# ▣ 실습 목표

☞ 확장(Extend) ACL(Access Control List)설정 방법을 익히고 라우터에서 패킷필터링 개념과 동작에 대하

여 학습한다

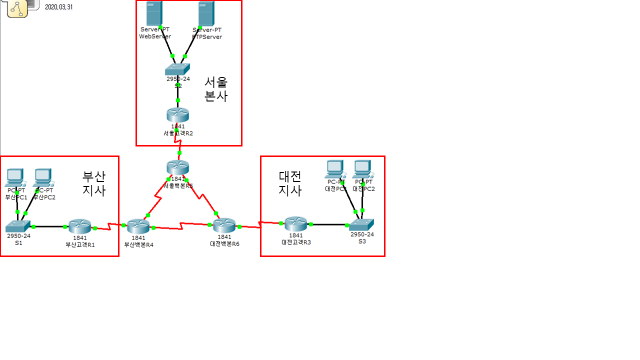
# ▣ 학습 내용

☞ EIGRP 동적 라우팅 설정

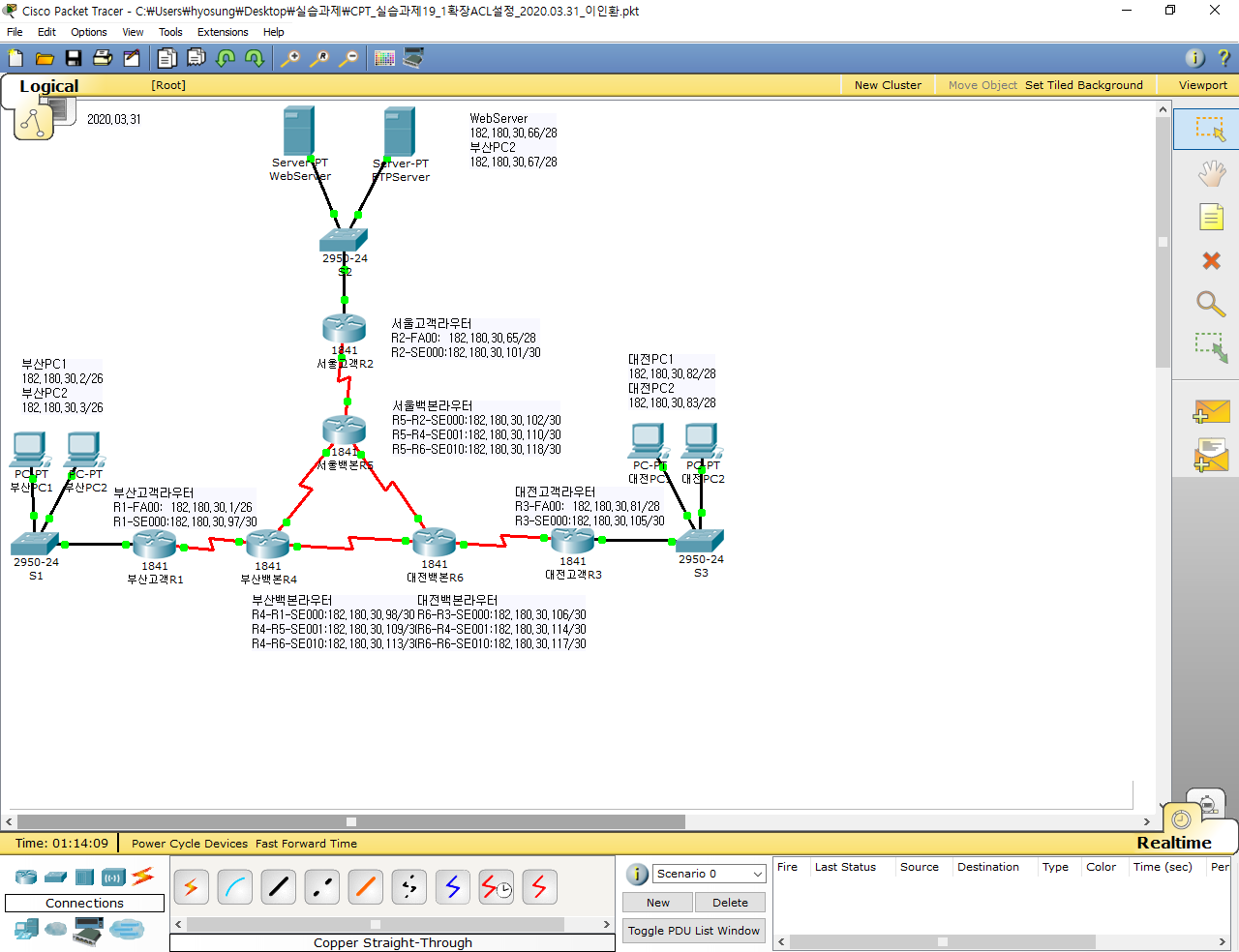
☞ 확장 ACL 설정

# 실습 환경

1. 네트워크 구성도

****

1. 시스코페킷트레이서 구성도



1. TCP/IP 프로토콜 설정(182.180.30.0/25에서 서울 PC 12대, 부산 PC 32대, 대전 PC 8대)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PC TCP/IP 프로토콜 설정 | | | | | |
| PC | | IPv4주소 | 넷마스크 | 게이트웨이 | PC 수 |
| 서울 | WebServer | 182.180.30.66 | 255.255.255.240  /28 | 182.180.30.65 | 12대 |
| FTPServer | 182.180.30.67 |
| 부산 | PC1 | 182.180.30.2 | /26  255.255.255.192 | 182.180.30.1 | 32대 |
| PC2 | 182.180.30.3 |
| 대전 | PC1 | 182.180.30.82 | /28  255.255.255.240 | 182.180.30.81 | 8대 |
| PC2 | 182.180.30.83 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 라우터명 | | FastEthernet0/0  IP 주소 및  서브넷 마스크 | Serial 0/0/0  IP 주소 및  서브넷 마스크 | 인터넷  Serial IP 주소 및  서브넷 마스크 |
| 서울 | R2 | 182.180.30.65 | 182.180.30.101 | 182.180.30.102 |
| 부산 | R1 | 182.180.30.1 | 182.180.30.97 | 182.180.30.98 |
| 대전 | R3 | 182.180.30.81 | 182.180.30.105 | 182.180.30.106 |

