

01 터널링과 VPN

터널링과 캡슐화

■ 터널링(Tunneling)

- 두 네트워크를 한 네트워크처럼 안전하게 사용할 수 있게 만드는 기술
- 터널링에서는 [그림 8-1]과 같이 터널링 장비를 지날 때 일반 라우터나 스위치처럼 원래 패킷에 있던 2계층이나 3계층 정보를 벗겨내지 않고 캡슐화를 수행

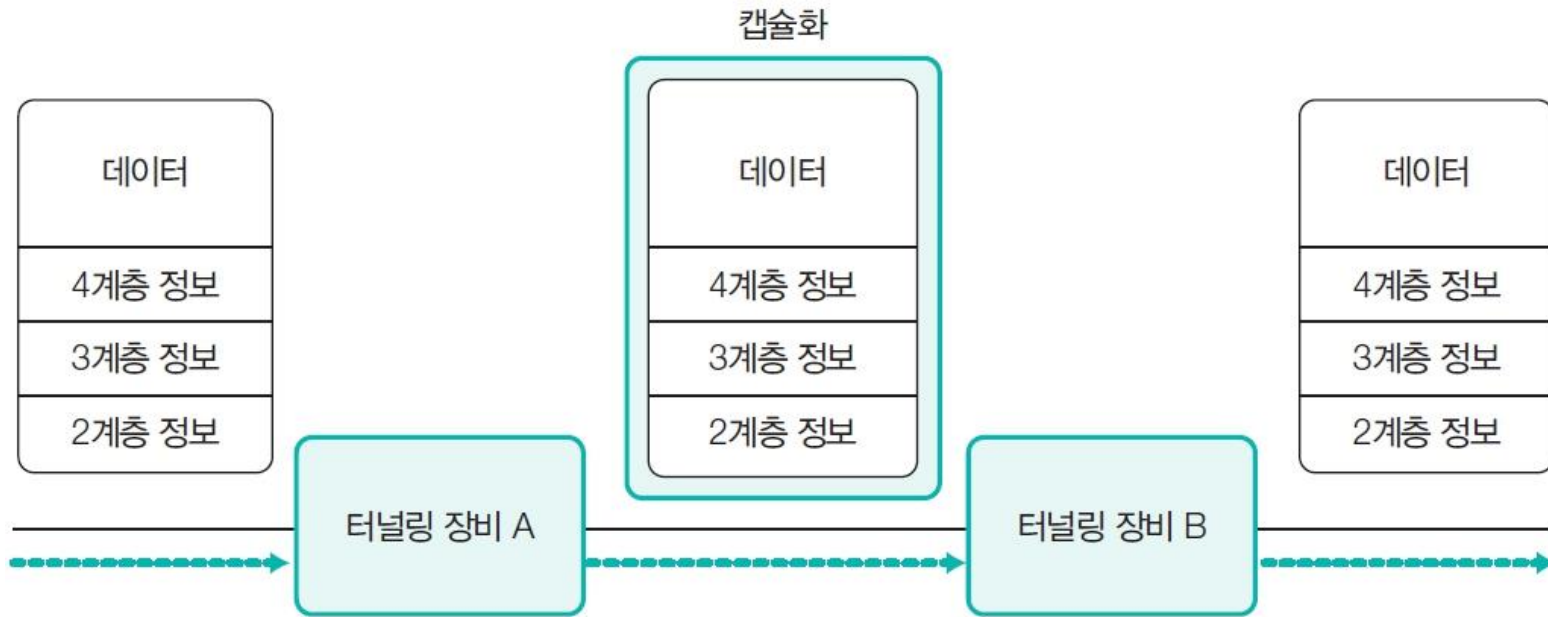


그림 8-1 터널링에서의 패킷 캡슐화

VPN의 용도

■ VPN

- 방화벽, 침입 탐지 시스템과 함께 사용되는 가장 일반적인 보안 솔루션 중 하나
- VPN은 한 달에 3만 원으로 이용할 수 있는 인터넷 회선을 임대 회선처럼 사용할 수 있게 해주는 솔루션
- 이를 위해서는 VPN이 임대 회선과 비슷한 수준의 기밀성을 제공해야 하는데 여기에는 암호화가 필요
- VPN에서 사용하는 암호화 프로토콜에는 PPTP, L2TF, IPSec, SSL 등이 있음

VPN의 용도

■ 해외여행을 하면서 국내 게임 서버 이용

- 대부분의 온라인 게임은 그 나라의 IP 주소만 사용해 접속 가능
- 국내에 VPN 장비를 마련해두면 VPN 장비에 접속해 국내 IP 주소를 할당받아 국내 게임 서버에 접근 가능

■ 집에서도 회사 내의 서버에 보안 상태로 접근

- 대부분 유동 IP 주소를 사용하므로 외부에서 접속할 경우 해킹에 노출될 위험이 높음
- VPN을 이용하면 회사 밖에서도 회사 서버에 접근 가능
- 네트워크 트래픽이 암호화되어 사용자는 VPN 인증과 함께 방화벽을 통한 서비스 통제, 접근 대상 서비스 인증을 거치므로 임의 접근보다 훨씬 높은 수준의 보안을 유지할 수 있음

