

2024-08-20

네트워크

VPN

# VPN

방화벽, 침입 탐지 시스템과 함께 사용되는 가장 일반적인 보안솔루션

VPN은 한달에 3만원으로 이용할 수 있는 인터넷 회선을 임대 회선처럼 사용할 수 있게 해주는 솔루션

이를 위해서는 VPN이 임대회선과 비슷한 수준의 기밀성을 제공해야 하는데 여기에는 암호화가 필요

VPN에서 사용하는 암호화 프로토콜에는 PPTP,L2TF,IPSec,SSL 등이 있다

# VPN의 용도

## 1. 해외여행을 하면서 국내 게임 서버 이용

대부분의 온라인 게임은 그 나라 의 IP 주소만 사용해 접속 가능

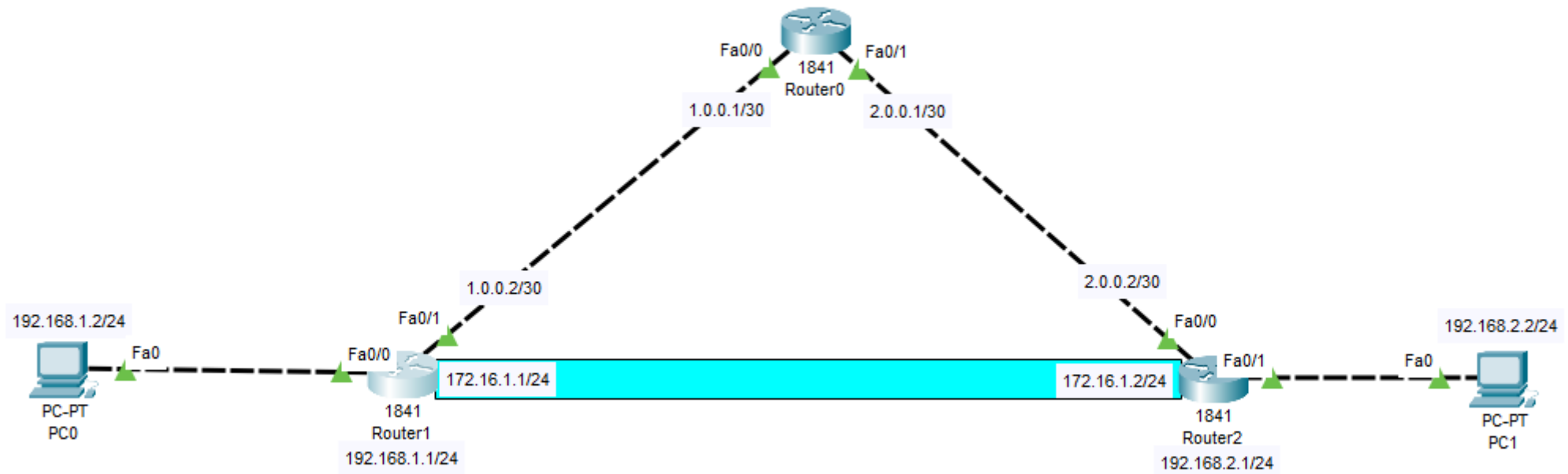
국내에 VPN 장비를 마련해두면 VPN 장비에 접속해 국내 IP 주소를 할당 받아 국내 게임 서버에 접근 가능