# 라우터 기본 설정

단계 1 라우터 시스템 이름 R1 변경 및 enable,enable secret 패스워드 설정 후 확인

☞설정

Router>enable

Router#configure terminal

Router(config)#hosname R1

R1(config)#enable password 1234

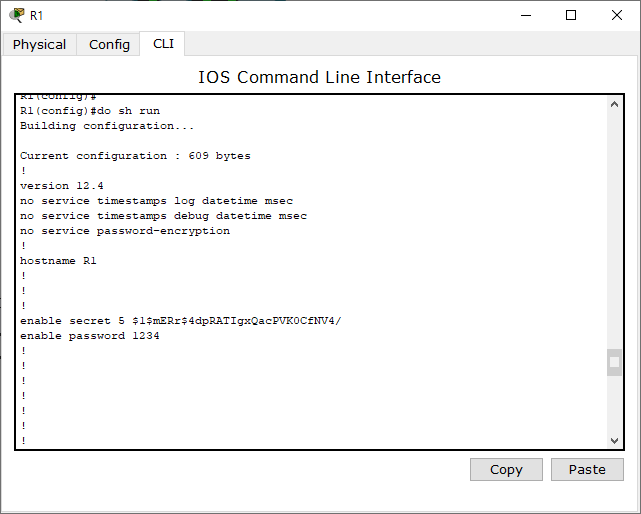
R1(config)#enable secret 1234

☞확인

R1#show running-config

R1(config)#do show running-config

R1(config)#do sh run



단계 2 라우터 Telnet 원격접속 시 VTY 네트워크 보안 환경설정 후 확인

☞설정

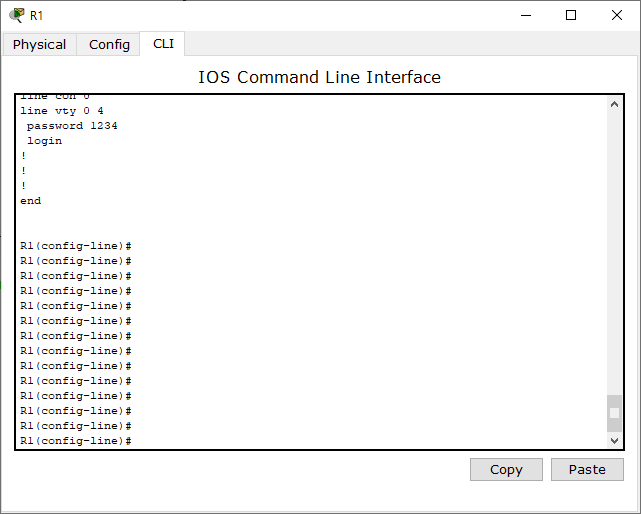
R1(config)#line vty 0 4

R1(config-line)#password 1234

R1(config-line)#login

☞확인

R1(config-line)#do sh run



