실습개요

네트워크 보안 실습을 통해 방화벽, ACL, NAT 설정 방법을 익히고,
특정 트래픽에 대한 허용/차단 및 주소 변환 기능을 확인한다.

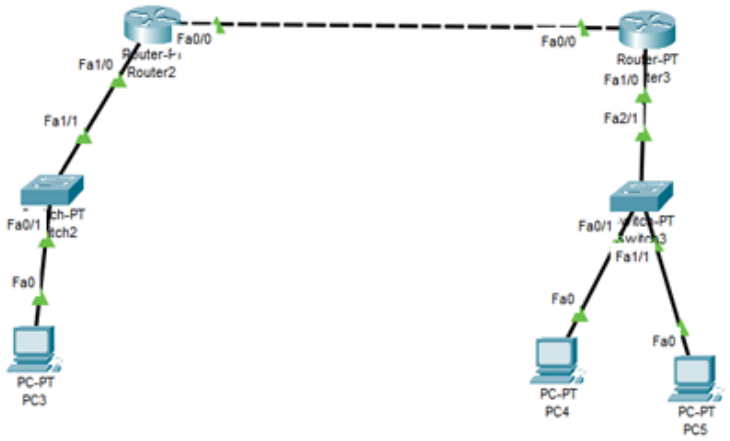
목차

- 표준 ACL 을 이용해 특정 호스트에 대한 ping 허용/거부 설정하기
  - ACL 규칙 생성 및 적용
  - ping 연결 테스트 전/후 비교
- 방화벽을 이용해 IP/ICMP 프로토콜 허용/차단 설정하기
  - 서버 방화벽 규칙 설정 (ICMP 차단, IP 차단, 허용 전환)
  - ping 및 웹 접속 테스트
- NAT 설정하기
  - 내부/외부 인터페이스 지정
  - Static NAT 매핑
  - NAT 적용 전/후 통신 테스트
  - NAT 테이블 확

실습 환경

- 사용 도구:
  - Cisco Packet Tracer

표준 ACL 을 이용해 특정 호스트에 대한 ping 허용/거부 설정하기

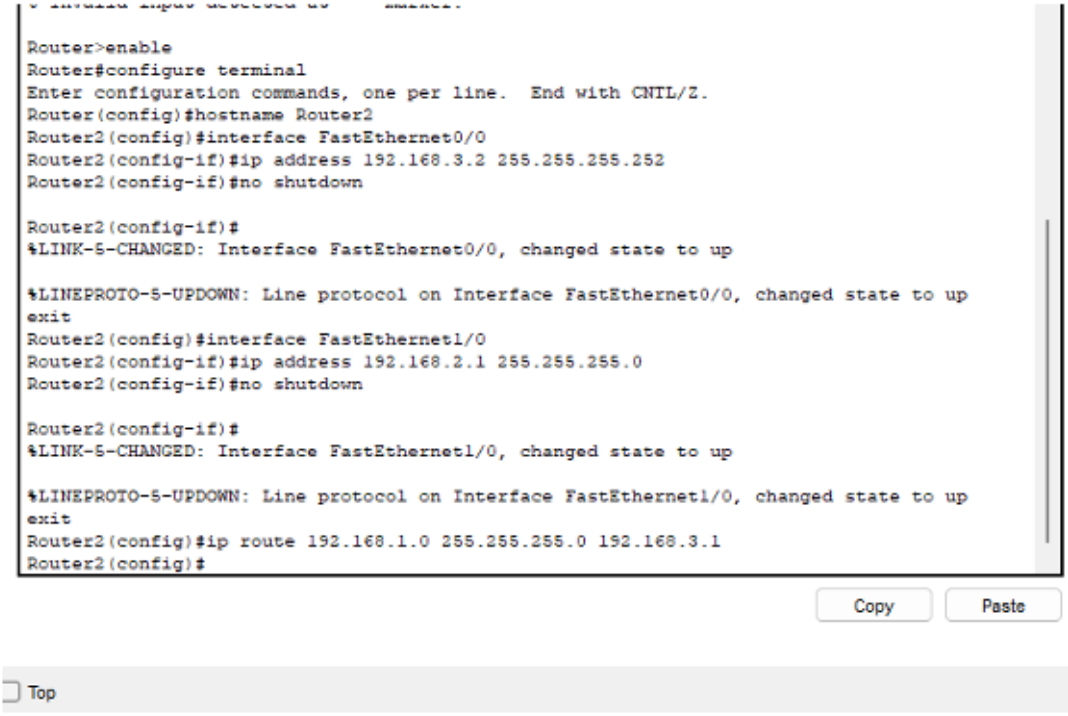


두 개의 LAN 을 라우터를 통해 서로 연결한 기본적인 라우팅 네트워크 구조로 만듦
각 LAN 에는 스위치와 여러 PC 가 있고, 각각의 라우터가 다른 네트워크를 중계

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Router2
Router2(config)#interface FastEthernet0/0