VPN의 용도

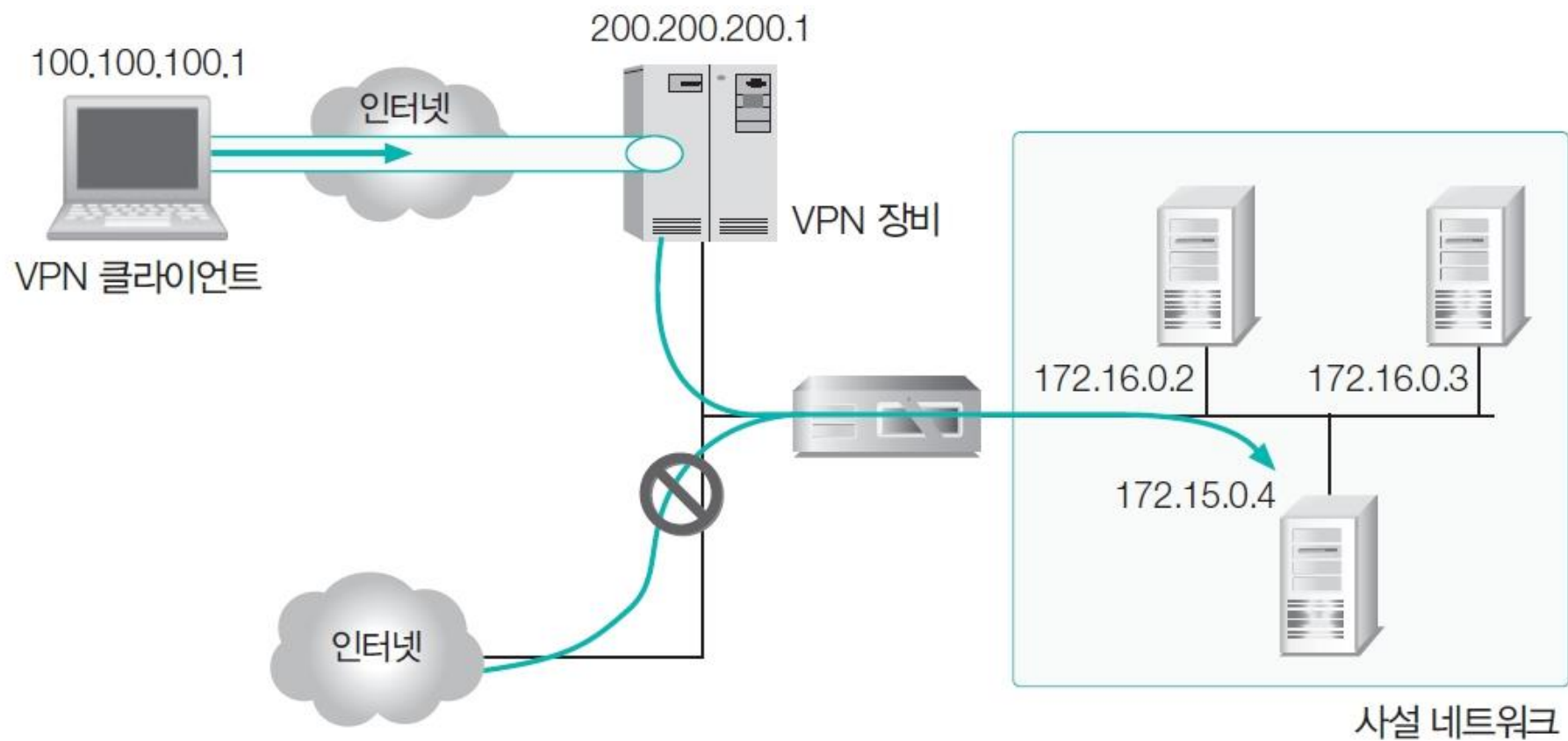


그림 8-2 VPN을 이용한 외부에서의 접근

VPN의 용도

■ 원격의 두 지점을 내부 네트워크처럼 이용

- VPN은 인증을 제공하기도 하지만 인증 없이 터널링을 제공하기도 함

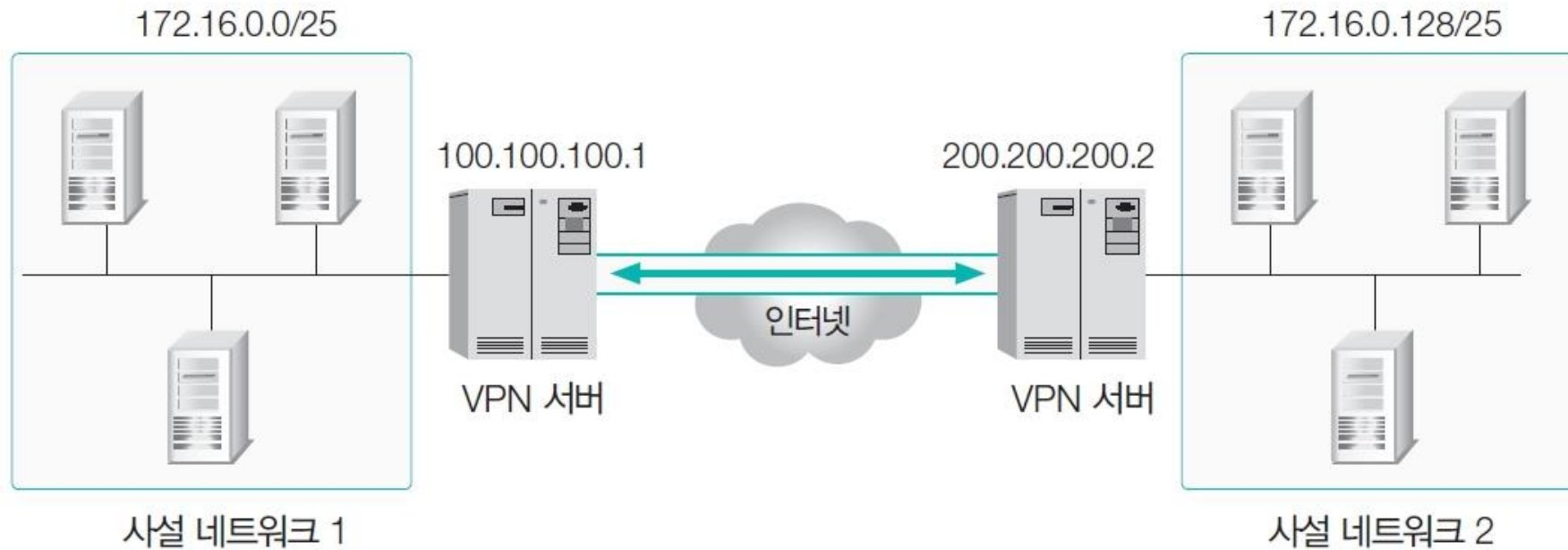
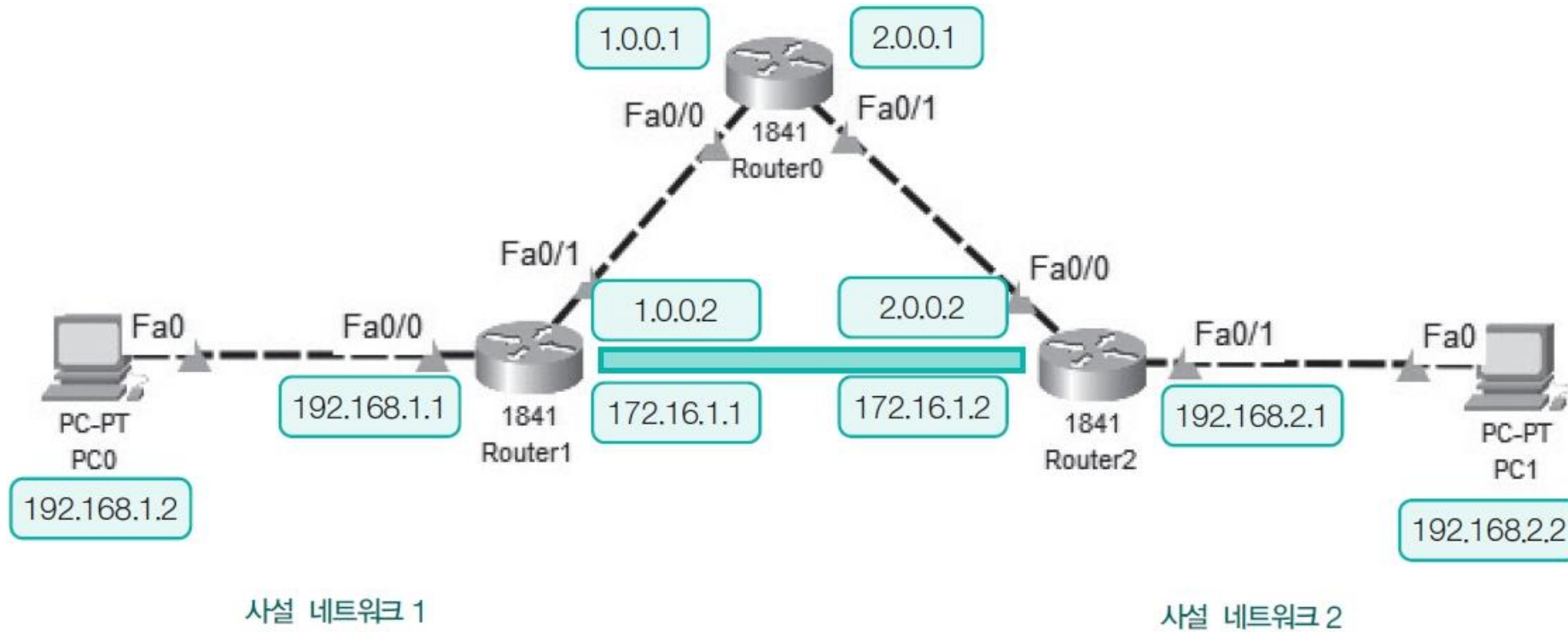


그림 8-3 VPN을 이용한 터널링

[실습 8-1] 패킷 트레이서에서 VPN 설정하기

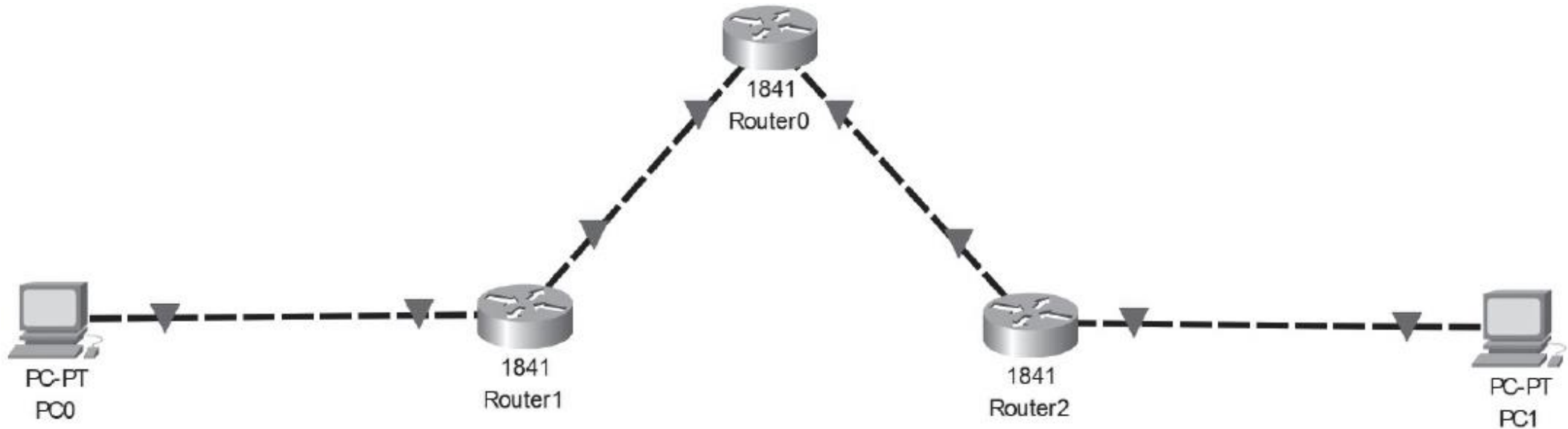
- 사설 네트워크 1(192.168.1.x)과 사설 네트워크 2(192.168.2.x)를 외부 인터넷 망을 이용해 VPN으로 가상 사설 네트워크로 연결하는 실습해보기



[실습 8-1] 패킷 트레이서에서 VPN 설정하기

1 네트워크 구성하기

PC 2대, 라우터 3대를 연결



[실습 8-1] 패킷 트레이서에서 VPN 설정하기

2 사설 네트워크 1, 2의 PC 설정하기

2-1 사설 네트워크 1에 있는 PC0을 클릭한 후 [Desktop]-[IP Configuration] 메뉴를 선택해 IP 주소를 다음과 같이 설정

The screenshot shows the configuration window for PC0 in a network simulator. The 'Desktop' tab is selected, and the 'IP Configuration' menu is open. The 'Interface' is set to 'FastEthernet0'. Under 'IP Configuration', the 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

Under 'IPv6 Configuration', the 'Static' radio button is also selected. The fields are filled with the following values:

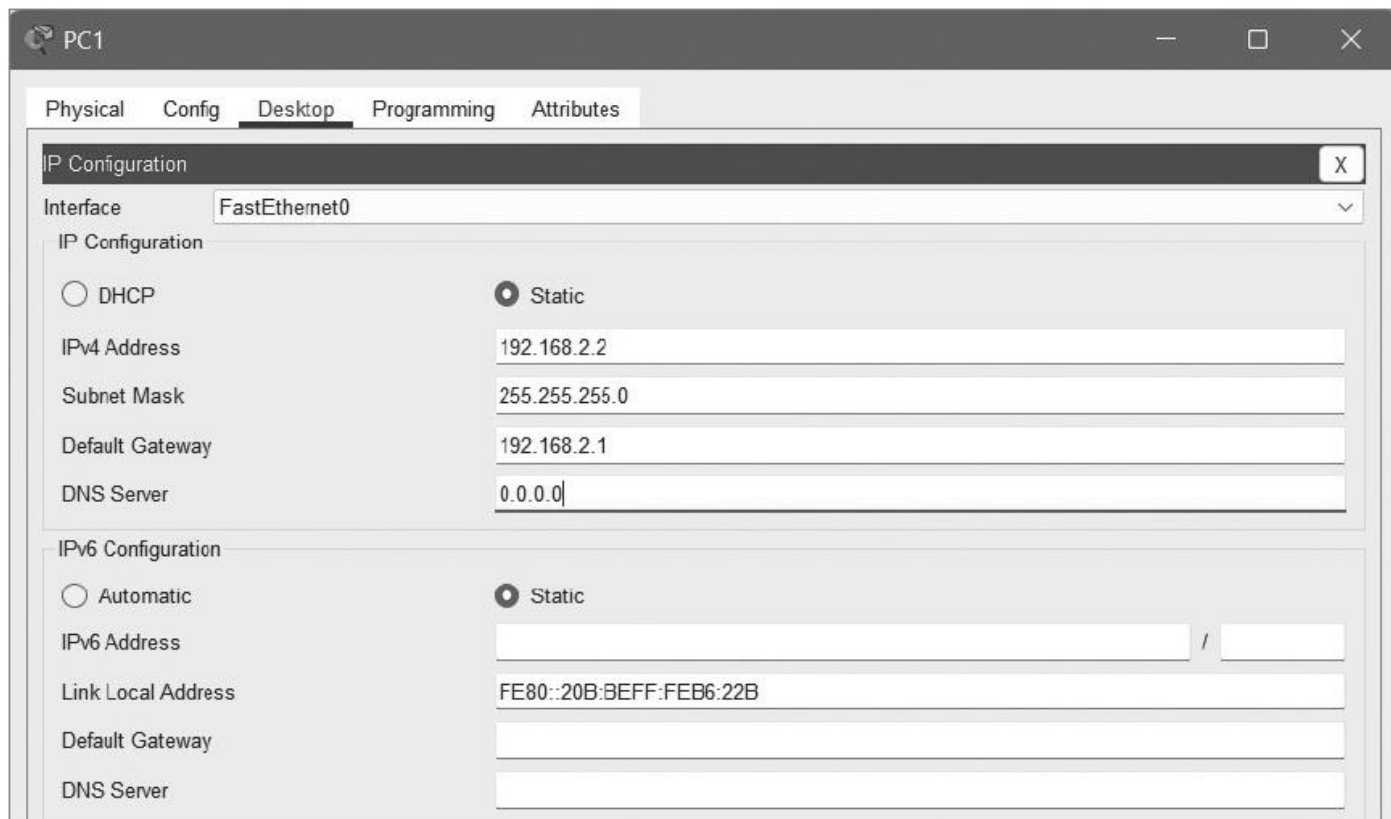
Field	Value
IPv6 Address	
Link Local Address	FE80::20A:F3FF:FE9D:5E22
Default Gateway	
DNS Server	

Under '802.1X', the 'Use 802.1X Security' checkbox is unchecked. The 'Authentication' dropdown is set to 'MD5'. The 'Username' and 'Password' fields are empty.

