHadmin` และ Password: `55Hadm!n2020` (บันทึกผลว่าสำเร็จหรือไม่)



- **c.** ทำแบบข้อ b. แต่เปลี่ยนเป็นเชื่อมต่อผ่านหมายเลข IPv6 (บันทึกผลว่าสำเร็จหรือไม่)



คำถามท้ายหัวข้อ: ทำไมโพรโทคอล Telnet ถึงถูกมองว่าเป็นความเสี่ยงทางด้านความปลอดภัย?

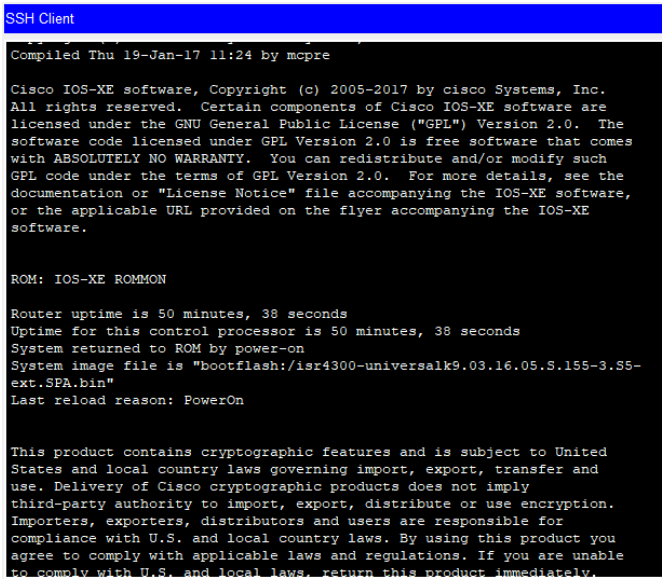
คำตอบ:

- **ส่งข้อมูลแบบ Plaintext (ข้อความธรรมดา):** ข้อมูลทุกอย่างที่คุณพิมพ์ ไม่ว่าจะเป็น **Username, Password** หรือคำสั่งควบคุมอุปกรณ์ จะถูกส่งไปบนสายสัญญาณเป็นข้อความดิบ ๆ ตรง ๆ
- **เสี่ยงต่อการโดนดักฟัง (Sniffing):** หากมีผู้ไม่หวังดีอยู่ในเครือข่ายทางผ่าน และใช้โปรแกรมดักจับแพ็กเก็ต (เช่น Wireshark) เขาจะสามารถอ่านรหัสผ่านและข้อความทั้งหมดที่คุณพิมพ์คุยกับเร้าเตอร์ได้ทันทีโดยไม่ต้องถอดรหัสเลยครับ
- **ขาดการตรวจสอบความถูกต้อง (No Authentication/Integrity Check):** ตัวโพรโทคอลไม่มีกลไกป้องกันการปลอมแปลงข้อมูลระหว่างทาง ทำให้เสี่ยงต่อการถูกโจมตีแบบ Man-in-the-Middle (MitM)

Part 3: แสดงข้อมูลของเร้าเตอร์ (Display Router Information)

ในส่วนนี้ให้ใช้คำสั่งประเภท *`show`* ต่าง ๆ ผ่านเซสชัน *SSH* เพื่อตรวจสอบข้อมูลและตอบคำถามในใบงานดังนี้*:*

- **Step 1:** เปิดเซสชัน SSH จาก PC-A ไปยัง R1 ด้วย IPv6
- **Step 2:** ใช้คำสั่ง `show version` เพื่อตอบคำถามเกี่ยวกับ ชื่อไฟล์อิมเมจของ IOS, ขนาดของ NVRAM และขนาดของ Flash memory นอกจากนี้ให้ใช้คำสั่งแบบฟิลเตอร์ `show version | include register` เพื่อตอบคำถามว่าเร้าเตอร์จะบูตอย่างไรในการเปิดเครื่องครั้งถัดไปหากค่าคอนฟิกูเรชันรีจิสเตอร์เป็น `0x2142`?



```
uck9
cme - srst
cube


Technology Package License Information:

-----------------------------------------------------------------------
Technology    Technology-package                  Technology-package
              Current             Type            Next reboot
-----------------------------------------------------------------------
appxk9          None             None             None
uck9            None             None             None
securityk9      securityk9       Permanent        securityk9
ipbase          ipbasek9         Permanent        ipbasek9
security        securityk9       Permanent        securityk9
ipbase          ipbasek9         Permanent        ipbasek9

cisco ISR4321/K9 (1RU) processor with 1687137K/6147K bytes of memory.
Processor board ID FLM2041W2HD
2 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3223551K bytes of flash memory at bootflash:.


Configuration register is 0x2102
```

```
R1#show version | include register
Configuration register is 0x2102
```