단계 3 라우터 Console 접속 시 네트워크 보안 환경설정 후 확인

☞설정

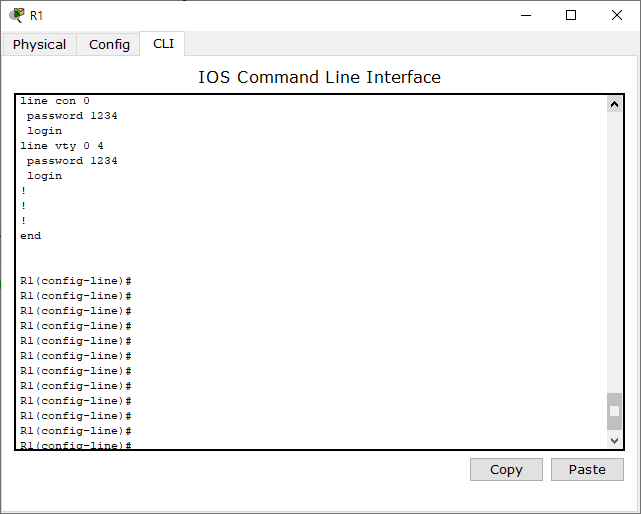
R1(config)#line console 0

R1(config-line)#password 1234

R1(config-line)#login

☞확인

R1(config-line)#do sh run



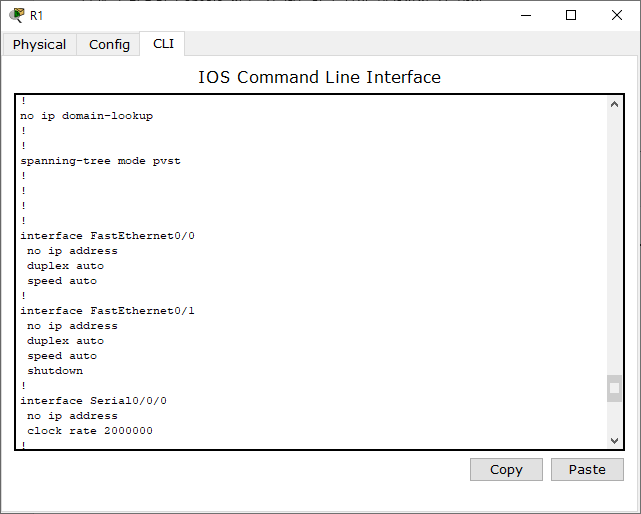
단계 4 라우터 DNA Lookup 기능 해제 설정 후 확인

☞설정

R1(config)#no ip domain-lookup

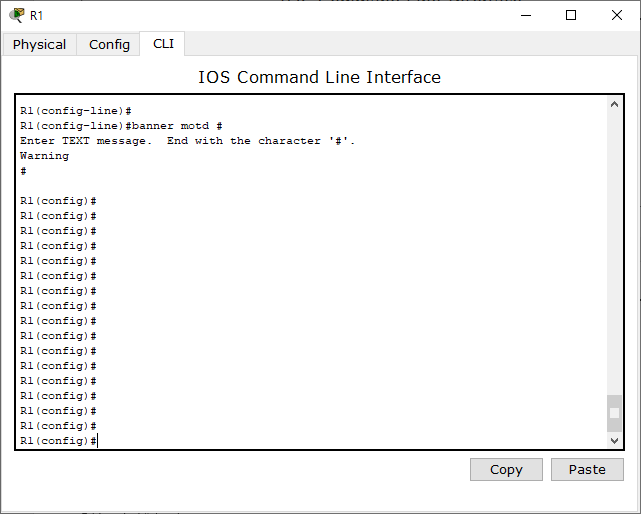
☞확인

R1(config)#do sh run



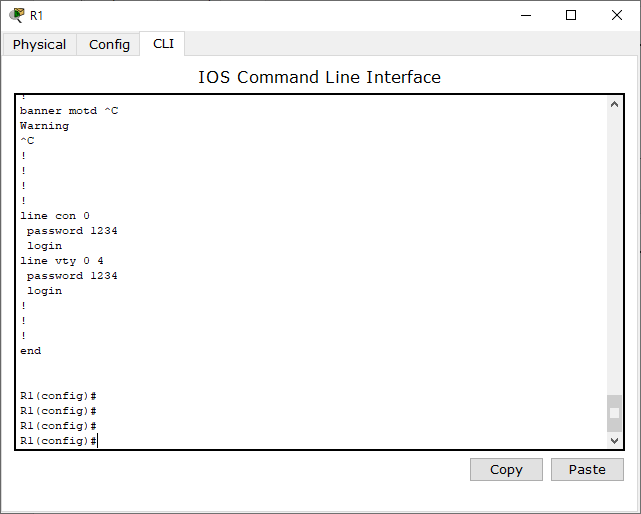
단계 5 라우터 원격 접속 시 경고 배너 메시지 작성 후 확인

☞설정



☞확인

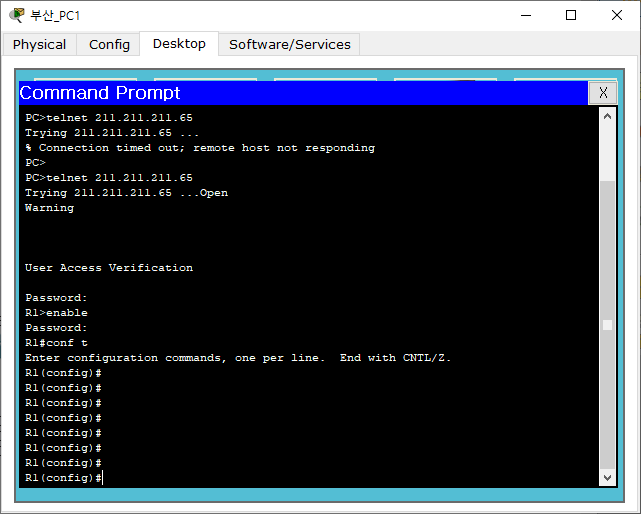
R1(config)#do sh run