[실습 8-1] 패킷 트레이서에서 VPN 설정하기

2 사설 네트워크 1, 2의 PC 설정하기

2-2 사설 네트워크 2에 있는 PC1을 클릭한 후 [Desktop]-[IP Configuration] 메뉴를 선택해 IP 주소를 다음과 같이 설정



The screenshot shows the configuration window for PC1 in a network simulator. The 'Desktop' tab is selected, and the 'IP Configuration' menu is open. The 'Interface' is set to 'FastEthernet0'. Under 'IP Configuration', the 'Static' radio button is selected. The IPv4 settings are as follows:

Field	Value
IPv4 Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	0.0.0.0

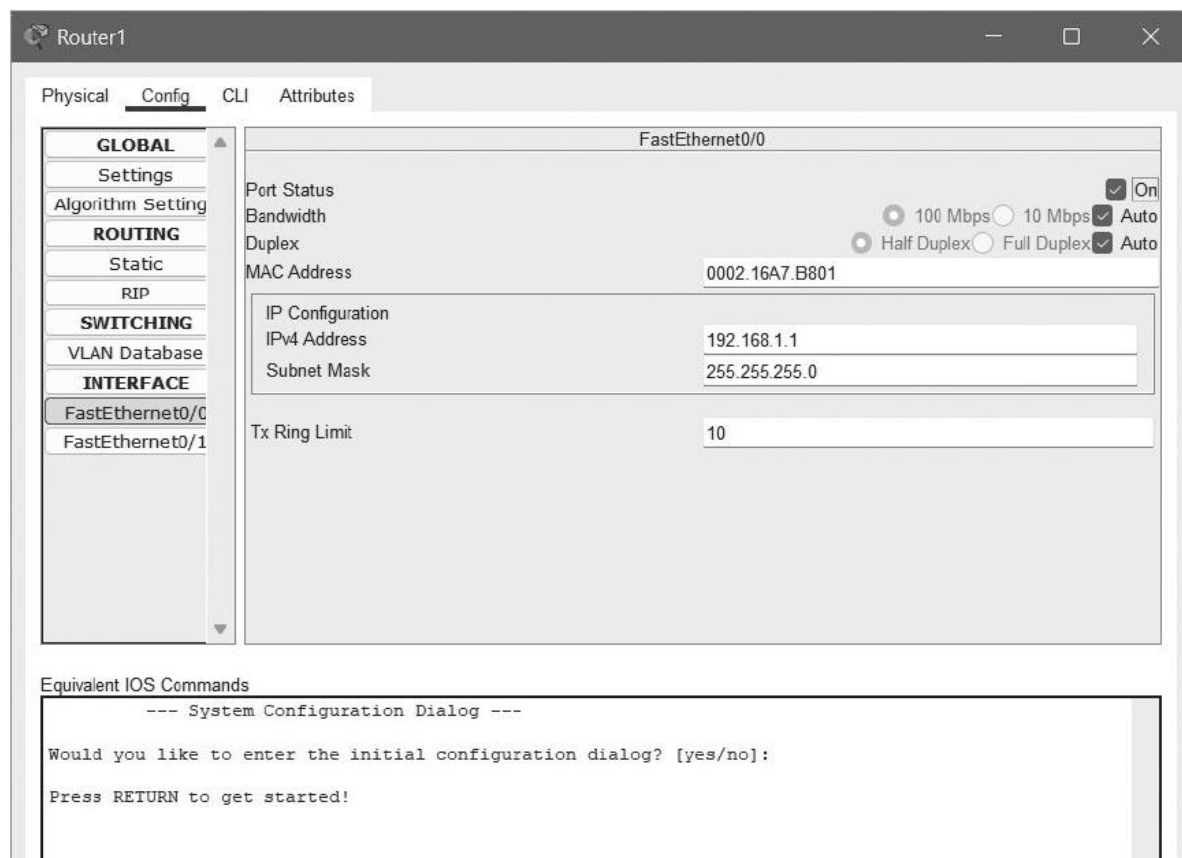
Under 'IPv6 Configuration', the 'Static' radio button is also selected. The IPv6 settings are as follows:

Field	Value
IPv6 Address	
Link Local Address	FE80::20B:BEFF:FEB6:22B
Default Gateway	
DNS Server	

[실습 8-1] 패킷 트레이서에서 VPN 설정하기

3 사설 네트워크 1의 라우터 설정하기

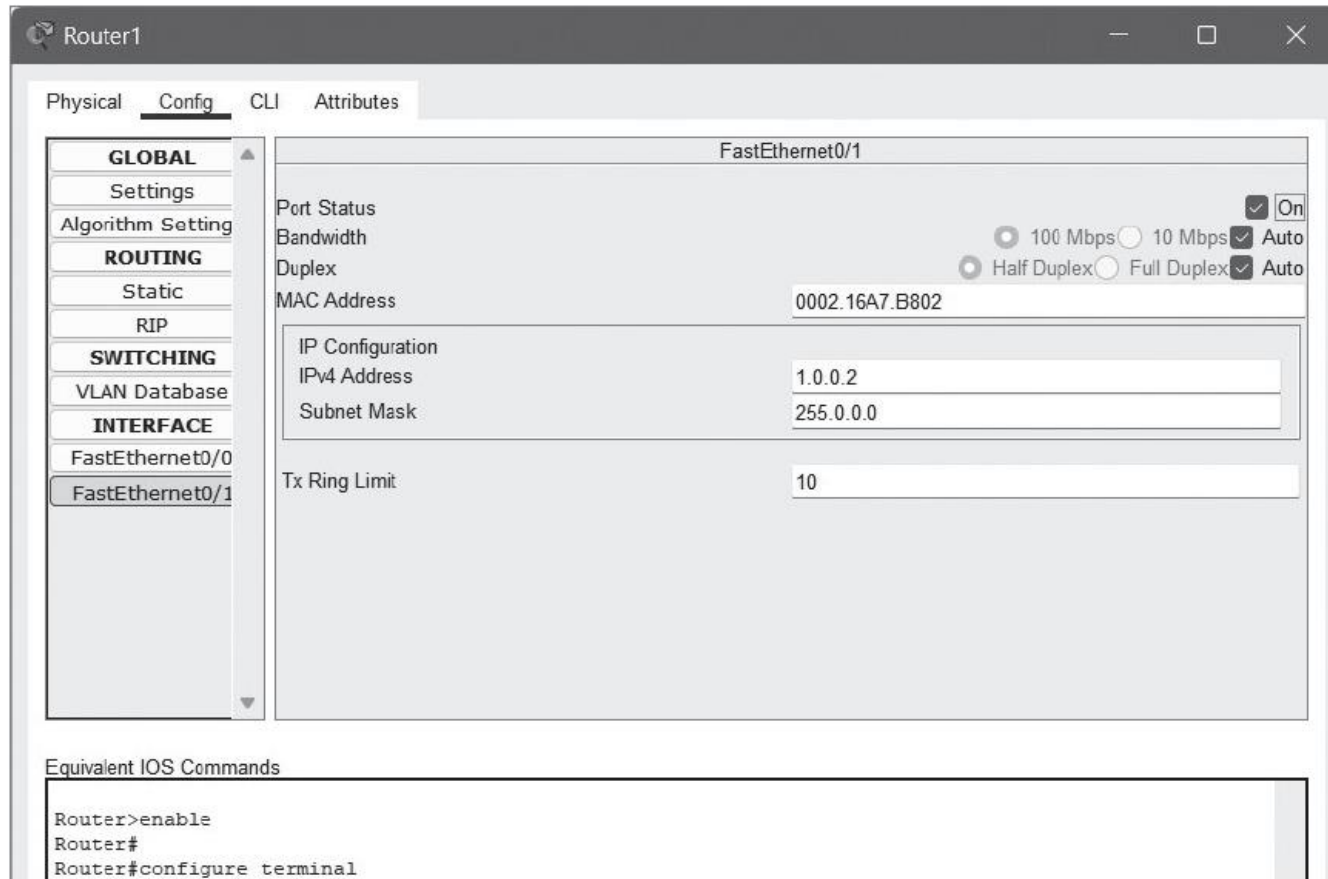
3-1 Router1을 클릭한 후 [Config]-[INTERFACE]-[FastEthernet0/0]을 선택해 IPv4 주소를 192.168.1.1로, 서브넷 마스크를 255.255.255.0으로 입력한 후 Port Status의 On을 체크



[실습 8-1] 패킷 트레이서에서 VPN 설정하기

3 사설 네트워크 1의 라우터 설정하기

3-2 [FastEthernet0/1]은 IPv4 주소를 1.0.0.2로, Subnet Mask를 255.0.0.0으로 입력한 후 Port Status의 On을 체크



[실습 8-1] 패킷 트레이서에서 VPN 설정하기

3 사설 네트워크 1의 라우터 설정하기

3-3 라우팅 테이블을 설정하기 위해 Router1을 클릭한 후 [Config]-[ROUTING]-[Static] 메뉴를 선택해 다음과 같이 입력한 후 [Add]를 누르기

The screenshot shows the 'Router1' configuration window with the 'Config' tab selected. The left sidebar shows the configuration tree with 'ROUTING' > 'Static' selected. The main area is titled 'Static Routes' and contains the following fields:

- Network: 0.0.0.0
- Mask: 0.0.0.0
- Next Hop: 1.0.0.1

Below these fields is an 'Add' button. At the bottom of the main area, there is a 'Network Address' section showing '0.0.0.0/0 via 1.0.0.1' and a 'Remove' button.