Router2(config-if)#ip address 192.168.3.1 255.255.255.252
Router2(config-if)#no shutdown

Router2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
exit
Router2(config)#interface FastEthernet1/0
Router2(config-if)#ip address 192.168.1.1 255.255.255.0
Router2(config-if)#no shutdown

Router2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
exit
Router2(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
exit
Router2#
%SYS-5-CONFIG_I: Configured from console by console
enable
Router2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)# ip route 192.168.2.0 255.255.255.0 192.168.3.2
Router2(config)#
```

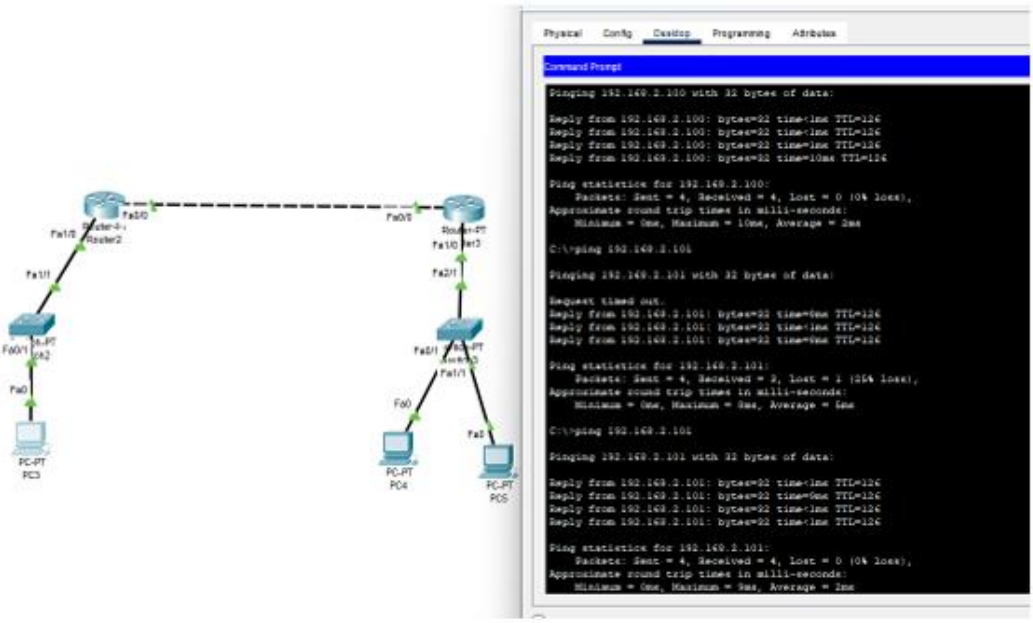
Copy Paste

IP 주소 192.168.3.1 과 서브넷 마스크 255.255.255.252 설정, no shutdown 명령어로 포트 활성화