단계 6 라우터 원격접속 시 배너 메시지 확인

부산본사 PC1 Command Prompt에서 부산지사 라우터로 접속

☞확인



단계 7 라우터 환경 설정 값 저장하기

☞설정

R1#write

R1#write memory

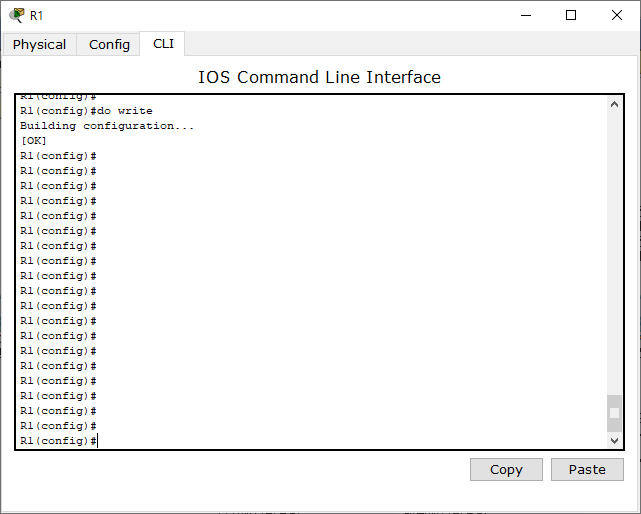
R1#copy running-config startup-config

R1(config)#do write

R1(config)#do write memory

R1(config)#do copy running-config startup-config

☞확인

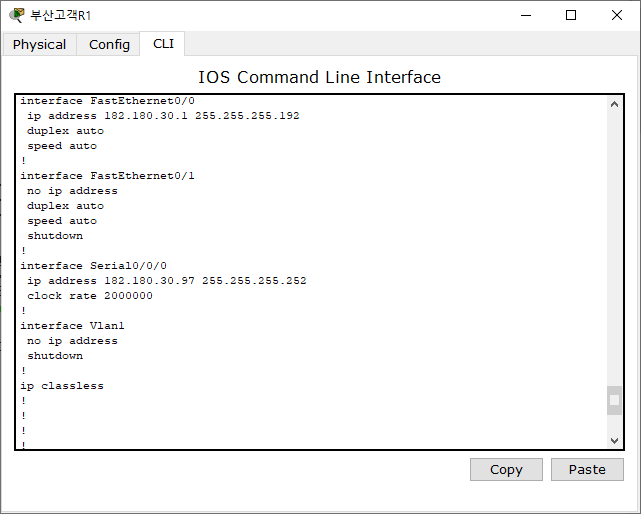


# 라우터 인터페이스 IP 주소 설정하기

단계 01 R1 이더넷 인터페이스 IP주소를 설정하고 확인한다

R1(config)#interface fastEthernet 0/0

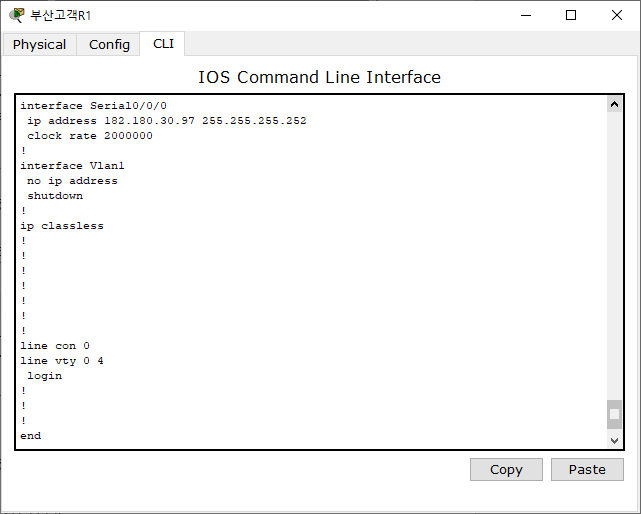
R1(config-if)#ip address 182.180.30.65 255.255.255.192