At the bottom of the window, the 'Equivalent IOS Commands' section shows the following commands:

```
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
```

[실습 8-1] 패킷 트레이서에서 VPN 설정하기

3 사설 네트워크 1의 라우터 설정하기

3-4 같은 화면에서 VPN 설정을 위해서 사설 네트워크 2로 가는 것을 다음과 같이 입력하고 [Add]를 누르기

The screenshot shows the 'Router1' configuration window with the 'Config' tab selected. The left sidebar contains a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under ROUTING, 'Static' is selected. The main area is titled 'Static Routes' and contains input fields for 'Network' (192.168.2.0), 'Mask' (255.255.255.0), and 'Next Hop' (172.16.1.2). Below these fields is an 'Add' button. A table below the 'Add' button lists the configured static routes:

Network Address
0.0.0.0/0 via 1.0.0.1
192.168.2.0/24 via 172.16.1.2

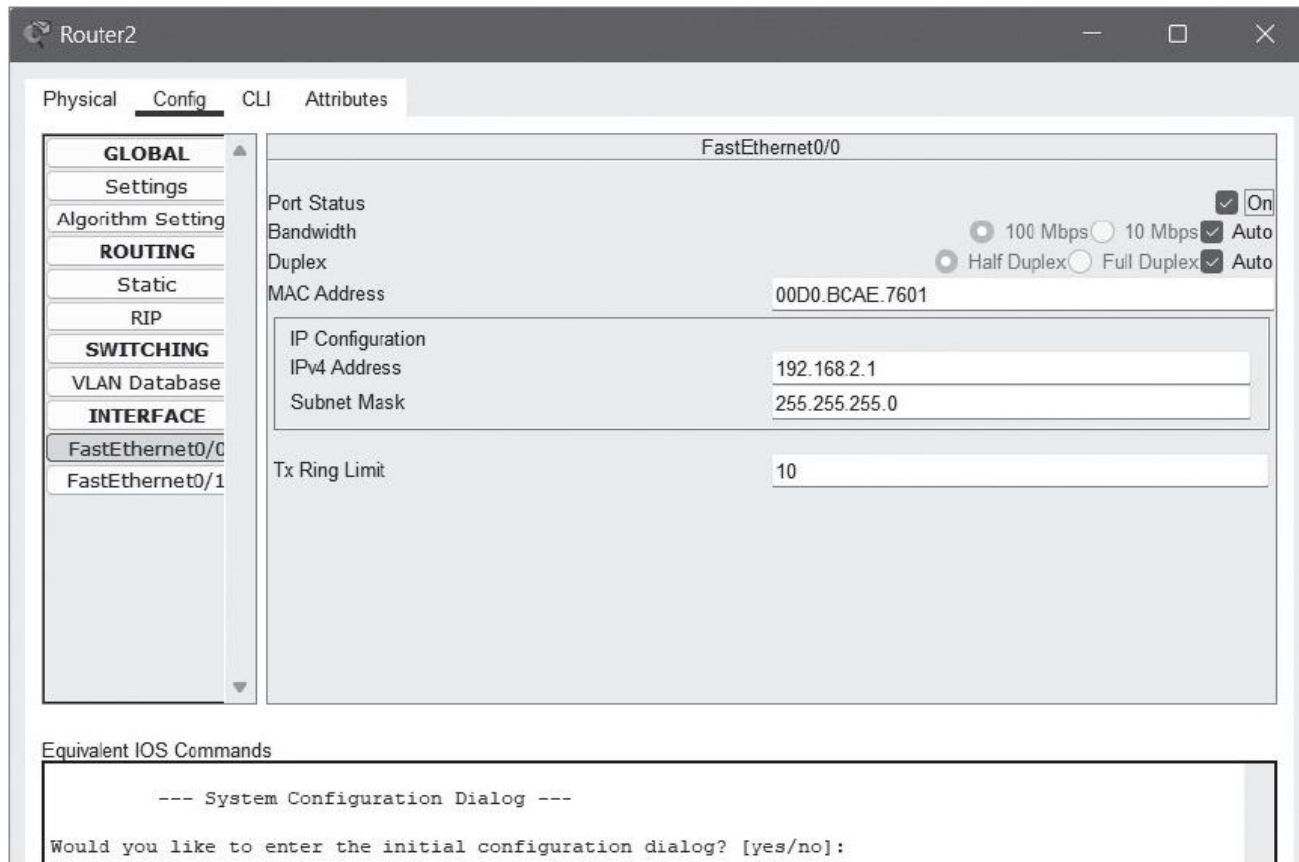
At the bottom right of the table is a 'Remove' button. At the bottom of the window, the 'Equivalent IOS Commands' section shows the following commands:

```
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 1.0.0.2 255.0.0.0
```

[실습 8-1] 패킷 트레이서에서 VPN 설정하기

4 사설 네트워크 2의 라우터 설정하기

4-1 Router2를 클릭한 후 [Config]-[INTERFACE]-[FastEthernet0/0] 메뉴를 선택해 IPv4 주소를 192.168.2.1로, 서브넷 마스크를 255.255.255.0으로 입력한 후 Port Status의 On을 체크



[실습 8-1] 패킷 트레이서에서 VPN 설정하기

4 사설 네트워크 2의 라우터 설정하기

4-2 [FastEthernet0/1]은 IPv4 주소를 2.0.0.2로, 서브넷 마스크를 255.0.0.0으로 입력한 후 Port Status의 On을 체크

The screenshot shows the configuration window for Router2, specifically the FastEthernet0/1 interface. The 'Config' tab is selected. The left sidebar shows the configuration tree with 'FastEthernet0/1' selected under the 'INTERFACE' section. The main area displays the configuration for FastEthernet0/1. The 'Port Status' section has 'On' checked. The 'Bandwidth' section has '100 Mbps' selected. The 'Duplex' section has 'Full Duplex' selected. The 'MAC Address' is 00D0.BCAE.7602. The 'IP Configuration' section shows 'IPv4 Address' as 2.0.0.2 and 'Subnet Mask' as 255.0.0.0. The 'Tx Ring Limit' is 10. At the bottom, the 'Equivalent IOS Commands' section shows the following commands:

```
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.1.2 255.255.255.0
Router(config-if)#ip address 192.168.1.2 255.255.255.0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
```


[실습 8-1] 패킷 트레이서에서 VPN 설정하기

4 사설 네트워크 2의 라우터 설정하기

4-3 Router2를 클릭한 후 [Config]-[ROUTING]-[Static]을 선택해 다음과 같이 입력한 후 [Add]를 누르기

The screenshot shows the 'Router2' configuration window with the 'Config' tab selected. The left sidebar shows a tree view with 'ROUTING' expanded and 'Static' selected. The main area is titled 'Static Routes' and contains the following fields:

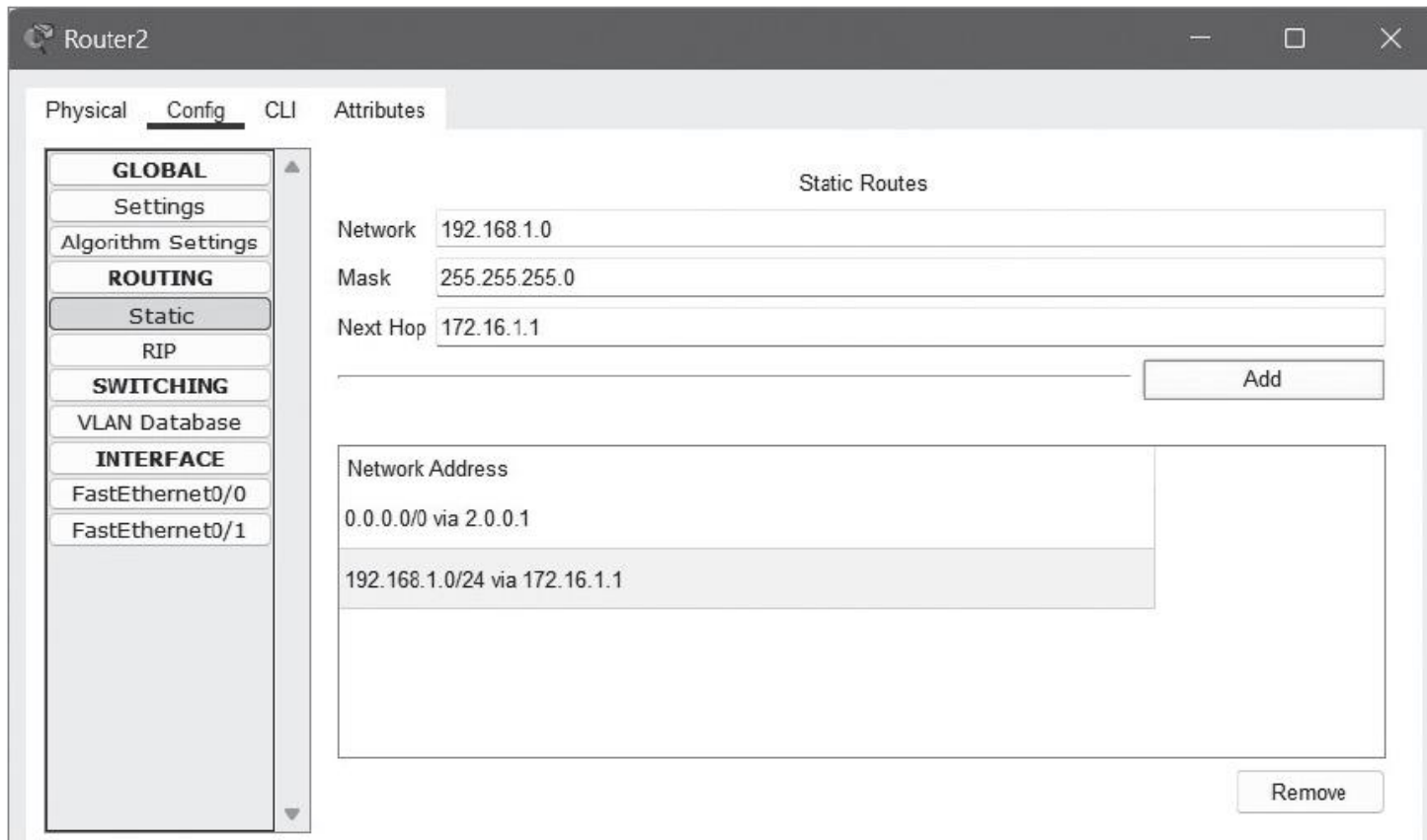
- Network: 0.0.0.0
- Mask: 0.0.0.0
- Next Hop: 2.0.0.1

Below these fields is an 'Add' button. At the bottom of the main area, there is a 'Network Address' section showing '0.0.0.0/0 via 2.0.0.1' and a 'Remove' button.