## 2. 집에서도 회사 내의 서버에 보안 상태로 접근

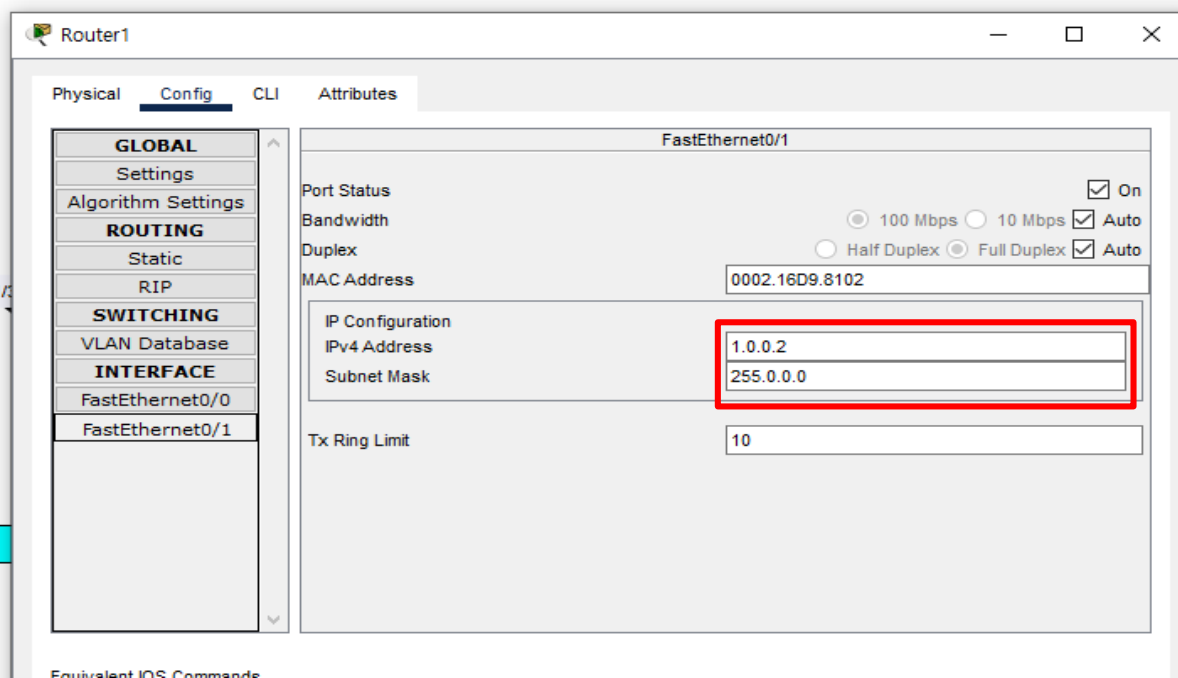
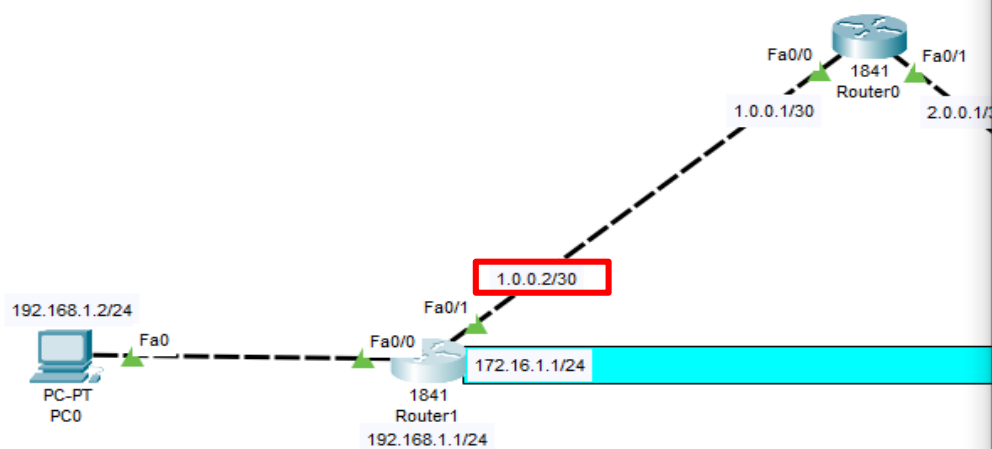
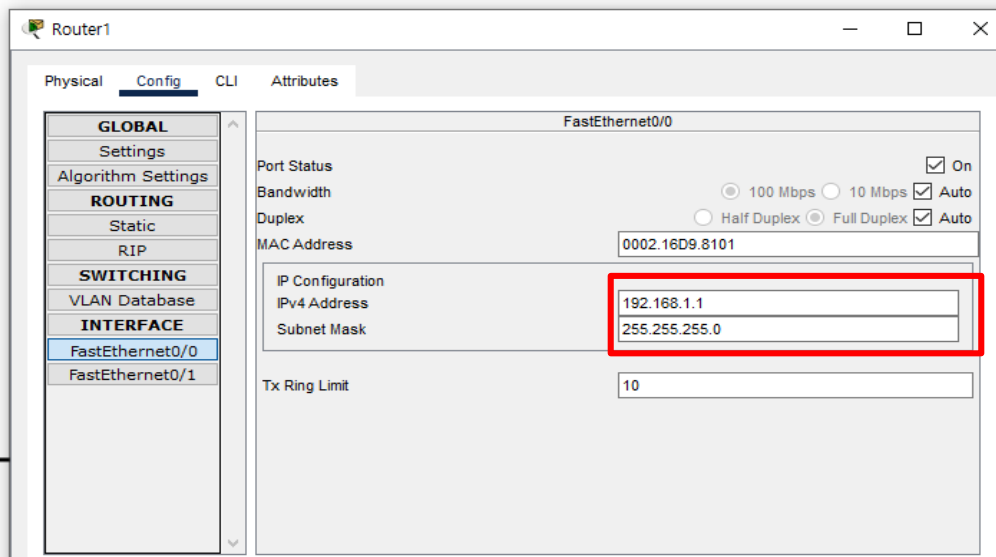
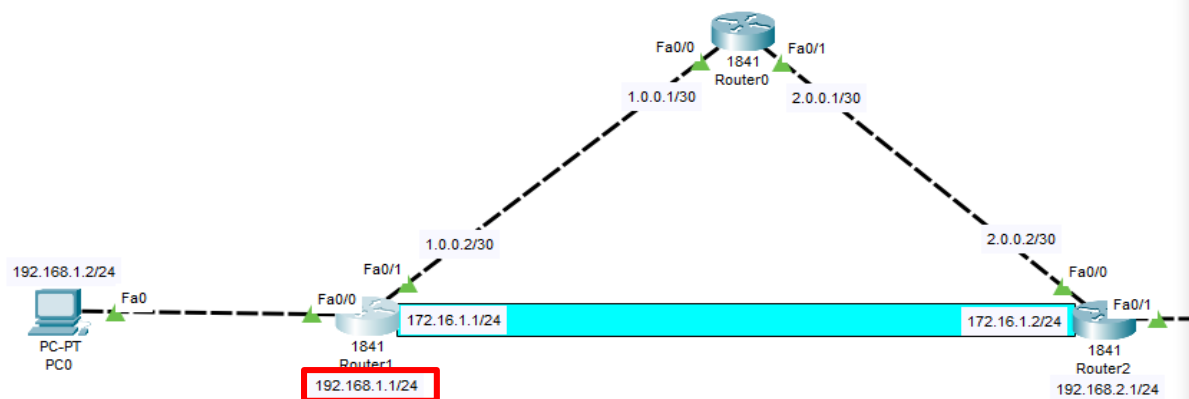
대부분 유동 IP주소를 사용하므로 외부에서 접속할 경우 해킹에 노출될 위험이 높음