단계 02 R1 시리얼 인터페이스 IP주소를 설정하고 확인한다

R1(config)#interface Serial 0/0/0

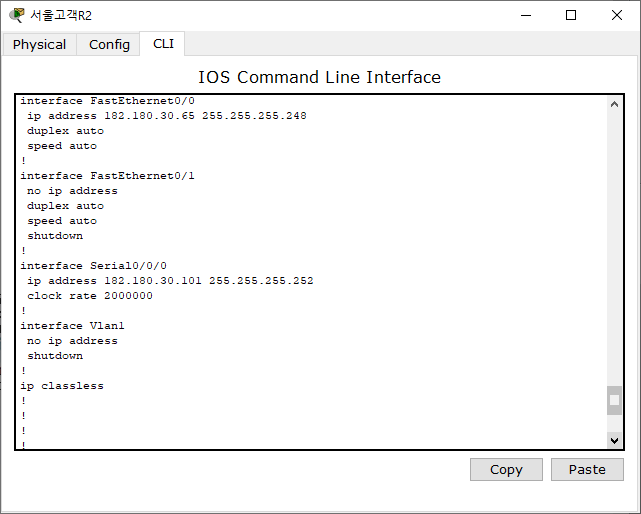
R1(config-if)#ip address 182.180.30.97 255.255.255.252



단계 03 R2 이더넷 인터페이스 IP주소를 설정하고 확인한다

R2(config)#interface fastEthernet 0/0

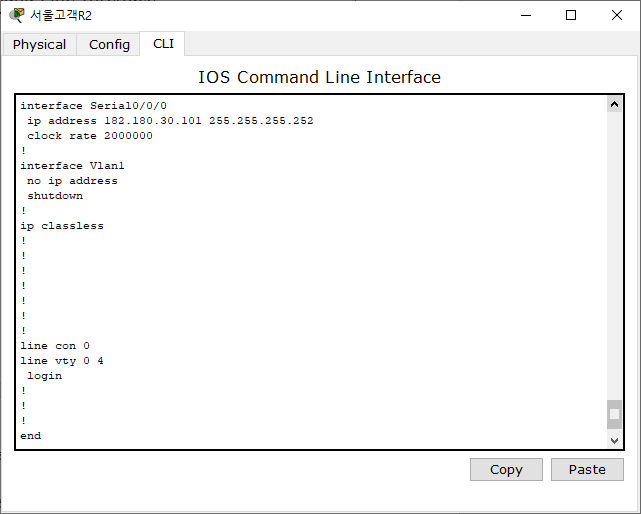
R2(config-if)#ip address 182.180.30.65 255.255.255.248



단계 04 R2 시리얼 인터페이스 IP주소를 설정하고 확인한다

R2(config)#interface Serial 0/0/0

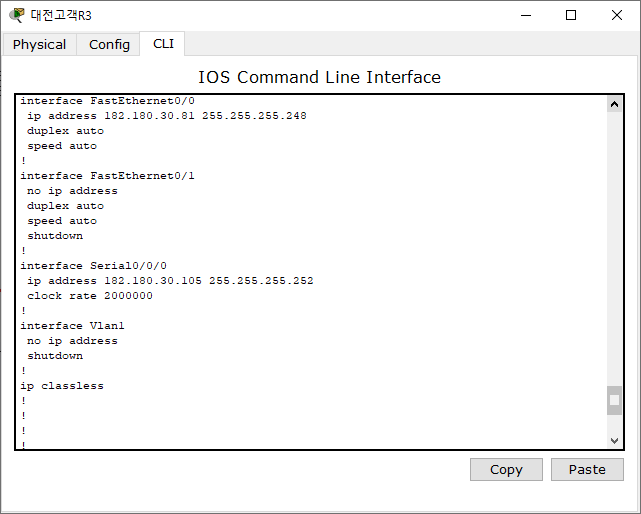
R2(config-if)#ip address 182.180.30.101 255.255.255.252



단계 05 R3 이더넷 인터페이스 IP주소를 설정하고 확인한다

R3(config)#interface fastEthernet 0/0

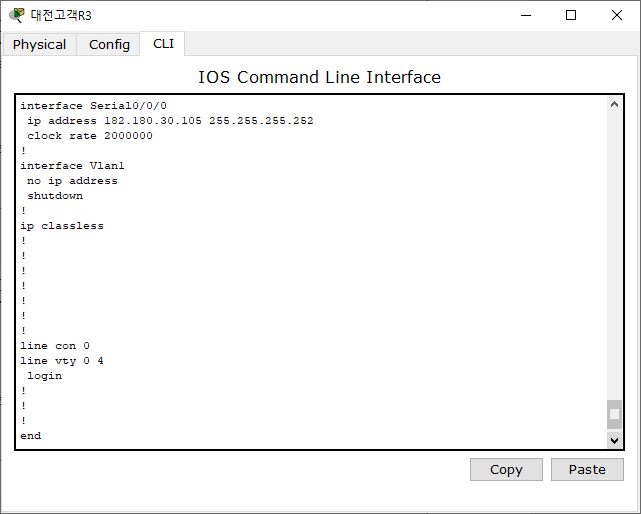
R3(config-if)#ip address 182.180.30.81 255.255.255.248