[실습 8-1] 패킷 트레이서에서 VPN 설정하기

4 사설 네트워크 2의 라우터 설정하기

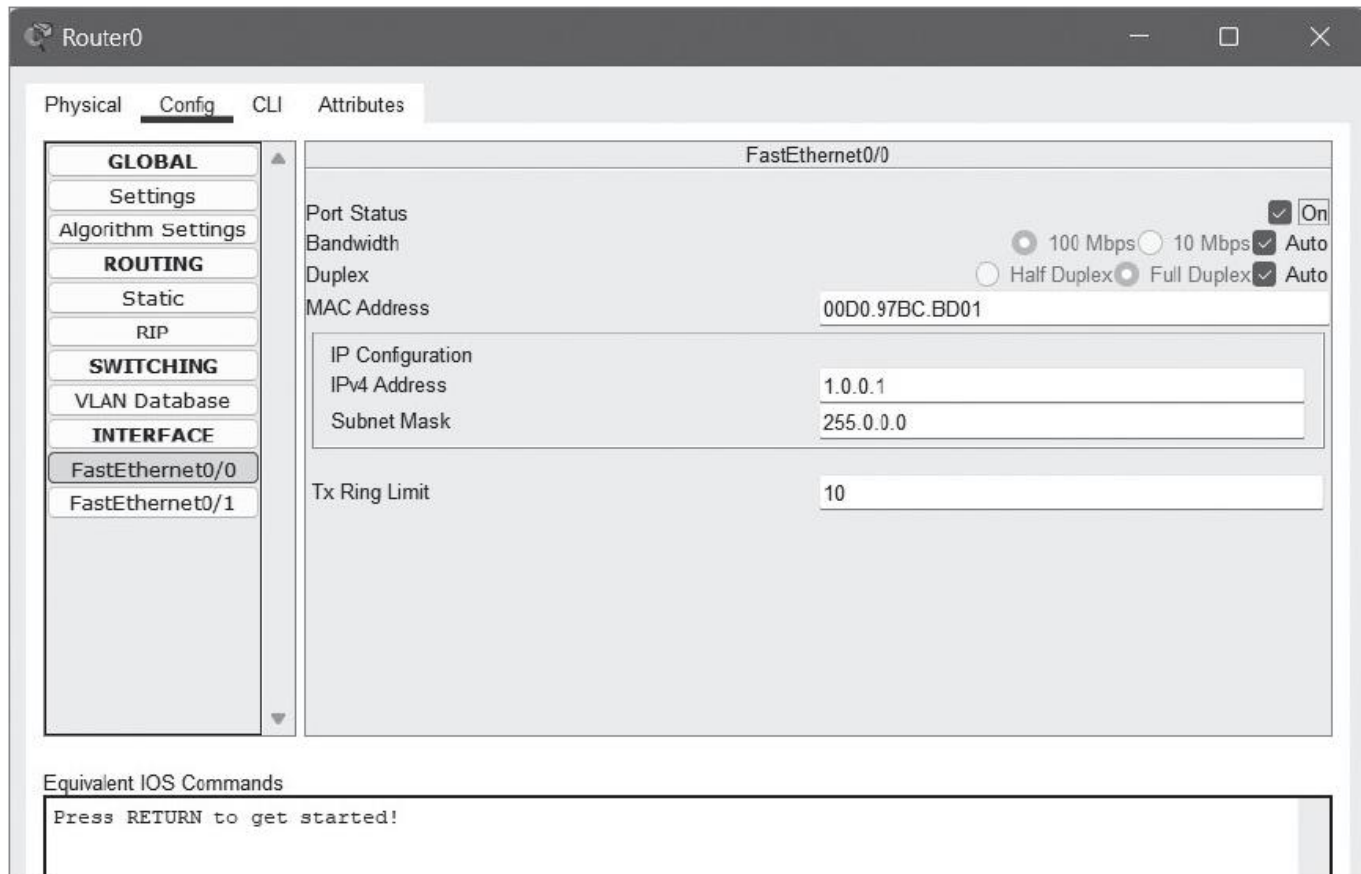
4-4 같은 화면에서 VPN 설정을 위해서 사설 네트워크 1로 가는 것을 다음과 같이 입력하고 [Add]를 누르기



[실습 8-1] 패킷 트레이서에서 VPN 설정하기

5 외부 라우터 설정하기

5-1 Router0을 클릭한 후 [Config]-[INTERFACE]-[FastEthernet0/0]을 선택해 IPv4 주소를 1.0.0.1로, 서브넷 마스크를 255.0.0.0으로 입력한 후 Port Status의 On을 체크



[실습 8-1] 패킷 트레이서에서 VPN 설정하기

5 외부 라우터 설정하기

5-2 [FastEthernet0/1]은 IPv4 주소를 2.0.0.1로, Subnet Mask를 255.0.0.0으로 입력한 후 Port Status의 On을 체크

The screenshot shows the configuration window for Router0, specifically the 'Config' tab for the FastEthernet0/1 interface. The left sidebar shows a tree view with 'FastEthernet0/1' selected under the 'INTERFACE' section. The main area displays the following settings:

- Port Status:** ☒ On
- Bandwidth:** ☒ 100 Mbps ☐ 10 Mbps ☒ Auto
- Duplex:** ☐ Half Duplex ☒ Full Duplex ☒ Auto
- MAC Address:** 00D0.97BC.BD02
- IP Configuration:**
 - IPv4 Address:** 2.0.0.1
 - Subnet Mask:** 255.0.0.0
- Tx Ring Limit:** 10

At the bottom, the 'Equivalent IOS Commands' section shows the following commands:

```
Router(config-if)#ip address 1.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-S-CHANGED: Interface FastEthernet0/0, changed state to up
```

[실습 8-1] 패킷 트레이서에서 VPN 설정하기

5 외부 라우터 설정하기

5-3 Router0을 클릭한 후 [Config]-[ROUTING]-[Static] 메뉴를 선택하고 다음과 같이 사설 네트워크 2의 IP로 이동할 경우 Next Hop에 2.0.0.2로 입력하고 [Add]를 누르기

The screenshot shows the configuration window for Router0. The 'Config' tab is selected, and the 'ROUTING' section is expanded, with 'Static' routes chosen. The 'Static Routes' configuration area shows the following fields:

- Network: 192.168.2.0
- Mask: 255.255.255.0
- Next Hop: 2.0.0.2

An 'Add' button is visible next to the Next Hop field. Below these fields, a summary box shows the configured route: '192.168.2.0/24 via 2.0.0.2'. A 'Remove' button is located at the bottom right of this summary box.

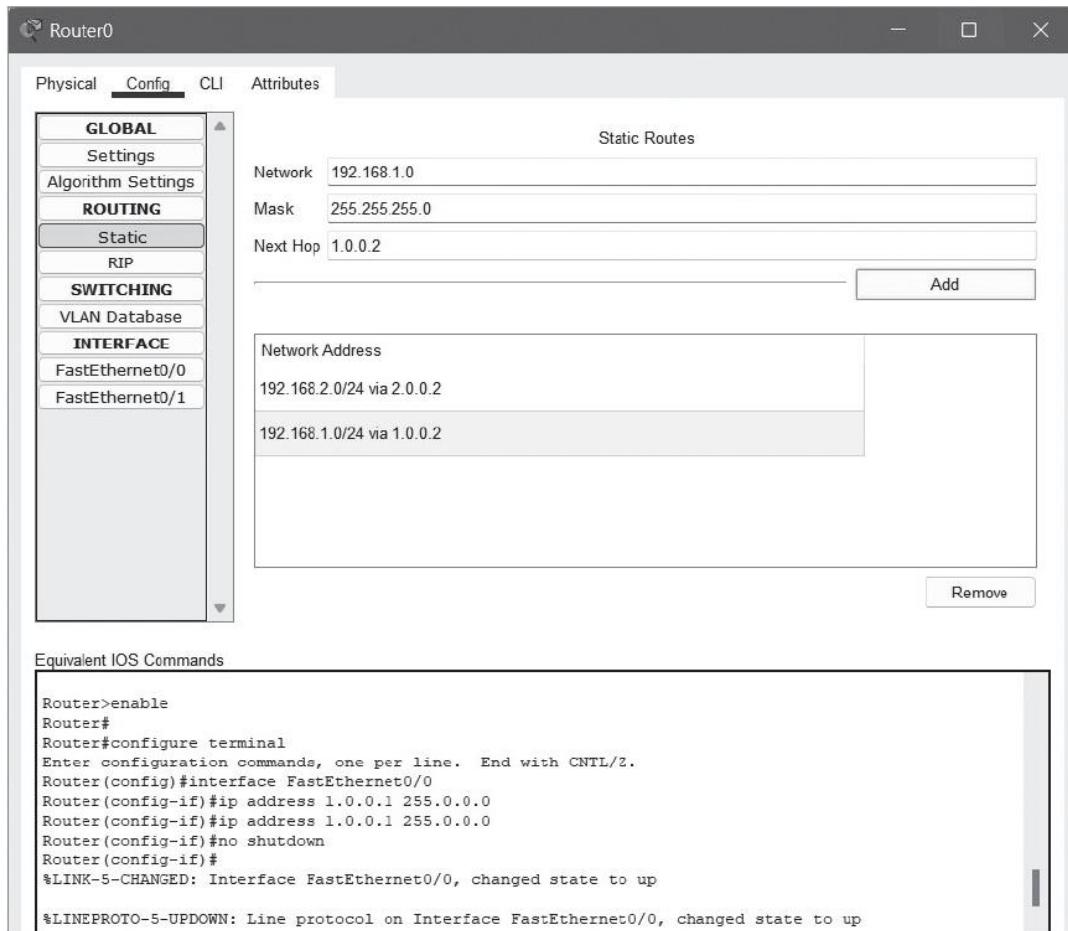
At the bottom of the window, the 'Equivalent IOS Commands' section displays the following commands:

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTRL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 1.0.0.1 255.0.0.0
Router(config-if)#ip address 1.0.0.1 255.0.0.0
```

[실습 8-1] 패킷 트레이서에서 VPN 설정하기

5 외부 라우터 설정하기

5-4 같은 화면에서 다음과 같이 사설 네트워크 1의 IP로 이동할 경우 Next Hop에 1.0.0.2로 입력하고 [Add]를 누르기



[실습 8-1] 패킷 트레이서에서 VPN 설정하기

6 터널링 설정하기

6-1 터널링 설정을 위해 Router1을 클릭한 후 [CLI] 메뉴를 선택해 다음과 같이 명령을 입력
터널링 번호를 부여하고, 터널링에 사용할 출발지 IP 주소, 터널링 포트, 목적지 IP 주소를 할당

```
Router>enable
```

```
Router#config t
```

```
Router(config)#interface tunnel 1
```

```
Router(config-if)#ip address 172.16.1.1 255.255.0.0
```

```
Router(config-if)#tunnel source FastEthernet0/1
```

```
Router(config-if)#tunnel destination 2.0.0.2
```

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

[실습 8-1] 패킷 트레이서에서 VPN 설정하기

6 터널링 설정하기

6-2 Router2에서도 동일한 방법으로 터널링을 설정하기 위해 Router1을 클릭한 후 [CLI] 메뉴를 선택해 다음과 같이 터널링 번호를 부여하고, 터널링에 사용할 출발지 IP 주소, 터널링 포트, 목적지 IP 주소를 할당하는 명령을 입력