ip address 192.168.1.1 255.255.255.0
내부 스위치와 연결되어 PC3 같은 내부 호스트들과 통신에 사용
no sutdown 으로 포트 활성화

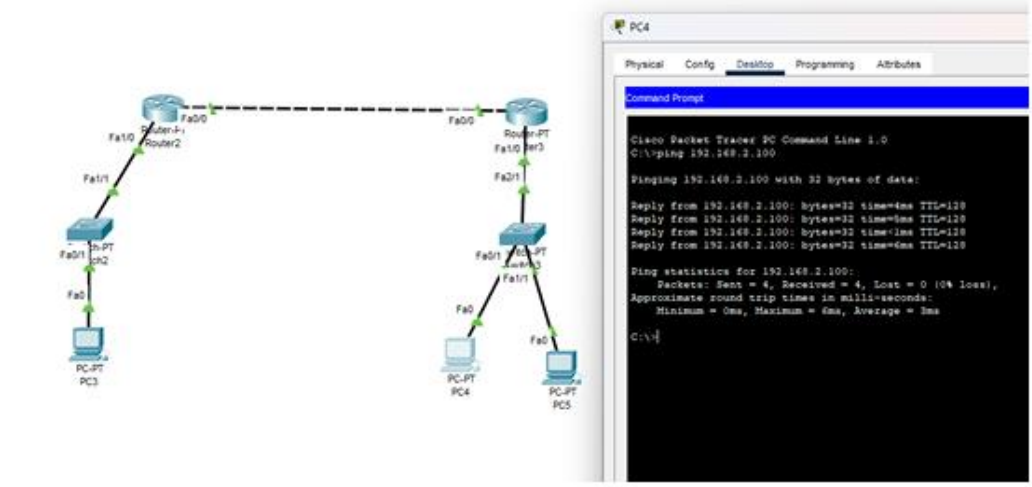


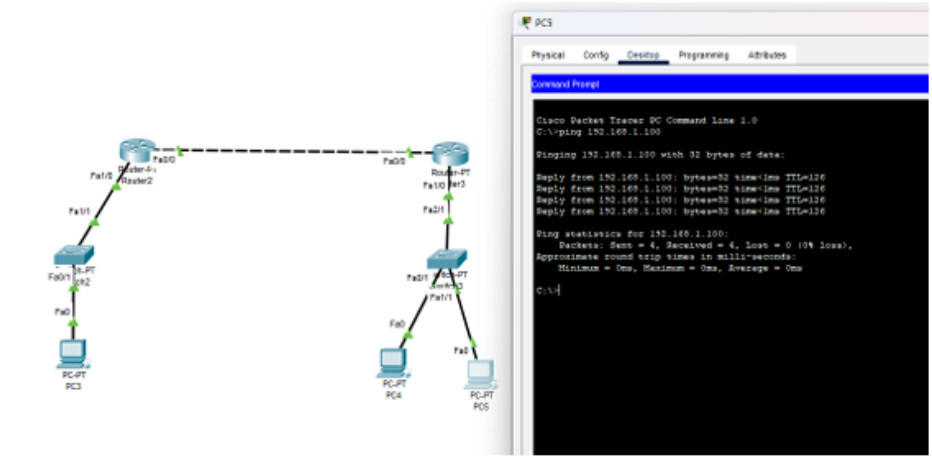
ip address 192.168.3.2 255.255.255.252
IP 주소 192.168.3.2 를 설정 Router2 의 192.168.3.1 과 연결
nos shutdown 으로 포트 활성화
interface FastEthernet1/0
ip address 192.168.2.1 255.255.255.0no shutdown
이 포트는 Switch ↔ PC2 개 연결을 위한 포트
내부 네트워크 주소 192.168.2.0/24 에서 게이트웨이 역할을 수행

Router0(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2
Router1(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1
정적라우팅을 설정하였음

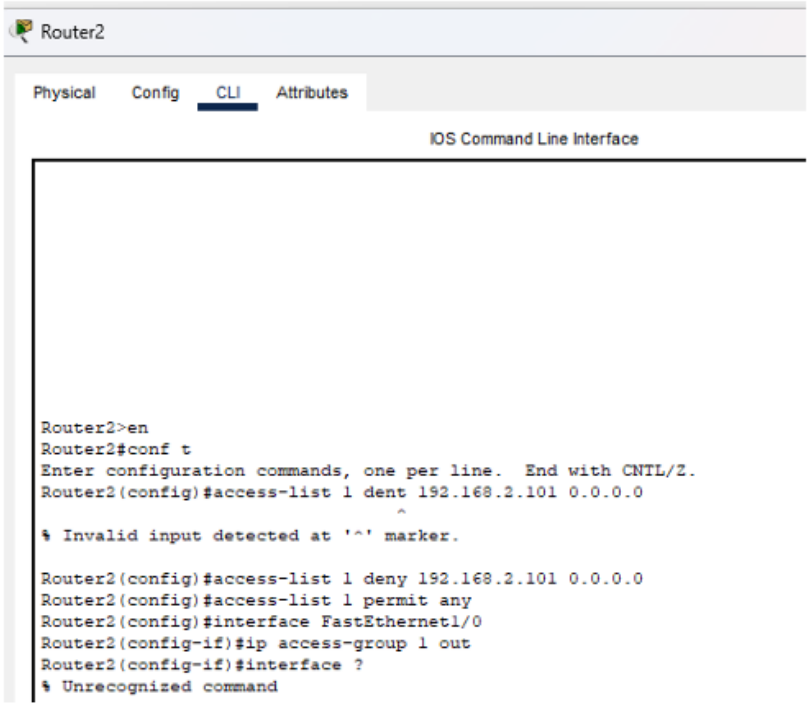


PC3 에서 오른쪽 네트워크의 PC4(192.168.2.100)와 PC5(192.168.2.101) 로 ping 을 보내고 성공적으로 연결이 되었음