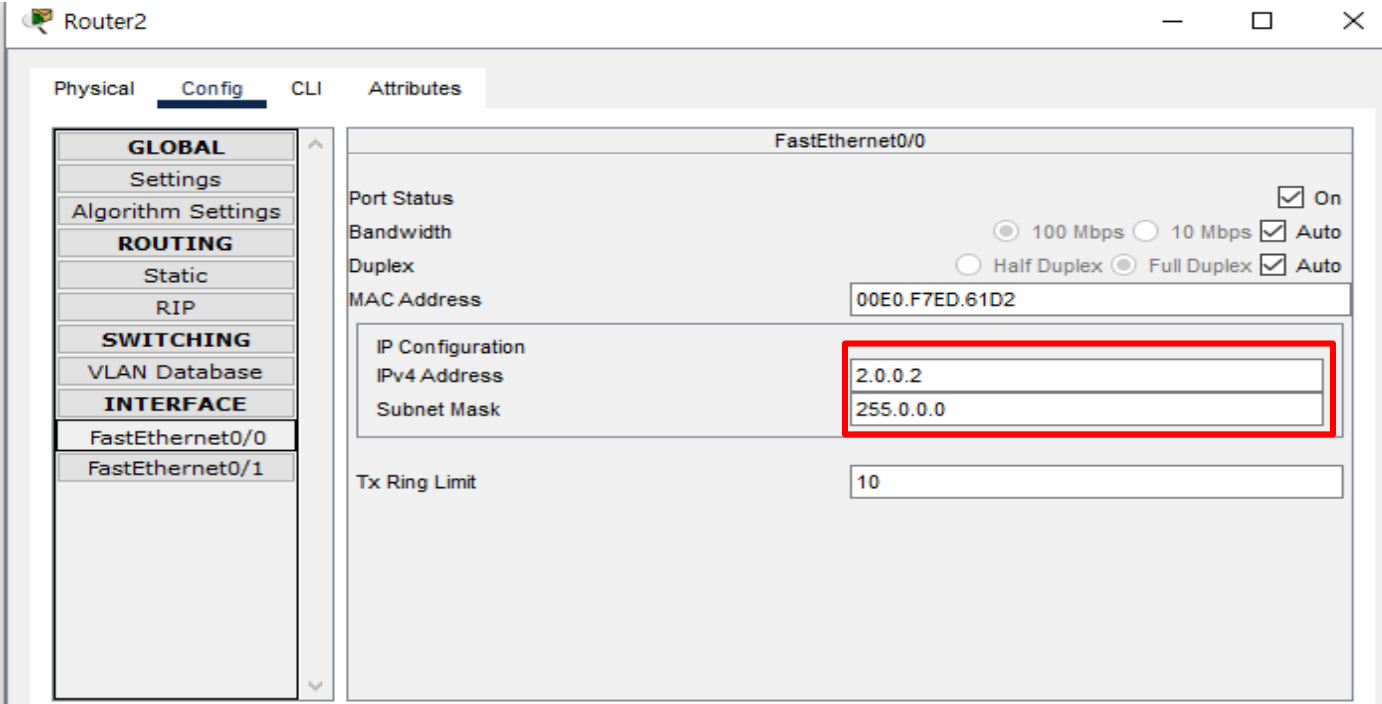
VPN을 이용하면 회사 밖에서도 회사 서버에 접근가능

# VPN 예제

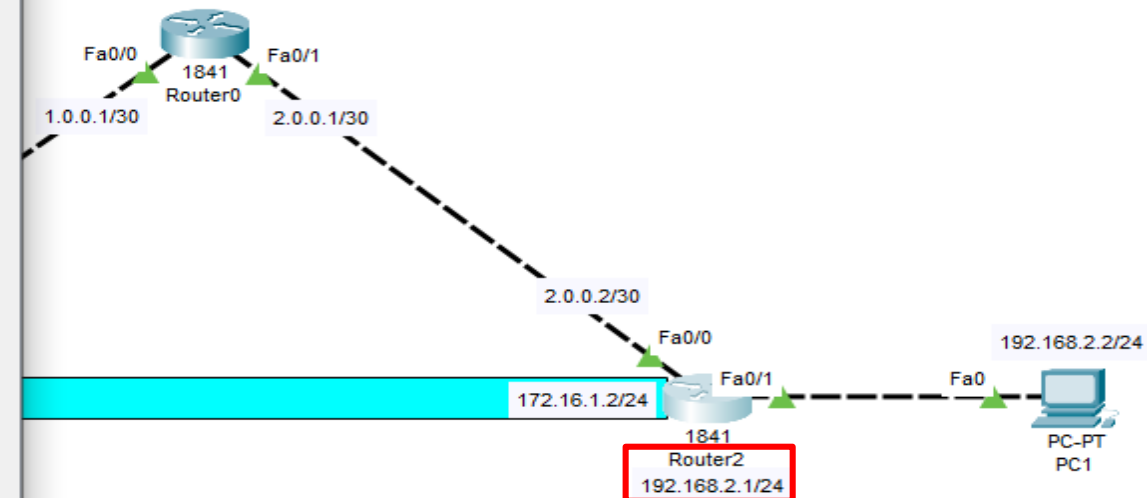