단계 06 R3 시리얼 인터페이스 IP주소를 설정하고 확인한다

R3(config)#interface Serial 0/0/0

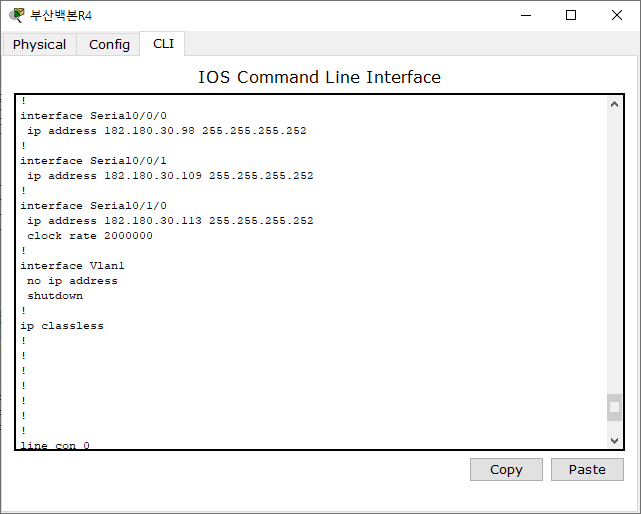
R3(config-if)#ip address 182.180.30.105 255.255.255.252



단계 07 R4 시리얼 인터페이스 IP주소를 설정하고 확인한다

R4(config)#interface Serial 0/0/0

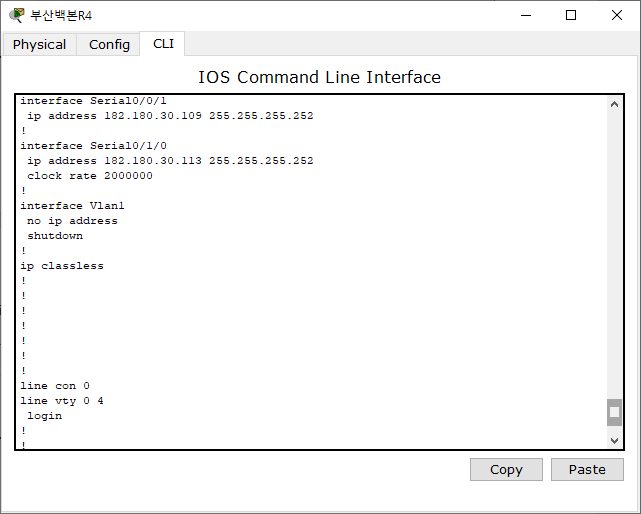
R4(config-if)#ip address 182.180.30.98 255.255.255.252



단계 08 R4 시리얼 인터페이스 IP주소를 설정하고 확인한다

R4(config)#interface Serial 0/0/1

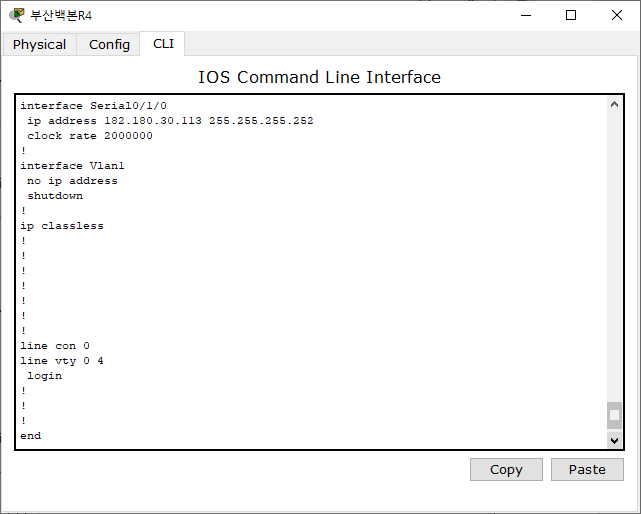
R4(config-if)#ip address 182.180.30.109 255.255.255.252



단계 09 R4 시리얼 인터페이스 IP주소를 설정하고 확인한다

R4(config)#interface Serial 0/1/0

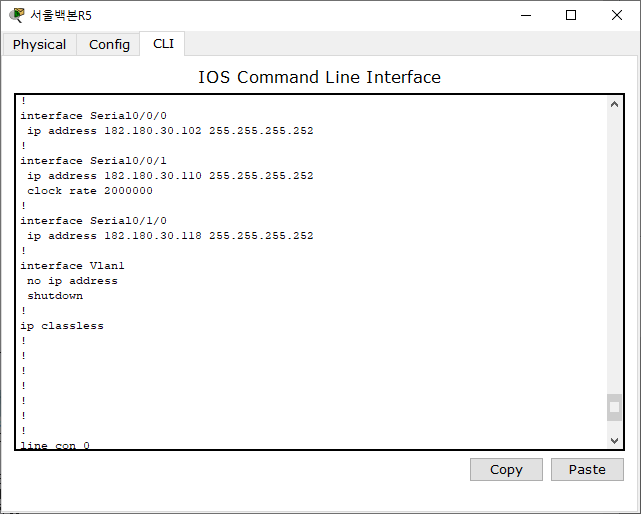
R1(config-if)#ip address 182.180.30.113 255.255.255.252