- **Step 3:** ใช้คำสั่ง `show startup-config` เพื่อดูว่ารหัสผ่านถูกแสดงผลอย่างไรในเอาต์พุต และใช้คำสั่ง `show running-config | section vty` เพื่อบันทึกผลลัพธ์ที่ได้

```
R1#show startup-config
Using 1519 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 12
!
hostname R1
!
login block-for 120 attempts 3 within 60
!
!
enable secret 5 $1$mERr$2q6B19eTeuK92k7m8Bhgz/
!
!
!
!
!
!
ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
!
username SSHadmin secret 5 $1$mERr$fuFUxOtVJZMfnQOcoB7vt/
```

```
R1#show running-config | section vty
line vty 0 4
 exec-timeout 4 0
 password 7 08654F471A1A0A56533D383D60
 login local
 transport input ssh
```

- **Step 4:** ใช้คำสั่ง `show ip route` เพื่อระบุว่าโค้ด (Code) ใดในตารางเส้นทางที่หมายถึงเครือข่ายที่เชื่อมต่อโดยตรง และมีเส้นทางที่ขึ้นต้นด้วยโค้ด **C** ทั้งหมดกี่รายการ

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.0/24 is directly connected, Loopback0
L       10.0.0.1/32 is directly connected, Loopback0
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.0.1/32 is directly connected, GigabitEthernet0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
```

- **Step 5:** ใช้คำสั่งสรุปพอร์ต เช่น `show ip interface brief` และ `show ipv6 int brief` เพื่อตอบคำถามเกี่ยวกับสถานะพอร์ต ความหมายของ `[up/up]` และเปลี่ยนค่าของ Server ให้รับ IPv6 อัตโนมัติ (ไม่ใช่ Static) แล้วใช้คำสั่ง `ipconfig` บน Server เพื่อบันทึก IP, Default gateway รวมถึงทดสอบ ping

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.0.1     YES manual up                    up
GigabitEthernet0/0/1   192.168.1.1     YES manual up                    up
Loopback0              10.0.0.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

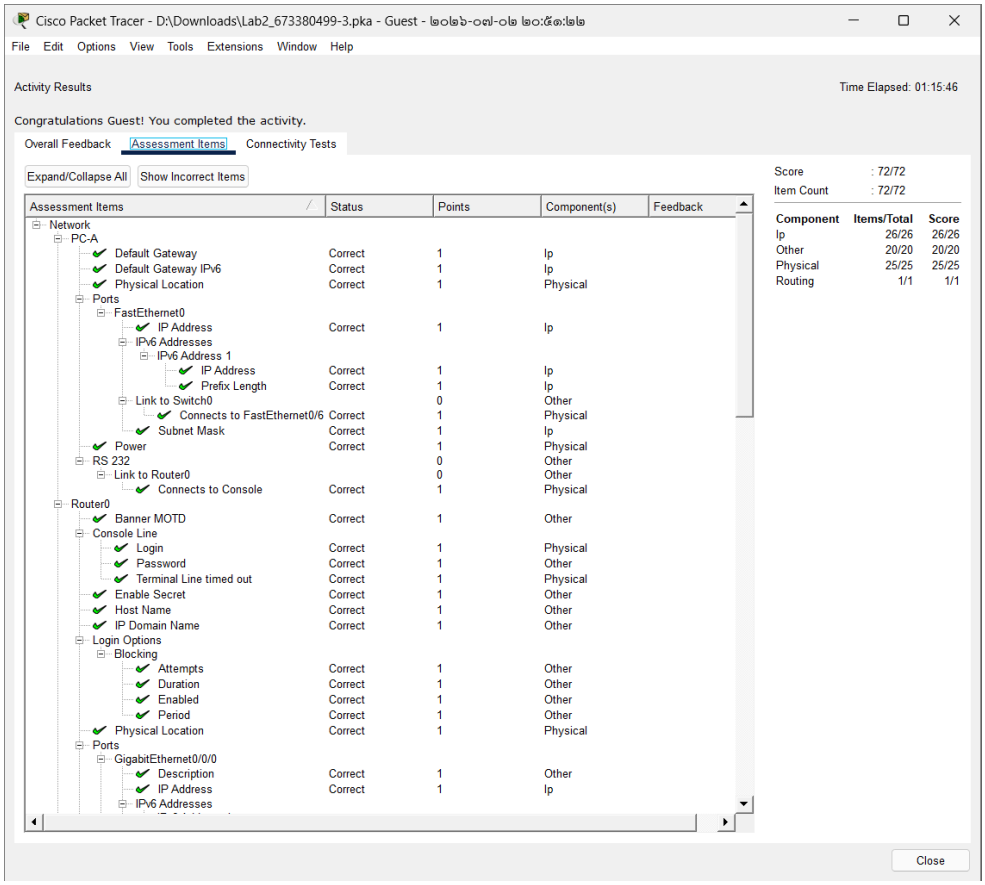