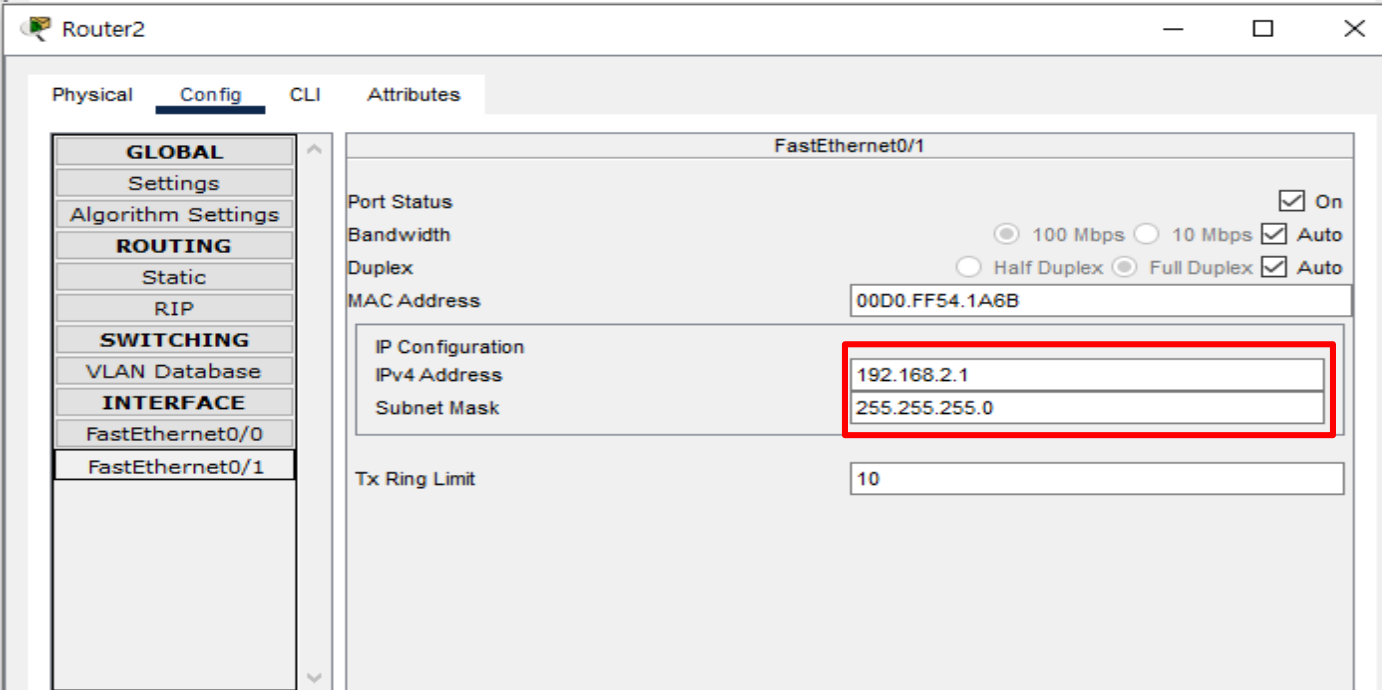
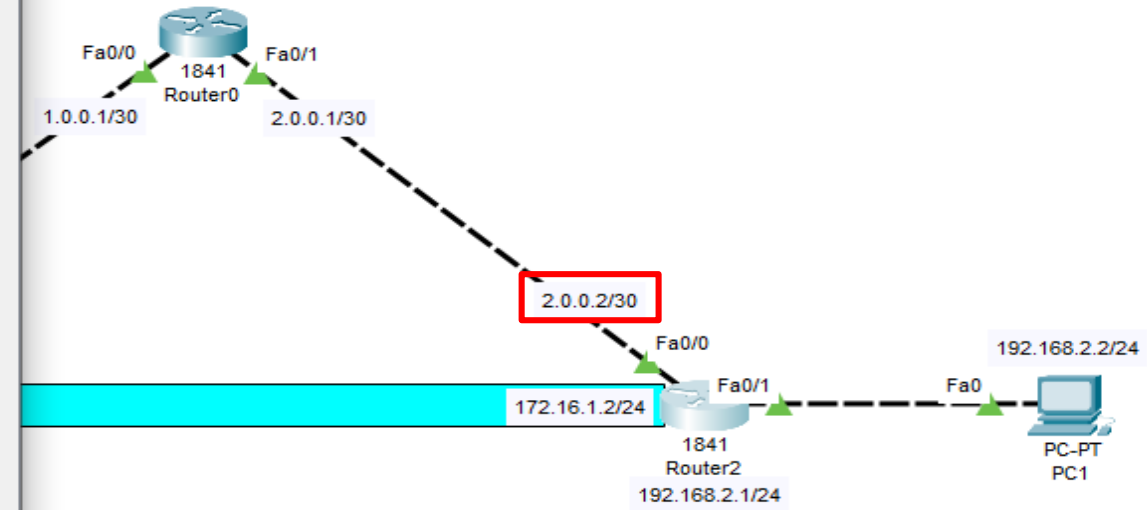