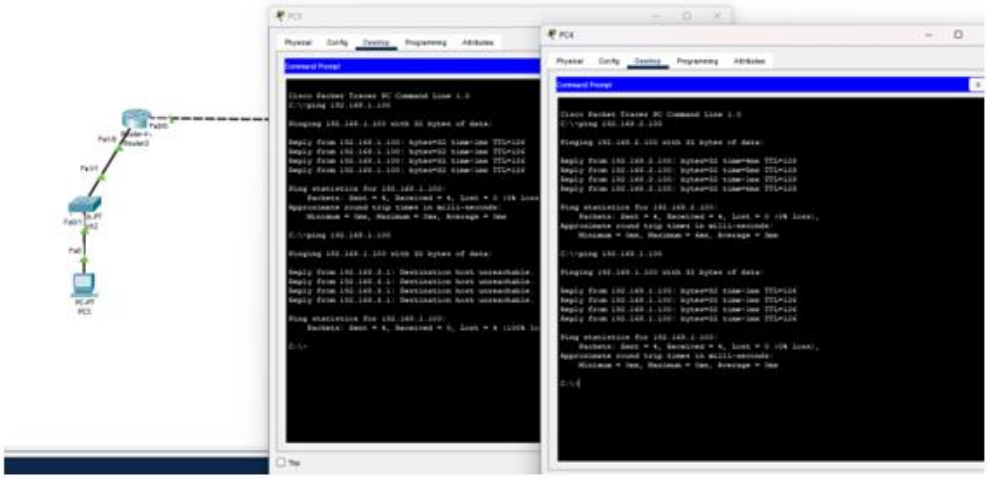




왼쪽 pc d 오른쪽 pc 모두 정상적으로 ping test 로 연결이 정상적으로 되는걸 확인할 수 있음



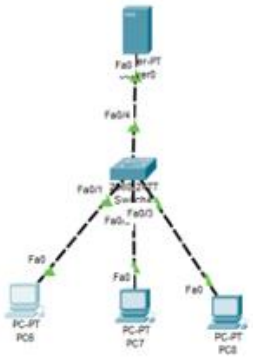
ACL : 192.168.2.101 로부터 나가는 트래픽을 차단하고 나머지는 허용
Router2 의 Fa1/0 인터페이스 내부 LAN 과 연결된 포트에 PC5 의 응답 차단함

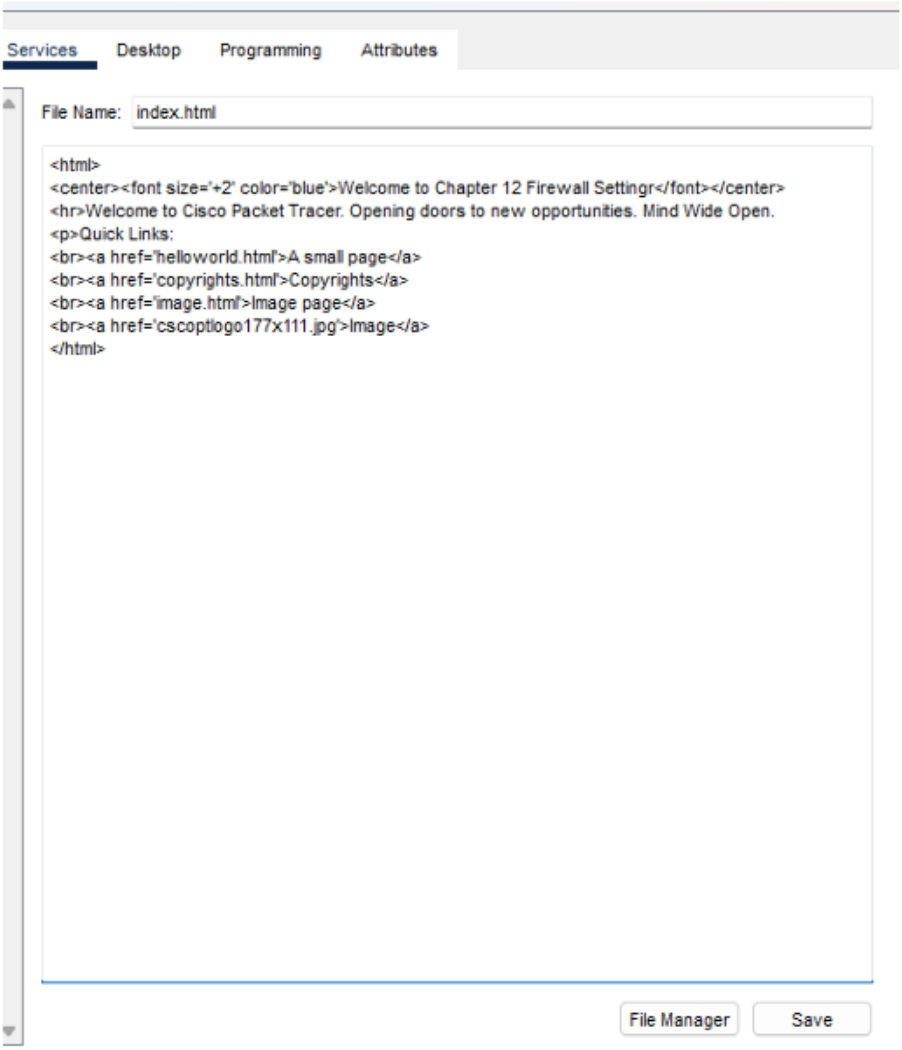


Pc 4 는 ping 192.168.1.100 성공
ACL 에 차단 대상이 아님 → 통신 가능

ping 192.168.1.100 → 실패
ACL 에서 deny 대상이므로 Router2 에서 차단됨

방화벽을 이용해 IP/ICMP 프로토콜 허용/차단 설정하기





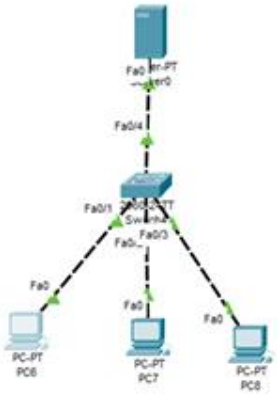
서버설정

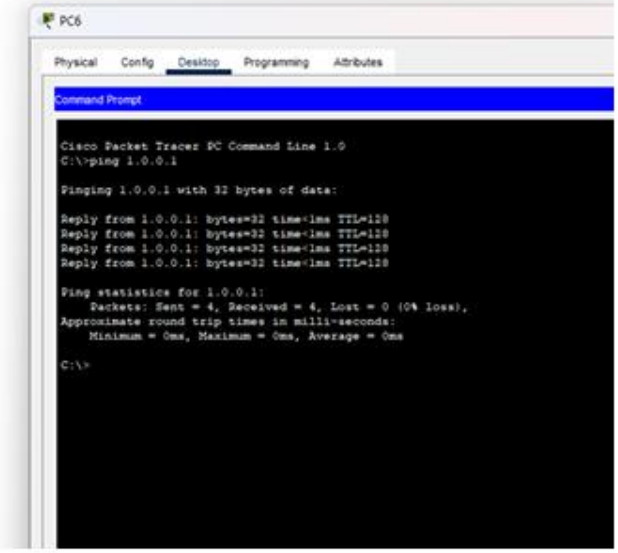
Server0에서 웹 서버 기능을 활성화

Services 탭 → HTTP 항목에서:HTTP: On

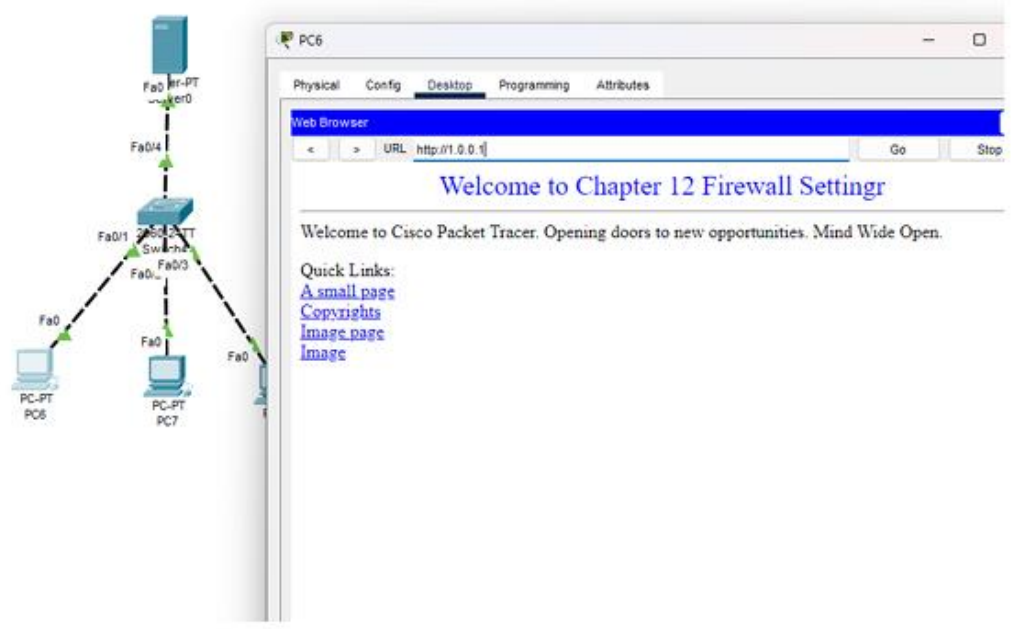
기본 웹 페이지(index.html)는 직접 수정하여 Welcome이 나오도록 하였음

결과적으로, 클라이언트 PC들은 브라우저로 http://서버IP주소 접속 시 웹페이지를 확인할 수 있음.