```
Router>enable
```

```
Router#config t
```

```
Router(config)#interface tunnel 2
```

```
Router(config-if)#ip address 172.16.1.2 255.255.0.0
```

```
Router(config-if)#tunnel source FastEthernet0/0
```

```
Router(config-if)#tunnel destination 1.0.0.2
```

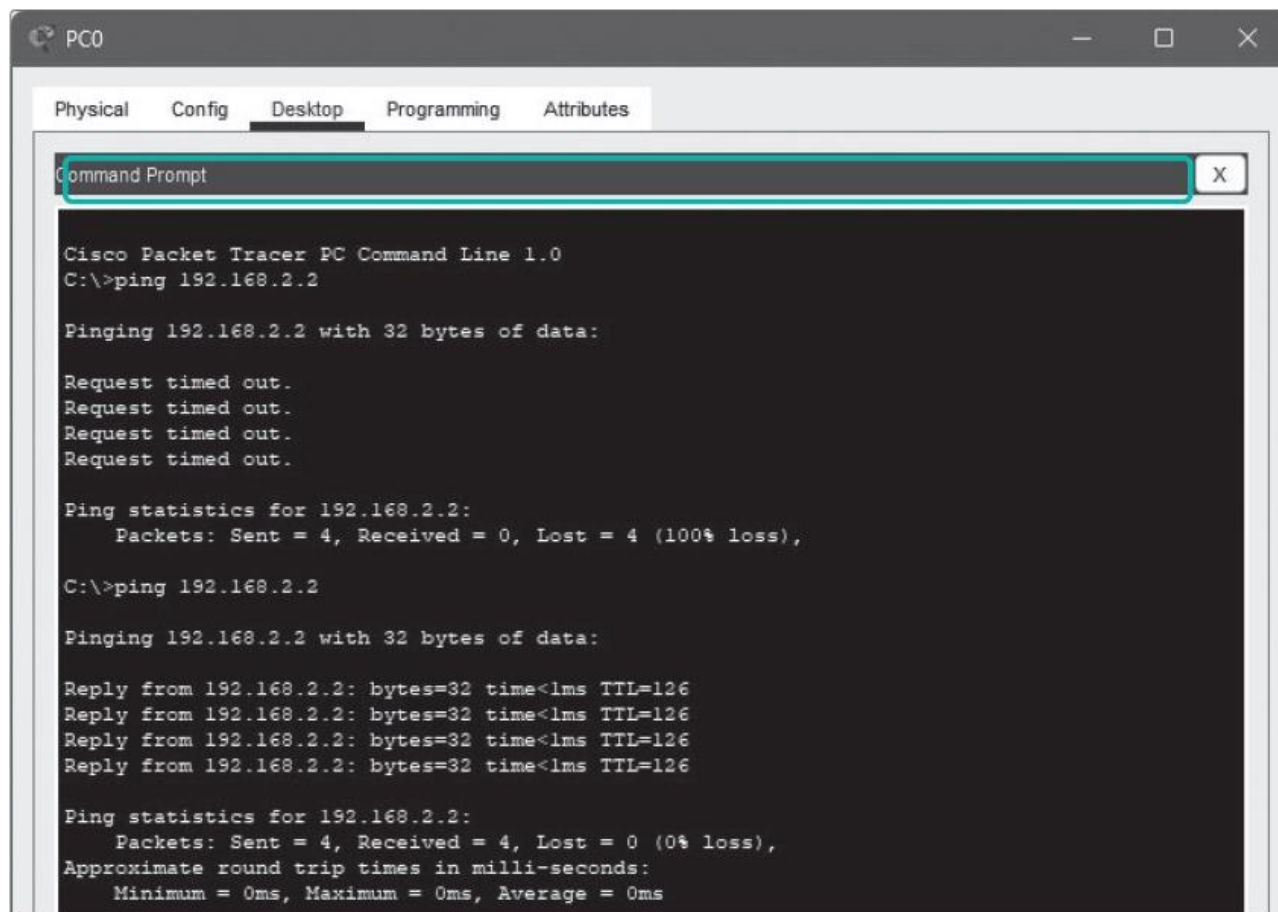
```
Router(config-if)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to up no shut
```


[실습 8-1] 패킷 트레이서에서 VPN 설정하기

6 터널링 설정 확인하기

C:W>ping 192.168.2.2



The screenshot shows a Cisco Packet Tracer PC Command Prompt window for PC0. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, and a Command Prompt window is open. The Command Prompt shows the following text:

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

Pinging 192.168.2.2 with 32 bytes of data:

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

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.2.2

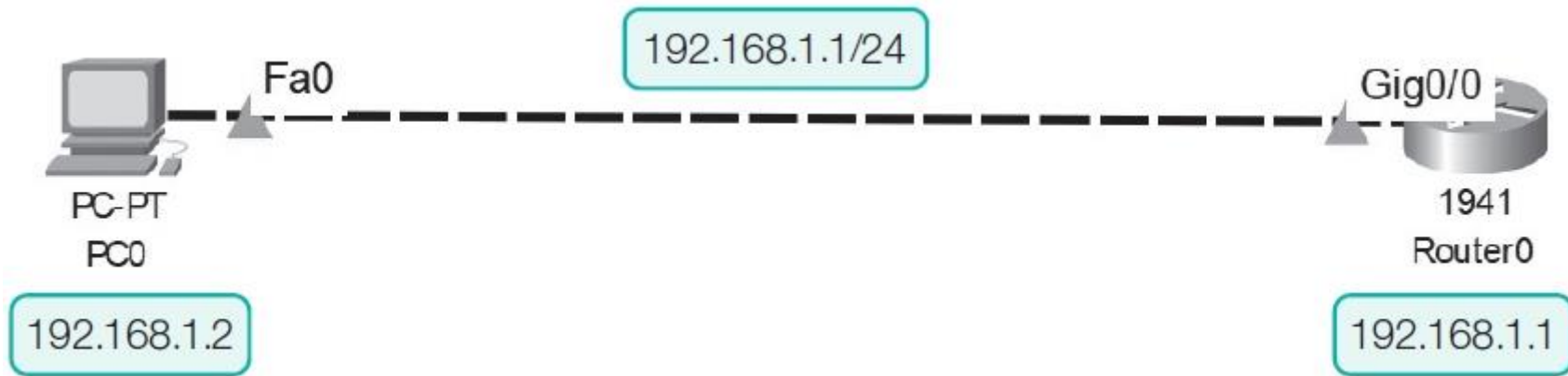
Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<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
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 = 0ms, Average = 0ms
```

[실습 8-2] SSH 터널링하기

- PC0과 Router0을 SSH로 연결한 후 로그인을 통해 원격 PC0에서 Router0를 제어하는 방법을 실습해보기



[실습 8-2] SSH 터널링하기

1 네트워크 구성하기

- 앞의 네트워크 구성도를 참고해 PC 1대, 라우터 1대 연결하기

[실습 8-2] SSH 터널링하기

2 PC 설정하기

- PC0을 클릭한 후 [Desktop]-[IP Configuration] 메뉴를 선택해 IP 주소를 다음과 같이 설정

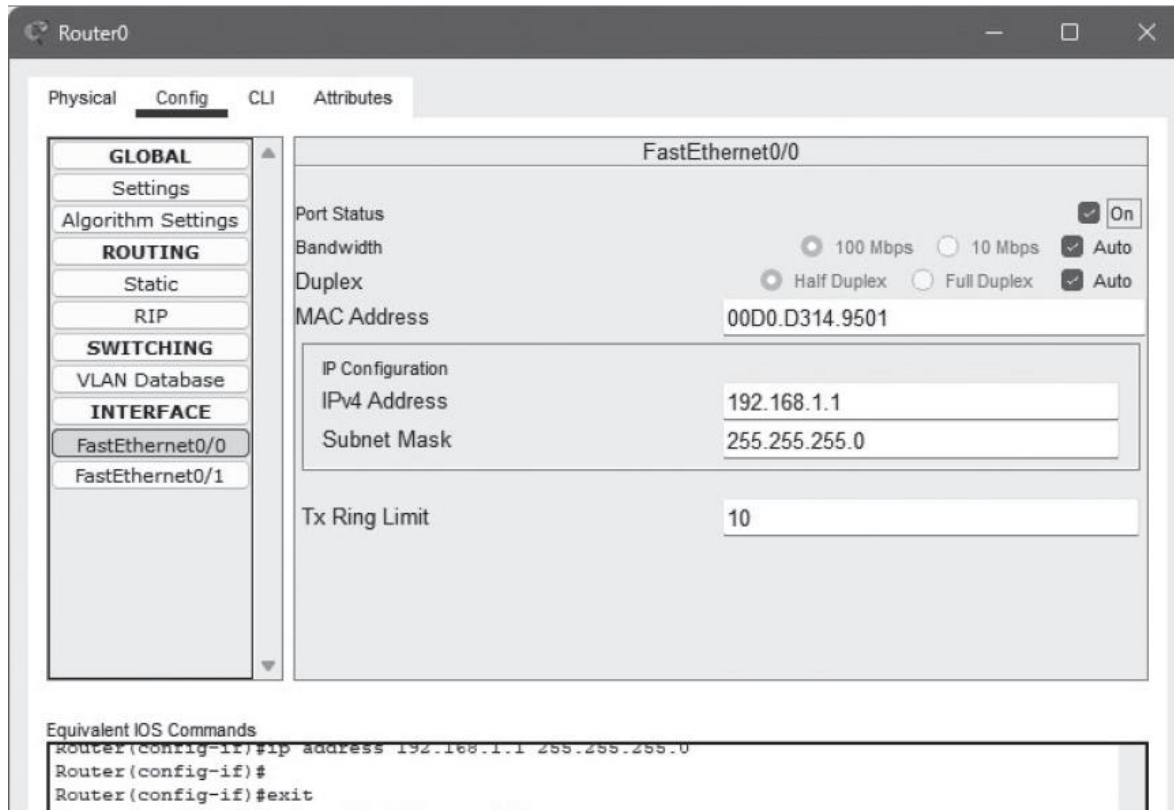
The screenshot shows the configuration window for PC0, specifically the 'Desktop' tab. The 'IP Configuration' sub-tab is active, displaying settings for the 'FastEthernet0' interface. The 'Static' radio button is selected for the IP configuration. The IPv4 Address is set to 192.168.1.2, Subnet Mask to 255.255.255.0, Default Gateway to 192.168.1.1, and DNS Server to 0.0.0.0. The IPv6 Configuration section shows the 'Static' radio button selected, with the IPv6 Address field empty, Link Local Address set to FE80::201:97FF:FE3E:C00, and Default Gateway and DNS Server fields empty. The 802.1X section shows the 'Use 802.1X Security' checkbox unchecked and the Authentication dropdown set to MD5.

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0
IPv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	
Link Local Address	FE80::201:97FF:FE3E:C00
Default Gateway	
DNS Server	
802.1X	
<input type="checkbox"/> Use 802.1X Security	
Authentication	MD5

[실습 8-2] SSH 터널링하기

3 라우터 설정하기

- Router0을 클릭한 후 [Config]-[INTERFACE]-[FastEthernet0/0] 메뉴를 선택해 IPv4 주소를 192.168.1.1로, 서브넷 마스크를 255.255.255.0으로 입력한 후 Port Status의 On을 체크해 PC0의 Fa0과 Router0의 Gig0/0으로 연결



[실습 8-2] SSH 터널링하기

4 SSH 설정하기

4-1 Router1을 클릭한 후 [CLI] 메뉴를 선택해 다음과 같이 명령을 입력하여 SSH를 설정
SSH를 설정하기 위해 RSA 공개키 암호화 방식을 사용

Router(config-if)#ip domain-name ssh1

Router(config)#crypto key generate rsa

% Please define a hostname other than Router.