## Router1 의 설정

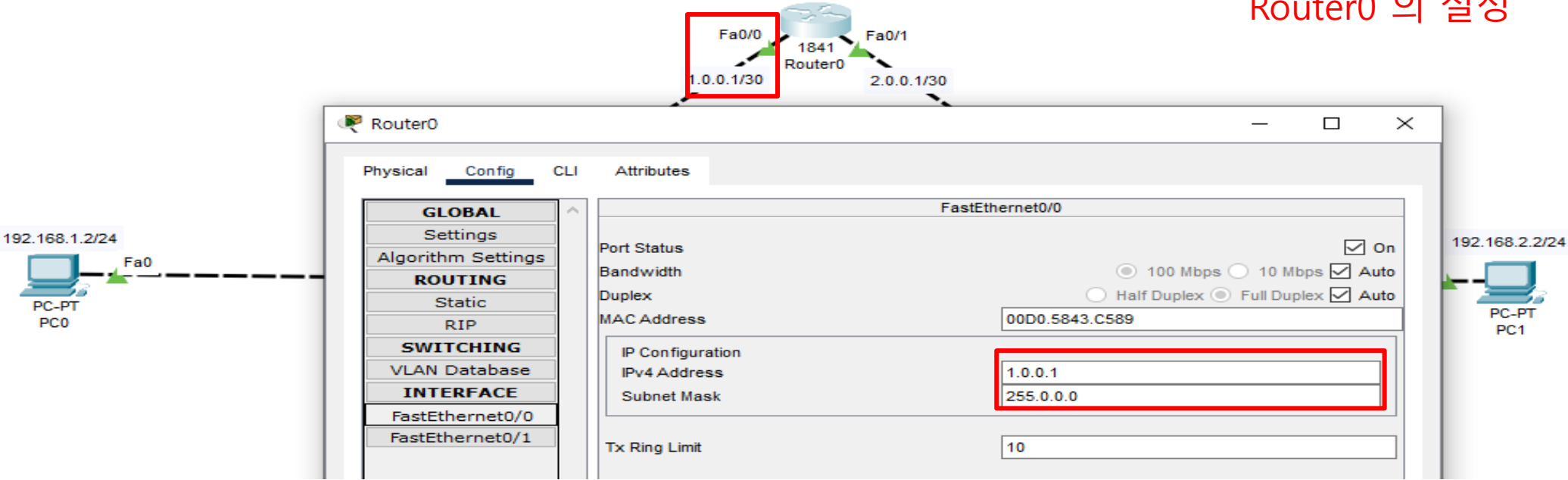




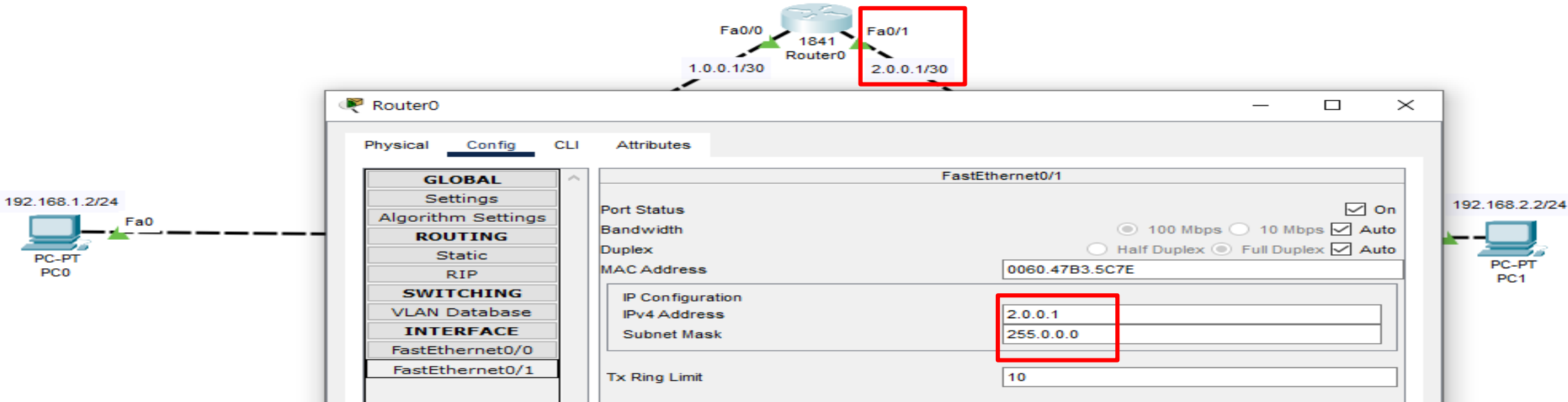
## Router2 의 설정



Router0 의 설정

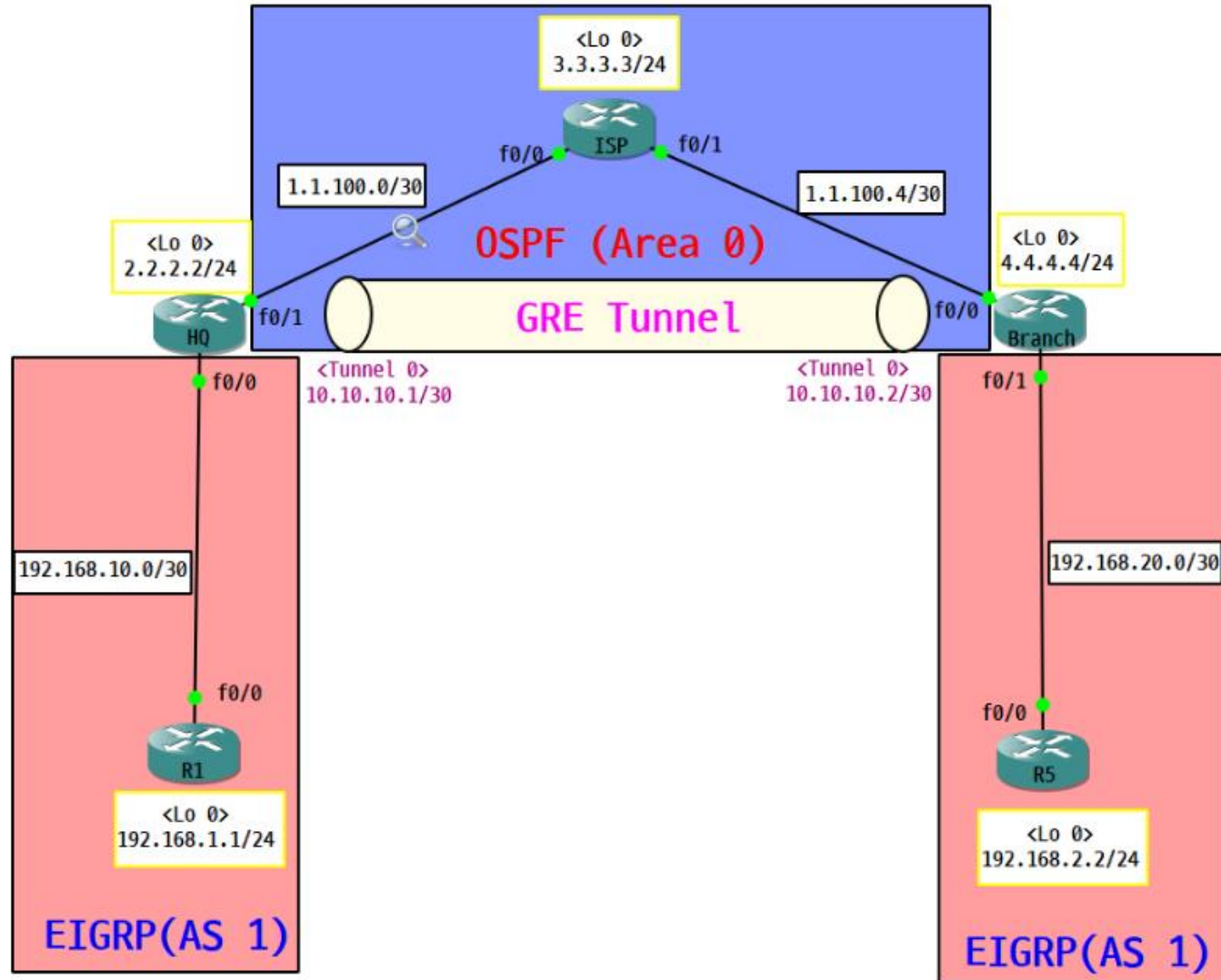


The diagram shows a central router labeled '1841 Router0'. It has two interfaces: Fa0/0 on the left connected to PC-PT PC0 (192.168.1.2/24) and Fa0/1 on the right connected to PC-PT PC1 (192.168.2.2/24). The IP addresses for the interfaces are 1.0.0.1/30 for Fa0/0 and 2.0.0.1/30 for Fa0/1. Below the diagram is the configuration window for Router0, specifically for the FastEthernet0/0 interface. The 'Config' tab is active, and the 'INTERFACE' section is expanded. The 'IP Configuration' section shows the IPv4 Address set to 1.0.0.1 and the Subnet Mask set to 255.0.0.0, both highlighted with a red box. Other settings like Port Status (On), Bandwidth (100 Mbps), Duplex (Full Duplex), and MAC Address (00D0.5843.C589) are also visible.