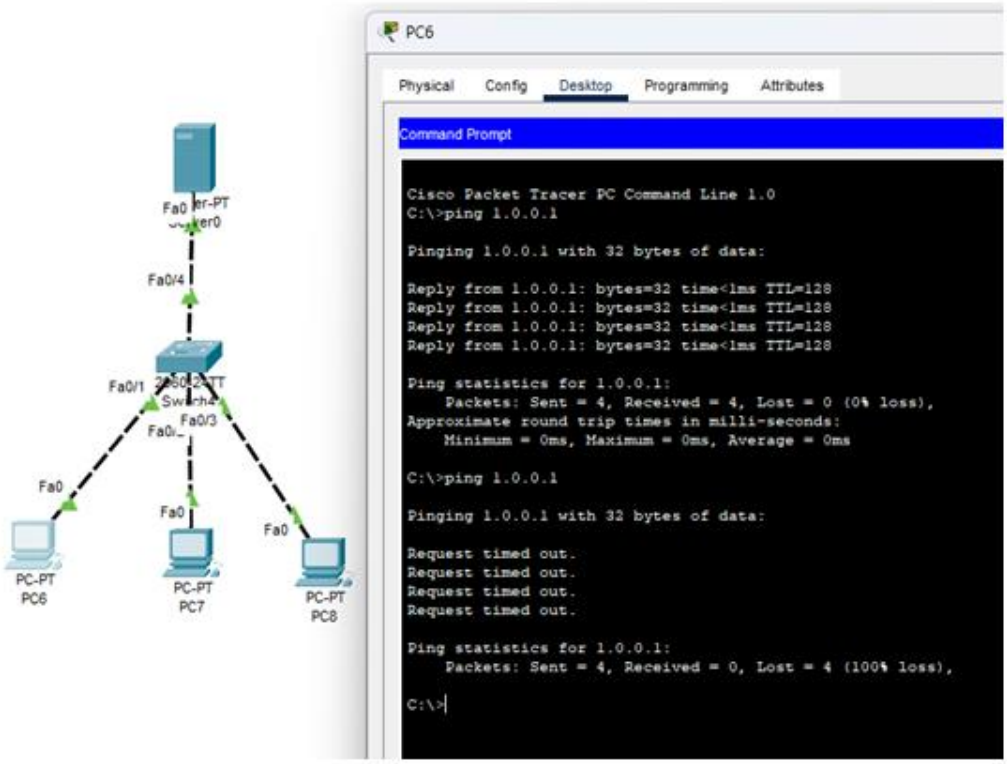


네트워크가 정상적으로 작동을 하였음

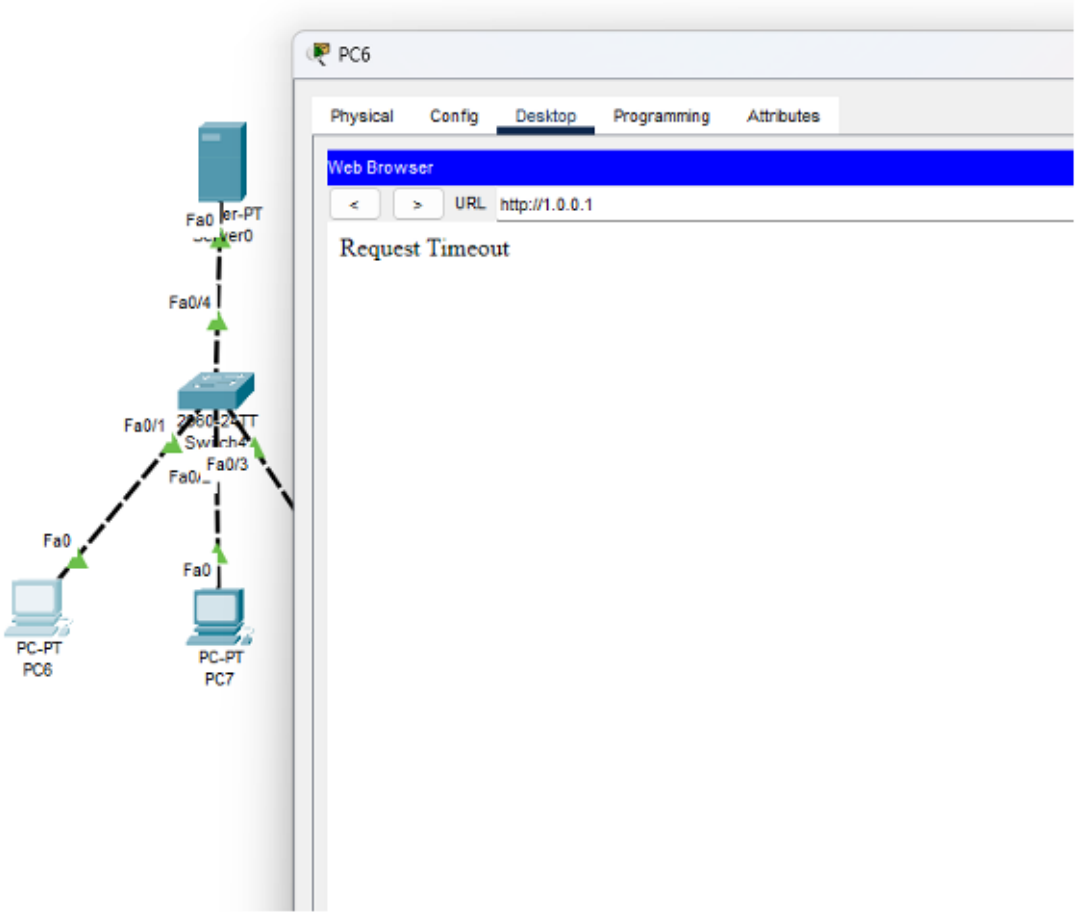


PC 의 웹 브라우저에서 http://1.0.0.1 입력
서버에 저장된 index.html 페이지가 열림
아까 서버에서 index.html 에서 등록했던 페이지임

Server0 의 HTTP 서비스가 요청을 받아 index.html 파일을클라이언트에 전송
PC 가 브라우저가 HTML 을 해석해 화면에 출력
PC 는 DHCP 를 통해 IP, 서브넷 마스크, 게이트웨이 등을 자동으로 할당받음
그래서 Server0 와 같은 네트워크상에서 통신 가능



Action: 'Deny'
Protocol: 'ICMP'
Remote IP: 0.0.0.0
Remote Wildcard Mask: 255.255.255.255
설정을 한 후 서버에 cimp ping 을 보냈더니 Request timed out 이 뜸
icmp: ping 명령어에 사용되는 프로토콜
Remote IP = 0.0.0.0 + Wildcard Mask = 255.255.255.255