[실습 8-2] SSH 터널링하기

4-2 hostname 명령을 이용해 Router0의 이름을 변경

Router(config)#hostname sshserver

sshserver(config)#crypto key generate rsa

The name for the keys will be: sshserver.ssh1

Choose the size of the key modulus in the range of 360 to 2048 for your

**General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.**

[실습 8-2] SSH 터널링하기

4-3 RSA 키를 360에서 2048비트까지 설정할 수 있는데, 여기서는 2048비트로 설정

How many bits in the modulus [512]: **2048**

% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

4-4 line 명령으로 다음과 같이 설정

sshserver(config)#**line vty 0 15**

*Mar 1 0:3:30.720: %SSH-5-ENABLED: SSH 1.99 has been enabled

[실습 8-2] SSH 터널링하기

4-5 사용자 등록을 위해 username을 hanbit으로 등록하고, password를 cisco로 설정하고 do wr로 끝을 맺음

```
sshserver(config-line)#transport input ssh
```

```
sshserver(config-line)#ip ssh ver 2
```

```
sshserver(config)#username hanbit privilege 15 password cisco
```

```
sshserver(config)#do wr
```

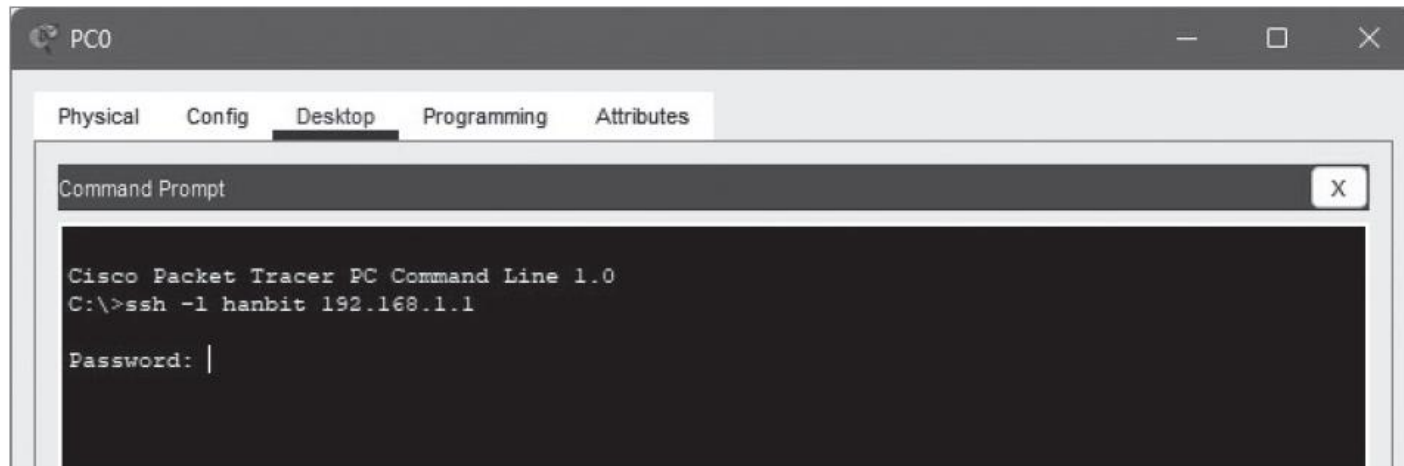
Building configuration...

[OK]

[실습 8-2] SSH 터널링하기

4-6 PC0과 Router0을 SSH 연결로 접속하기 위해 PC0을 클릭한 후 [Desktop]-[Command Prompt] 메뉴를 선택해 다음과 같이 명령을 입력. 패스워드를 물으면 cisco를 입력. 안전한 SSH 채널을 이용해 Router0(호스트 이름은 sshserver)에 접속된 것을 확인 가능

C:\>ssh -l hanbit 192.168.1.1



02 은닉 채널

은닉 채널과 ackcmd 툴

■ 은닉 채널(Covert Channel)

- 기본 통신 채널에 기생하는 것으로, 표면적인 목적 외의 정보나 은닉 메시지를 전송하기 위한 것
- 은닉 메시지는 다른 사람은 볼 수 없고 송신자와 수신자만 알 수 있도록 한 것
 - 은닉 채널 자체가 암호화는 아님

■ ackcmd의 패킷 전송 과정

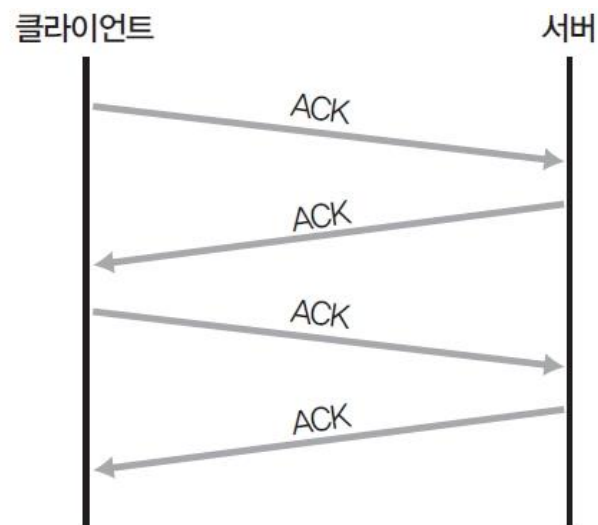


그림 8-4 ackcmd의 패킷 전송 과정

클라이언트와 서버 간의 TCP 통신에서는 목적에 따라 [그림 8-4]와 같이 SYN, ACK, FIN 등의 패킷을 사용한다.

그런데 ackcmd 툴은 ACK 패킷만 이용한다. 즉, 세션이 성립되지 않는다. 그래서 방화벽이나 운영체제 연결 기록도 남지 않는다. TCP의 ACK 패킷을 UDP처럼 사용하는 것과 같다고 생각할 수 있다.

세션 성립 없이 ACK만을 이용해 클라이언트와 서버가 주고받는 형태는 다음과 같다. 단순히 ACK 패킷만 주고받는 것처럼 보이지만 실제로는 ACK 패킷 안에 숨겨진 데이터를 주고받는 것이다.

은닉 채널과 방화벽 우회

- 은닉 채널은 데이터를 숨겨 방화벽을 우회하는 데 사용하기도 함
- 공격자가 방화벽 안에 있는 웹 서버와 통신하려면?
 - ackcmd는 공격자가 공격 대상 서버의 웹 서비스를 이용할 때 발생하는 것과 유사한 형태로 ACK 패킷을 발생시켜 서로 통신을 수행하게 됨

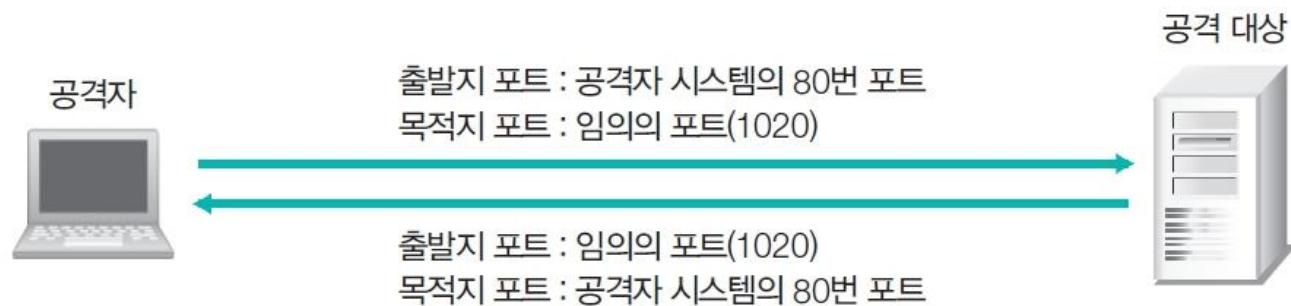
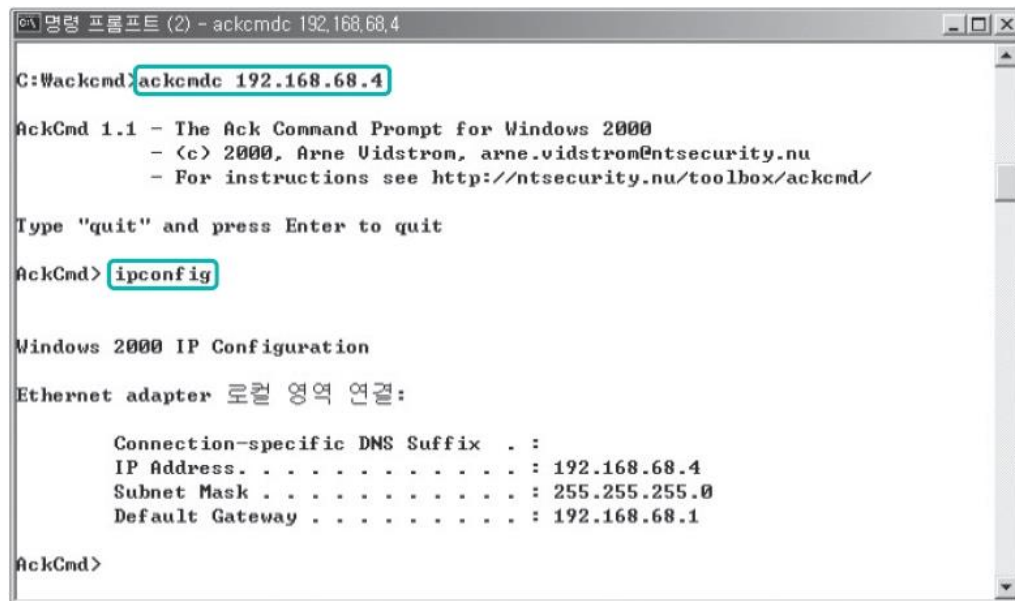


그림 8-5 ackcmd 패킷의 통신 포트

은닉 채널과 방화벽 우회

- ackcmd 툴이 통신하는 패킷을 캡처해보면 ACK 패킷으로 통신을 수행하고 있음을 확인
- 클라이언트로 서버에 접속해 ipconfig 명령을 수행한 후 내용을 열람하면 다음과 같음



```
명령 프롬프트 (2) - ackcmd 192.168.68.4
C:\Wackcmd>ackcmd 192.168.68.4

AckCnd 1.1 - The Ack Command Prompt for Windows 2000
- <c> 2000, Arne Vidstrom, arne.vidstrom@ntsecurity.nu
- For instructions see http://ntsecurity.nu/toolbox/ackcmd/

Type "quit" and press Enter to quit

AckCnd> ipconfig

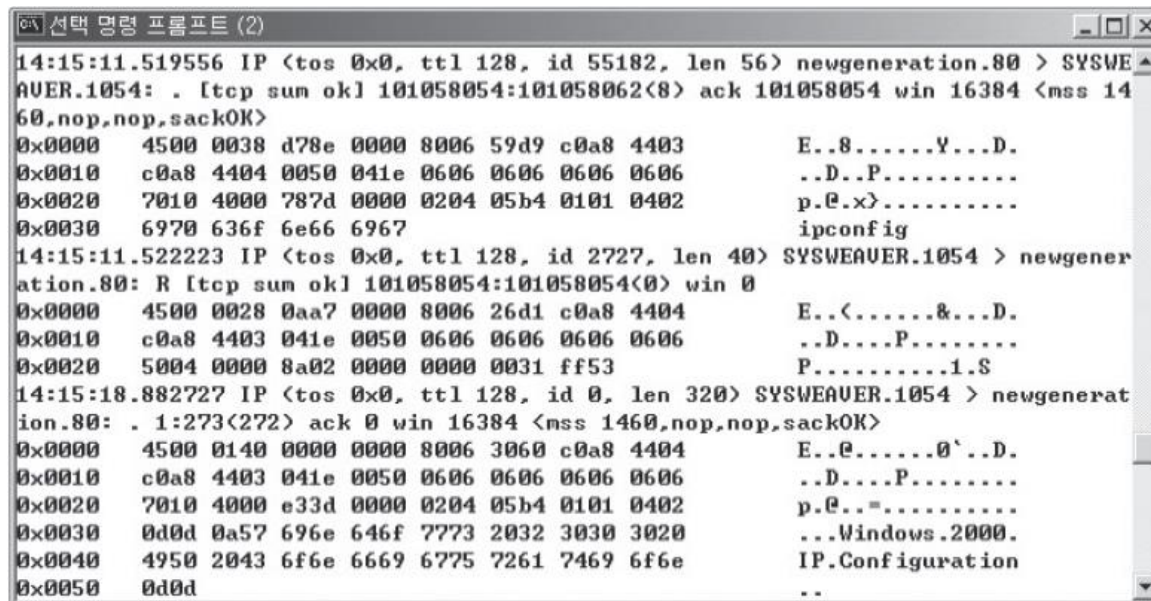
Windows 2000 IP Configuration

Ethernet adapter 로컬 영역 연결:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.68.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.68.1

AckCnd>
```