The diagram shows the same network setup as above, but with the focus on the Fa0/1 interface. The IP address for Fa0/1 is 2.0.0.1/30. Below the diagram is the configuration window for Router0, specifically for the FastEthernet0/1 interface. The 'Config' tab is active, and the 'INTERFACE' section is expanded. The 'IP Configuration' section shows the IPv4 Address set to 2.0.0.1 and the Subnet Mask set to 255.0.0.0, both highlighted with a red box. Other settings like Port Status (On), Bandwidth (100 Mbps), Duplex (Full Duplex), and MAC Address (0060.47B3.5C7E) are also visible.

# GRE LAB





# VPN 예제

## GRE Tunnel

- Cisco에서 개발한 Tunneling Protocol이다.
- 특정 망을 통과할 수 없는 패킷들은 통과가 가능하도록 해주는 프로토콜이다.
- GRE Tunnel이 출구 인터페이스인 경우 원본 IP 패킷에 4Byte의 GRE헤더와 20Byte의 New IP헤더가 추가되어 전송된다. (New IP 헤더 + GRE헤더 + 원본 IP 헤더 + Data)
- 추가적인 24Byte의 오버헤드가 발생된다.

## tunnel mode gre ip

터널 인터페이스 기본 모드가 gre ip 모드이기 때문에 별도로 입력하지 않아도 된다.