모든 IP 주소에서 오는 ICMP 요청을 차단하겠다는 뜻
즉, 누구든지 Server 에게 ping 보내면 거부(Deny) 하겠다는 방화벽 규칙임
서버에서 ICMP 패킷을 ㅂ방화벽이 차단하므로 응답이 오지 않은 것임



Action: 'Deny'

Protocol: 'IP'

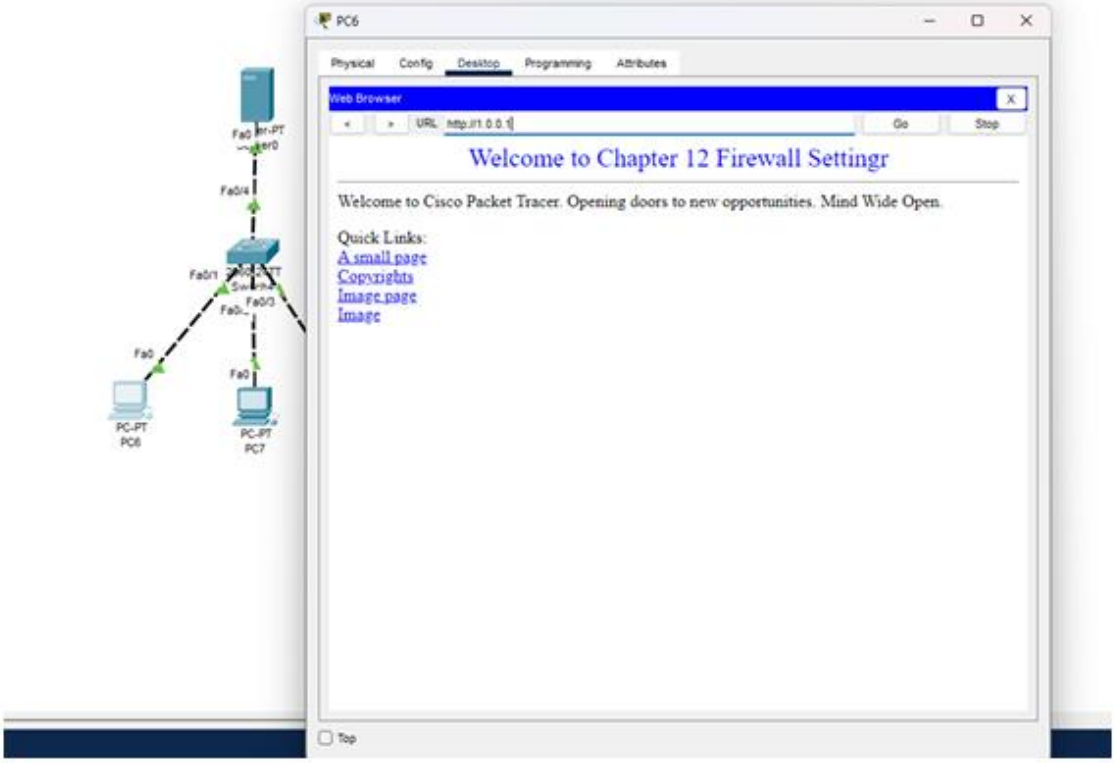
Remote IP: 0.0.0.0

Remote Wildcard Mask: 255.255.255.255

설정을 한 후 웹을 접속해본 결과

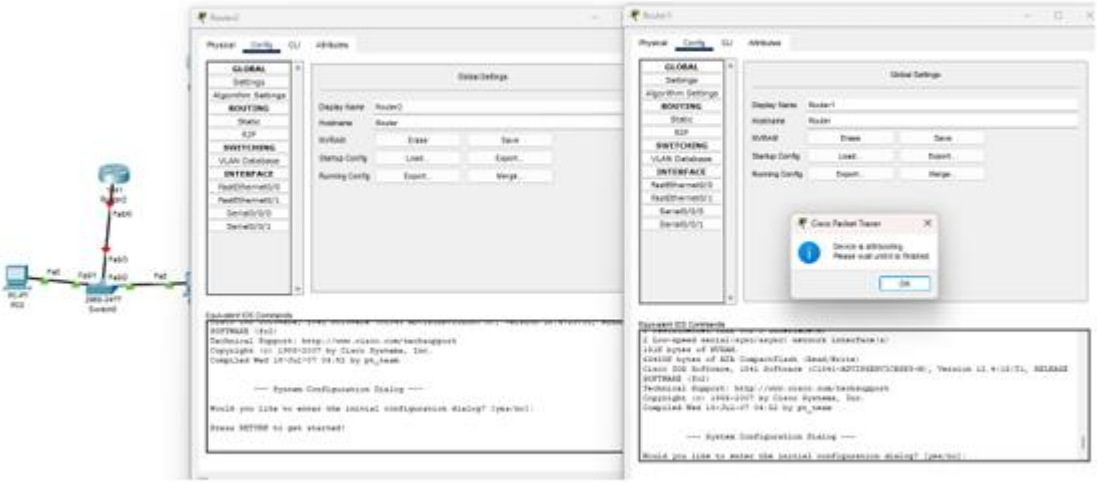
Request Timeout 이 나옴 모든 IP 주소로부터 들어오는 모든 종류의 IP 를 차단한 것임

pc 는 서버의 웹서버의 접속을 시도하지만 방화벽이 모든 IP 트래픽을 차단하여 응답이 없는 상태임

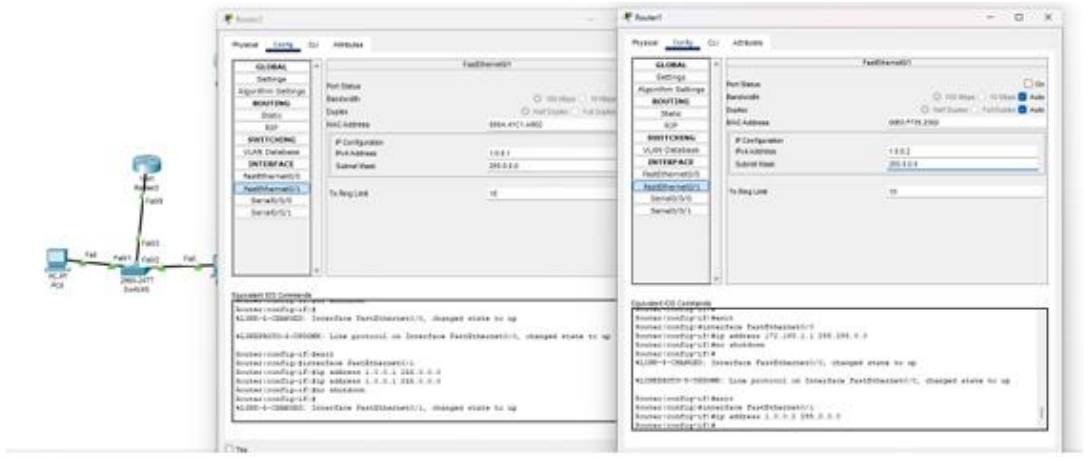


다시 ICPM/IP 프로토콜을 방화벽 규칙에다가 허용을 하면 정상적으로 작동함

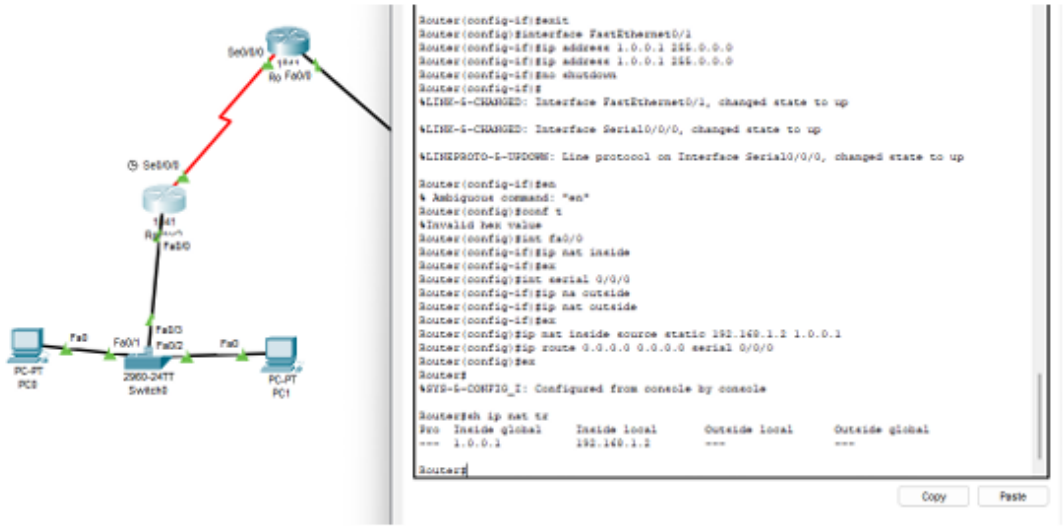
NAT 설정하기



라우터간 연결을 하려면 시리얼 모듈을 설치해야함