단계 10 R5 시리얼 인터페이스 IP주소를 설정하고 확인한다

R5(config)#interface Serial 0/0/0

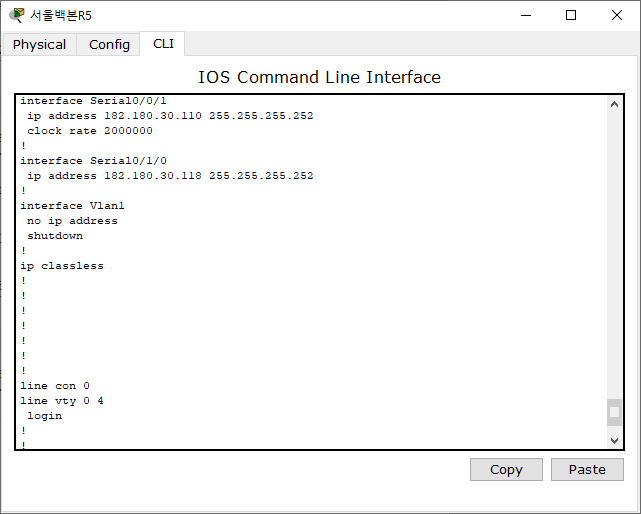
R5(config-if)#ip address 182.180.30.102 255.255.255.252



단계 11 R5 시리얼 인터페이스 IP주소를 설정하고 확인한다

R5(config)#interface Serial 0/0/1

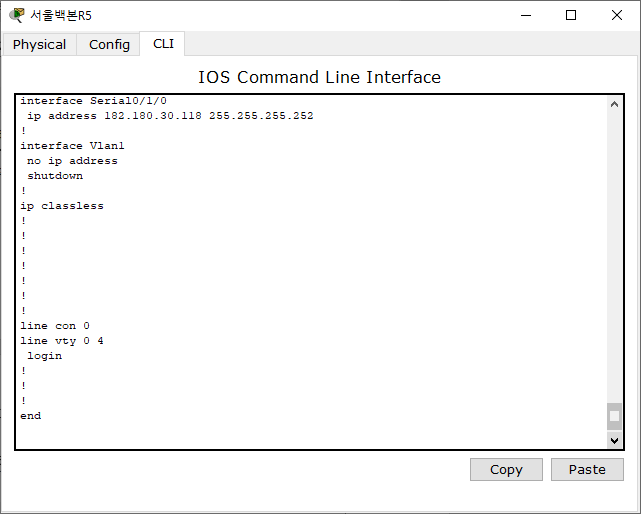
R5(config-if)#ip address 182.180.30.110 255.255.255.252



단계 12 R5 시리얼 인터페이스 IP주소를 설정하고 확인한다

R5(config)#interface Serial 0/1/0

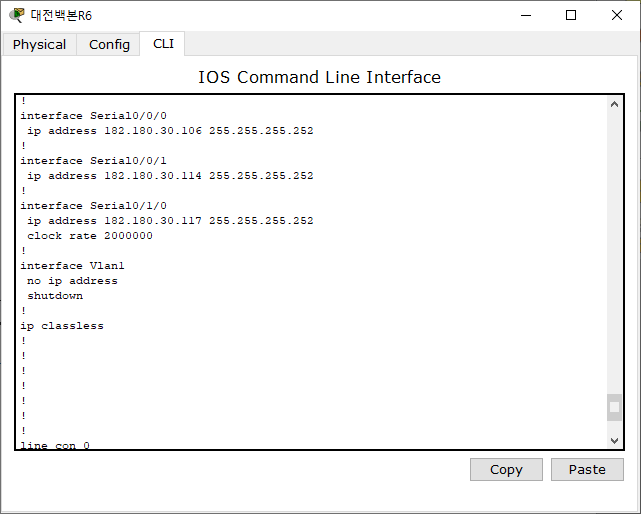
R5(config-if)#ip address 182.180.30.118 255.255.255.252