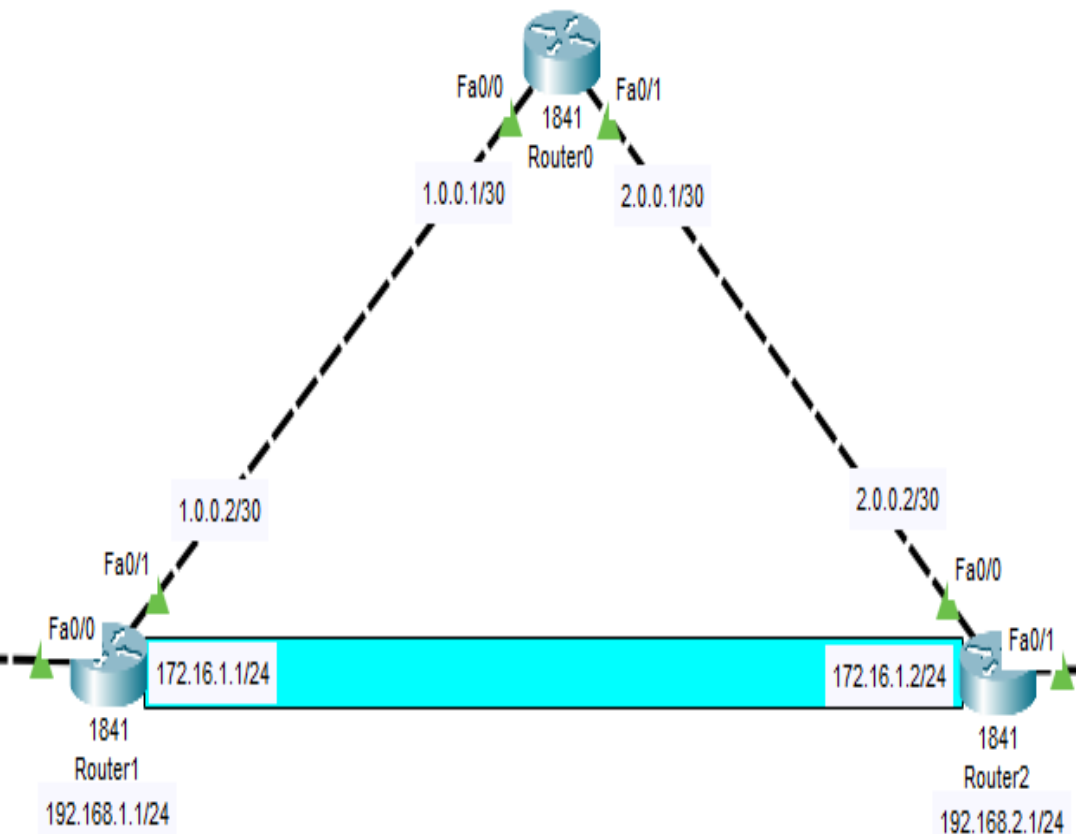
## tunnel source 1.1.100.1

터널 인터페이스의 실제 출발지 IP입력

## tunnel destination 1.1.100.6

터널 인터페이스의 실제 목적지 IP입력

# VPN 예제



Router1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int tunnel 1

Router(config-if)#
%LINK-S-CHANGED: Interface Tunnell, changed state to up

Router(config-if)#ip add 172.16.1.1 255.255.0.0
Router(config-if)#tunnel source Fa0/1
Router(config-if)#tunnel destination 2.0.0.2
Router(config-if)#
%LINEPROTO-S-UPDOWN: Line protocol on Interface Tunnell, changed state to up

Router(config-if)#no shut
Router(config-if)#
```

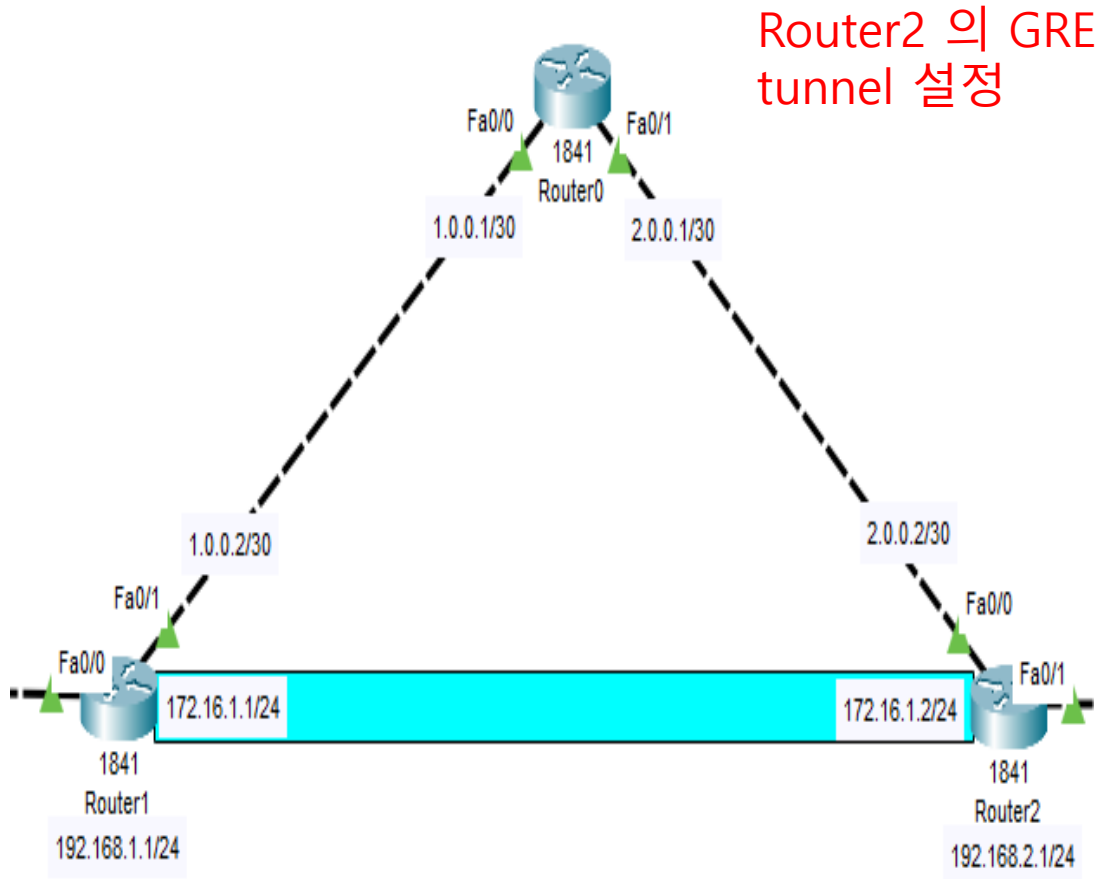
Router1 의 GRE tunnel 설정

tunnel source  
터널 인터페이스의  
실제 출발지 IP입력

tunnel destination  
터널 인터페이스의  
실제 목적지 IP입력

Copy Paste

# VPN 예제



Router2 의 GRE  
tunnel 설정

```
Router2
IOS Command Line Interface
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 2.0.0.2 255.0.0.0
Router(config-if)#ip address 2.0.0.2 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#
Router(config)#ip route 0.0.0.0 0.0.0.0 2.0.0.1
Router(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.1
Router(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config)#int tunnel 2