기본 라우터에는 시리얼 포트는 탑재되어있지 않기 때문에 추가 모듈을 작창?하여 시리얼 포트가 생김

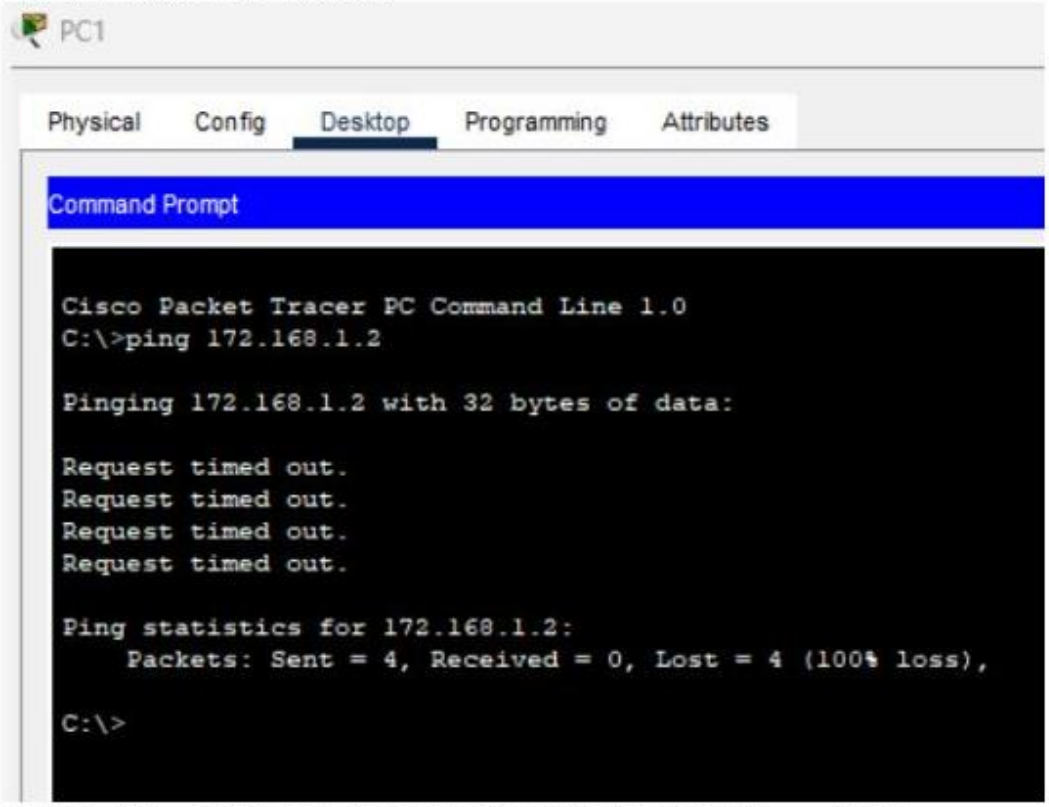


라우팅을 설정하고 시리얼을 활성화 시킴



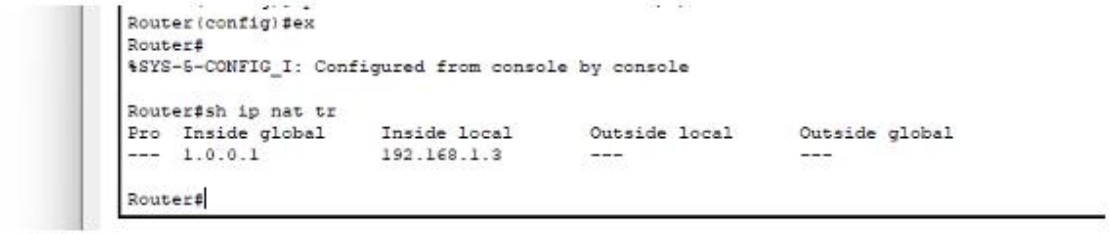
interface fa0/0
ip nat inside
NAT 기본 인터페이스를 지정
ip nat inside source static 192.168.1.2 1.0.0.1 정적 NAT 매핑 설정
내부 IP 192.168.1.2 가 외부에서는 1.0.0.1 로 보이도록 고정 매핑(static NAT)
ip route 0.0.0.0 0.0.0.0 serial 0/0/0
디폴트 게이트웨이 설정
Inside Local: 내부 실제 IP PC→ 192.168.1.2i
Inside Global: 외부에 보여지는 NAT 된 IP 1.0.0.1

매핑에 의해 NAT 가 잘 작동 중임

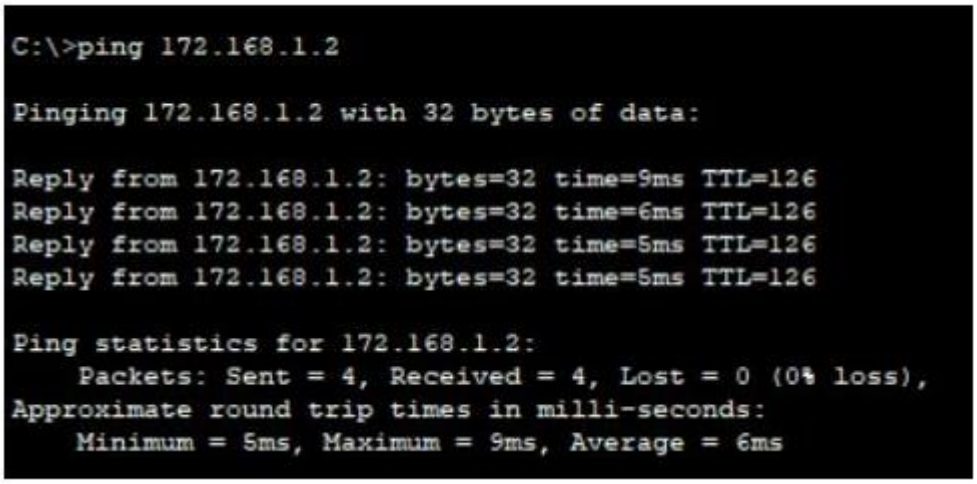


매핑되지 않은 pc1 에서 핑을 보내면 외부와 통신이 되지 않아서 time out 이 뜸