```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.0.1     YES manual up                    up
GigabitEthernet0/0/1   192.168.1.1     YES manual up                    up
Loopback0              10.0.0.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R1#show ipv6 int brief
GigabitEthernet0/0/0       [up/up]
    FE80::1
    2001:DB8:ACAD::1
GigabitEthernet0/0/1       [up/up]
    FE80::1
    2001:DB8:ACAD:1::1
Loopback0                  [up/up]
    FE80::1
    2001:DB8:ACAD:2::1
Vlan1                      [administratively down/down]
    unassigned
```

Reflection Questions (คำถามท้ายบทเรียน)

1. ในการตรวจสอบปัญหาการเชื่อมต่อเครือข่าย หากช่างเทคนิคสงสัยว่า**มีอินเทอร์เฟซ (พอร์ต) บางตัวไม่ได้เปิดใช้งาน** ควรใช้คำสั่ง `show` ใดเพื่อค้นหาปัญหานี้?

   คำตอบ: show ip interface brief หรือ show ipv6 interface brief สำหรับเวอร์ชัน IPv6

   คำสั่งนี้จะแสดงตารางสรุปพอร์ตทั้งหมดอย่างย่อ ทำให้ช่างเทคนิคเห็นสถานะได้อย่างรวดเร็วในบรรทัดเดียว หากพอร์ตไหนไม่ได้เปิดใช้งาน (ไม่ได้พิมพ์ `no shutdown`) สถานะจะโชว์ชัดเจนว่าเป็น **"administratively down"**

2. ในการตรวจสอบปัญหาการเชื่อมต่อเครือข่าย หากช่างเทคนิคสงสัยว่า**มีการตั้งค่า Subnet Mask ของอินเทอร์เฟซผิดพลาด** ควรใช้คำสั่ง `show` ใดเพื่อค้นหาปัญหานี้?

   คำตอบ: show running-config เจาะจงเฉพาะพอร์ตได้ด้วยคำสั่ง เช่น `show running-config interface g0/0/0` หรือใช้คำสั่ง `show ip interface` เพื่อดูรายละเอียดแบบเต็ม) เนื่องจากการดูแบบย่อ (interface brief) จะโชว์แค่หมายเลข IP แต่**ไม่แสดง Subnet Mask** ดังนั้น ช่างเทคนิคจึงจำเป็นต้องใช้คำสั่ง `show running-config` เพื่อเข้าไปดูการตั้งค่าที่เปิดใช้งานอยู่จริงในพอร์ตนั้น ๆ ซึ่งจะแสดงหมายเลข IP ควบคู่กับ Subnet Mask (เช่น `ip address 192.168.1.1 255.255.255.0`) ทำให้ตรวจเช็กความถูกต้องได้แม่นยำ