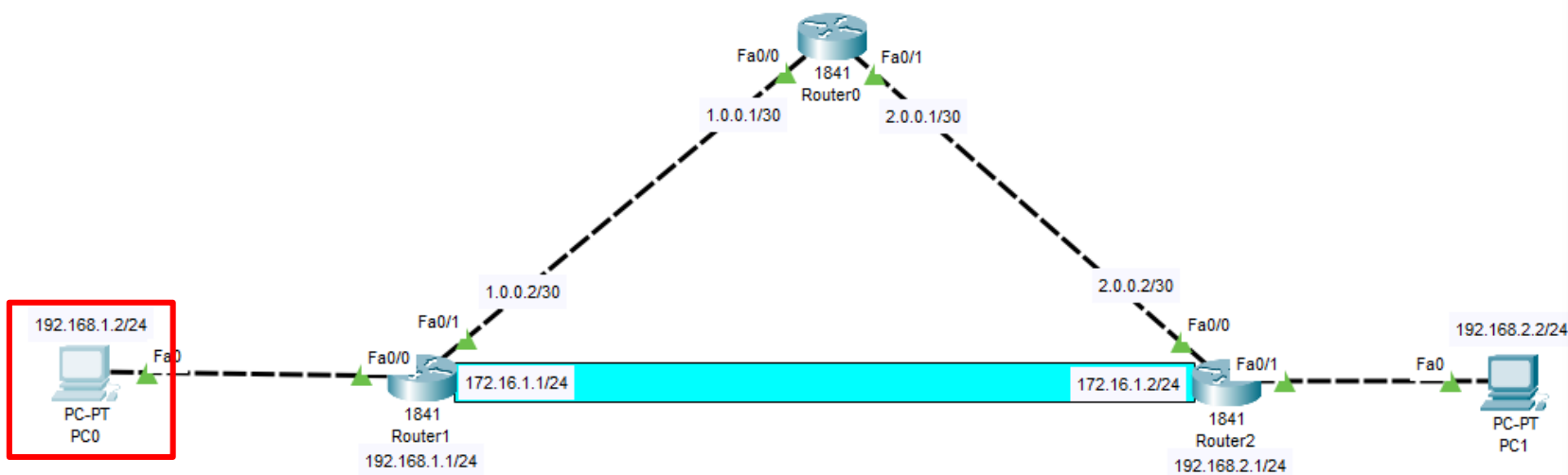
Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel2, changed state to up

Router(config-if)#ip add 172.16.1.2 255.255.0.0
Router(config-if)#tunnel source Fa0/0
Router(config-if)#tunnel destination 1.0.0.2
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to up

Router(config-if)#no shut
Router(config-if)#
Router(config-if)#
```

# VPN 예제

tracert 로 경로확인



PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=3ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>tracert 192.168.2.2

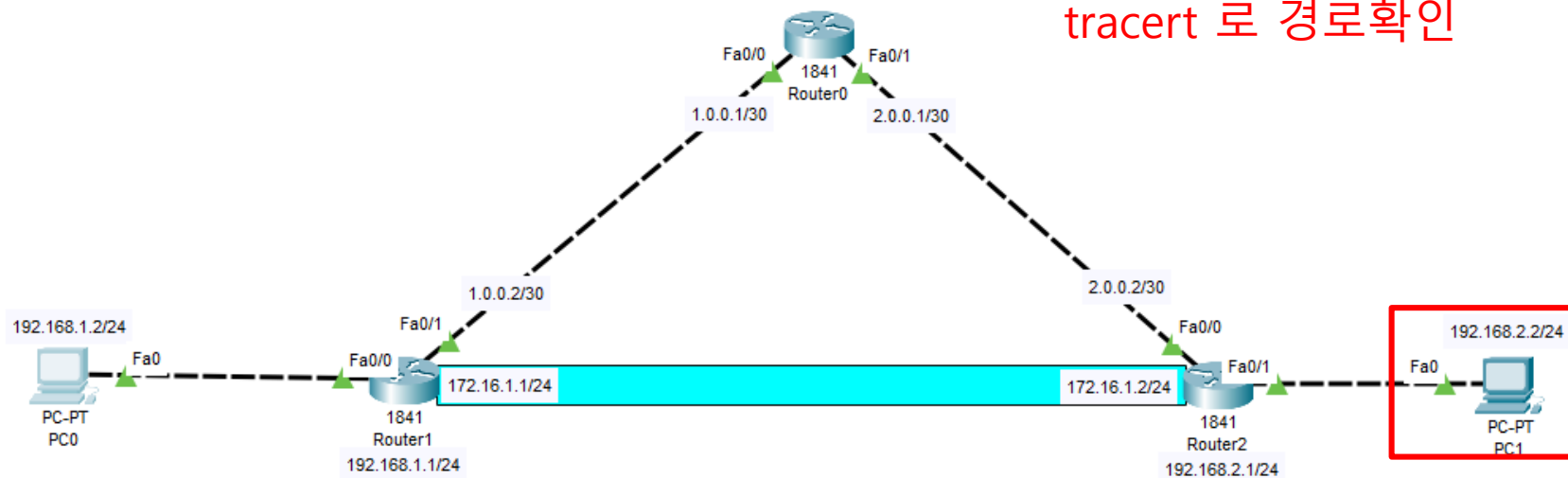
Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.1.1
  2  0 ms    0 ms    0 ms    172.16.1.2
  3  0 ms    0 ms    3 ms    192.168.2.2

Trace complete.

C:\>
```

# VPN 예제



tracert 로 경로확인

PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.2.1
  2  0 ms    0 ms    0 ms    172.16.1.1
  3  0 ms    0 ms    0 ms    192.168.1.2

Trace complete.

C:\>
```