pc1 은 Nat 변환이 안 되어 외부로 나갈 수 없음



pc1 설정



Pc1 을 설정을 하고 나면 이제 pc1도 ping을 보냈을 때 변환이 되어 나간것으로 성공적으로 ping test 를 하였음 방화벽 과제를 수행하고 느낀점 이번 실습을 통해 NAT의 개념과 설정 방법을 직접 적용해보며, 내부 사설 IP가 어떻게 공인 IP 로 변환되어 외부와 통신할 수 있는지를 실제로 체감할 수 있었다. 정적 NAT 설정부터 시리얼 포트 연결, 방화벽 설정, 그리고 ping 테스트를 통해 하나하나 정상 동작을 확인하면서 단순한 이론을 넘어서 네트워크 흐름을 실감할 수 있었다. 특히, NAT를 적용하지 않은 PC가 외부와 통신하지 못하는 문제를 통해 NAT 설정의 중요성과 제한성을 명확히 이해할 수 있었고, PAT나 동적 NAT 방식이 실무에서 더 널리 사용되는 이유도 납득되었다. 또한 방화벽 규칙에 따라 ping이나 웹 접속이 차단되는 것도 직접 확인해보며 보안 설정이 실제로 어떻게 동작하는지 배울 수 있었다. 실습을 통해 얻은 경험은 추후 실제 네트워크 설계나 방화벽, NAT 정책 설정 시 중요한 기반 지식이 될 것이라 느꼈다.