(a) ackcmd 접속 후 IP 확인 결과



```
선택 명령 프롬프트 (2)
14:15:11.519556 IP <tos 0x0, ttl 128, id 55182, len 56> newgeneration.80 > SYSWEAVER.1054: . [tcp sum ok] 101058054:101058062<8> ack 101058054 win 16384 <mss 1460,nop,nop,sackOK>
0x0000 4500 0038 d78e 0000 8006 59d9 c0a8 4403 E..8.....Y...D.
0x0010 c0a8 4404 0050 041e 0606 0606 0606 0606 ..D..P.....
0x0020 7010 4000 787d 0000 0204 05b4 0101 0402 p.e.x>.....
0x0030 6970 636f 6e66 6967 ipconfig
14:15:11.522223 IP <tos 0x0, ttl 128, id 2727, len 40> SYSWEAVER.1054 > newgeneration.80: R [tcp sum ok] 101058054:101058054<0> win 0
0x0000 4500 0028 0aa7 0000 8006 26d1 c0a8 4404 E..<.....&...D.
0x0010 c0a8 4403 041e 0050 0606 0606 0606 0606 ..D....P.....
0x0020 5004 0000 8a02 0000 0000 0031 ff53 P.....1.S
14:15:18.882727 IP <tos 0x0, ttl 128, id 0, len 320> SYSWEAVER.1054 > newgeneration.80: . 1:273<272> ack 0 win 16384 <mss 1460,nop,nop,sackOK>
0x0000 4500 0140 0000 0000 8006 3060 c0a8 4404 E..e.....0`..D.
0x0010 c0a8 4403 041e 0050 0606 0606 0606 0606 ..D....P.....
0x0020 7010 4000 e33d 0000 0204 05b4 0101 0402 p.e..=.....
0x0030 0d0d 0a57 696e 646f 7773 2032 3030 3020 ...Windows.2000.
0x0040 4950 2043 6f6e 6669 6775 7261 7469 6f6e IP.Configuration
0x0050 0d0d ..
```

(b) ackcmd 통신 시 패킷 내용

그림 8-6 ackcmd 패킷의 통신

[실습 8-3] 셀 백도어 설치하고 이용하기

- 실습 환경
- 클라이언트 시스템: 우분투 데스크톱
 - 서버 시스템: 우분투 서버
 - 필요 프로그램: dns2tcp

[실습 8-3] 셸 백도어 설치하고 이용하기

1 dns2tcp 설치하기

1-1 서버와 클라이언트에서 apt-get 명령으로 dns2tcp를 설치

(sudo) apt-get install dns2tcp

1-2 서버의 경우 dns2tcpd 명령으로 관련 옵션을 확인할 수 있음

dns2tcpd

```
root@ubuntu-S-16: /  
root@ubuntu-S-16:/# dns2tcpd  
Usage : dns2tcpd [ -i IP ] [ -F ] [ -d debug_level ] [ -f config-file ] [ -p pid  
file ]  
        -F : dns2tcpd will run in foreground  
root@ubuntu-S-16:/#
```


[실습 8-3] 셸 백도어 설치하고 이용하기

1 dns2tcp 설치하기

1-3 클라이언트도 dns2tcp 명령으로 다양한 관련 옵션을 확인할 수 있음

dns2tcp

```
root@ubuntu-14: /
root@ubuntu-14:/# dns2tcp
No DNS given, using 127.0.1.1 (first entry found in resolv.conf)
Missing parameter : need a dns zone
dns2tcp v0.5.2 ( http://www.hsc.fr/ )
Usage : dns2tcp [options] [server]
    -c                : enable compression
    -z <domain>       : domain to use (mandatory)
    -d <1|2|3>        : debug_level (1, 2 or 3)
    -r <resource>      : resource to access
    -k <key>           : pre-shared key
    -f <filename>      : configuration file
    -l <port|->        : local port to bind, '-' is for stdin (mandatory if resource defined without program )
    -e <program>       : program to execute
    -t <delay>         : max DNS server's answer delay in seconds (default is 3)
    -T <TXT|KEY>       : DNS request type (default is TXT)
    server            : DNS server to use
    If no resources are specified, available resources will be printed
root@ubuntu-14:/#
```

[실습 8-3] 셸 백도어 설치하고 이용하기

2 dns2tcp 서버 실행하기

2-1 dns2tcp 서버를 실행하기에 앞서 설정 파일을 만들어보기

dns2tcpd_config라는 파일을 다음과 같이 설정함

(sudo) vi ./dns2tcpd_config

```
root@ubuntu-S-16: /
listen = 0.0.0.0
port = 53
user = nobody
chroot = /home/nobody/
pid_file = /var/run/dns2tcp.pid
domain = dns2tcp.wishfree.com
key = secretkey
resources = ssh:127.0.0.1:22
```

1,1 All

[실습 8-3] 셸 백도어 설치하고 이용하기

2 dns2tcp 서버 실행하기

2-2 설정한 dns2tcpd_config를 이용해 dns2tcp 서버를 실행

이때 -d 옵션은 debug level 옵션으로, 실행 시 로그를 확인할 수 있음

(sudo) dns2tcpd -d 3 -f ./dns2tcpd_config

```
root@ubuntu-S-16: /  
root@ubuntu-S-16:/# dns2tcpd -d 3 -f ./dns2tcpd_config  
18:30:13 : Debug options.c:97   Add resource ssh:127.0.0.1 port 22  
18:30:13 : Debug socket.c:55   Listening on 0.0.0.0:53 for domain dns2tcp.wishf  
ree.com  
root@ubuntu-S-16:/#
```

[실습 8-3] 셸 백도어 설치하고 이용하기

2 dns2tcp 서버 실행하기

2-3 dns2tcp 서버를 실행한 후에는 netstat 명령을 통해 UDP 53번 포트가 dns2tcpd에 의해 열려 있음을 확인할 수 있음

53번 포트를 named가 같은 다른 프로그램이 사용하고 있다면 에러가 발생. 이 경우에는 kill 명령으로 해당 프로세스를 죽인 뒤 dns2tcpd를 실행

```
root@ubuntu-S-16: /
root@ubuntu-S-16:/# netstat -anp | grep 53
udp        0      0 0.0.0.0:53          0.0.0.0:*
20232/dns2tcpd
unix  2      [ ACC ]     STREAM  LISTENING   12534      1/init      /
run/snapd.socket
unix  2      [ ACC ]     STREAM  LISTENING   12539      1/init      /
run/uuid/request
unix  3      [   ]     STREAM  CONNECTED   35371      12680/vsftpd
unix  3      [   ]     STREAM  CONNECTED   35372      1/init      /
run/systemd/journal/stdout
root@ubuntu-S-16:/#
```

[실습 8-3] 셸 백도어 설치하고 이용하기

3 dns2tcp 클라이언트 실행하기

3-1 로컬 포트와 dns2tcp 서버의 IP 정보 등을 담고 있는 dns2tcpc_config 파일을 다음과 같이 설정

```
root@ubuntu-14: /  
domain = dns2tcp.wishfree.com  
resource = ssh  
local_port = 2222  
key = secretkey  
debug_level = 3  
server = 192.168.0.2
```

3-2 설정한 dns2tcpc_config를 이용해 dns2tcp 클라이언트를 실행
(sudo) dns2tcpc -f ./dns2tcpc_config

```
root@ubuntu-14: /  
root@ubuntu-14:/# dns2tcpc -f ./dns2tcpc_config  
debug level 3  
Debug socket.c:233      Create socket for dns : '192.168.0.2'  
Listening on port : 2222  
When connected press enter at any time to dump the queue
```

[실습 8-3] 셸 백도어 설치하고 이용하기

3 dns2tcp 클라이언트 실행하기

3-3 local_port 항목으로 설정한 2222번 포트에 대한 연결을 확인해보면, TCP 2222 포트가 dns2tcp에 의해 열려 있음

```
root@ubuntu-14: /  
root@ubuntu-14:/# netstat -anp | grep 2222  
tcp        0      0 127.0.0.1:2222      0.0.0.0:*          LISTEN  
28432/dns2tcp  
root@ubuntu-14:/#
```

[실습 8-3] 셸 백도어 설치하고 이용하기

4 dns2tcp를 이용해 통신 연결하기

4-1 dns2tcp를 이용해 ssh로 연결

ssh wishfree@127.0.0.1 -p 2222 -D 6789

```
wishfree@ubuntu-S-16: ~  
root@ubuntu-14:/# ssh wishfree@127.0.0.1 -p 2222 -D 6789  
wishfree@127.0.0.1's password:  
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-28-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com/  
  
86 packages can be updated.  
0 updates are security updates.  
  
Last login: Sun Jul 10 18:08:13 2016 from 127.0.0.1  
wishfree@ubuntu-S-16:~$
```

실행 옵션	내용
wishfree@127.0.0.1	로컬 시스템(127.0.0.1)의 wishfree 계정으로 로그인
-p 2222	목적지 포트는 2222번
-D 6789	출발지 포트는 6789번

[실습 8-3] 셸 백도어 설치하고 이용하기

4 dns2tcp를 이용해 통신 연결하기

4-2 dns2tcp 통신 패킷을 확인하면 다음과 같이 dns2tcpd에서 DNS 응답 패킷을 보내주는 형태

```
root@ubuntu-14: /
19:01:30.675572 IP (tos 0x0, ttl 64, id 18293, offset 0, flags [DF], proto UDP (
17), length 102)
192.168.0.2.domain > 192.168.0.200.47356: 46337* 1/0/0 +FIB1wHvBA.dns2tcp.wi
shfree.com. TXT "A+FIAAHvEA" "" (74)
0x0000: 4500 0066 4775 4000 4011 70f7 c0a8 0002 E..fGu@.@.p.....
0x0010: c0a8 00c8 0035 b8fc 0052 e2ab b501 8580 .....5...R.....
0x0020: 0001 0001 0000 0000 0a2b 4649 4231 7748 .....+FIB1wH
0x0030: 7642 4107 646e 7332 7463 7008 7769 7368 vBA.dns2tcp.wish
0x0040: 6672 6565 0363 6f6d 0000 1000 01c0 0c00 free.com.....
0x0050: 1000 0100 0000 0300 0d0b 412b 4649 4141 .....A+FIAA
0x0060: 4148 7645 4100 AHvEA.
```