단계 13 R6 시리얼 인터페이스 IP주소를 설정하고 확인한다

R6(config)#interface Serial 0/0/0

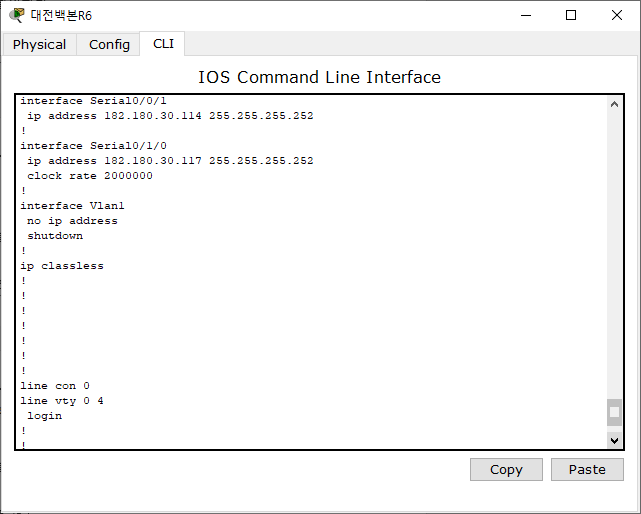
R6(config-if)#ip address 182.180.30.106 255.255.255.252



단계 14 R6 시리얼 인터페이스 IP주소를 설정하고 확인한다

R6(config)#interface Serial 0/0/1

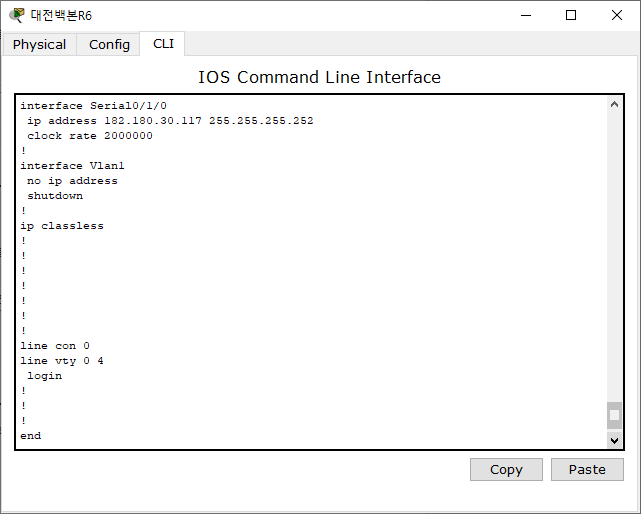
R6(config-if)#ip address 182.180.30.114 255.255.255.252



단계 15 R6 시리얼 인터페이스 IP주소를 설정하고 확인한다

R6(config)#interface Serial 0/1/0

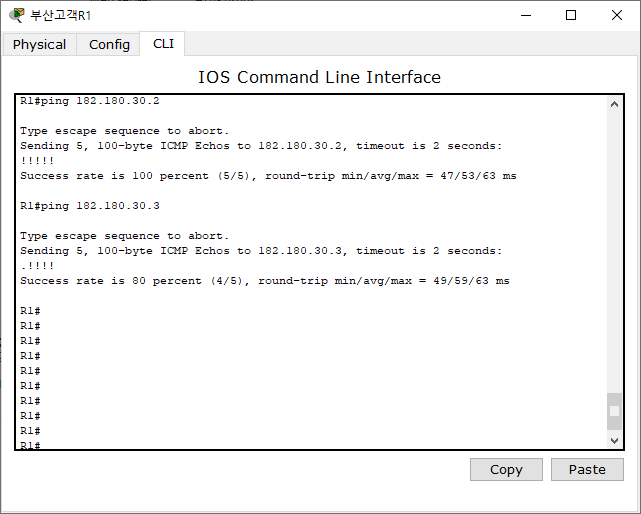
R6(config-if)#ip address 182.180.30.117 255.255.255.252



# Router에서 PC로, 이웃한 Router간 통신 확인을 한다

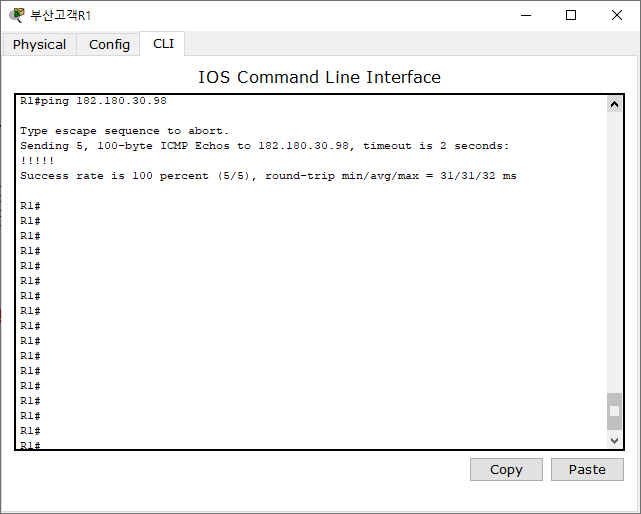
단계 01 R1 라우터에서 PC로 Ping 통신을 한다

☞확인



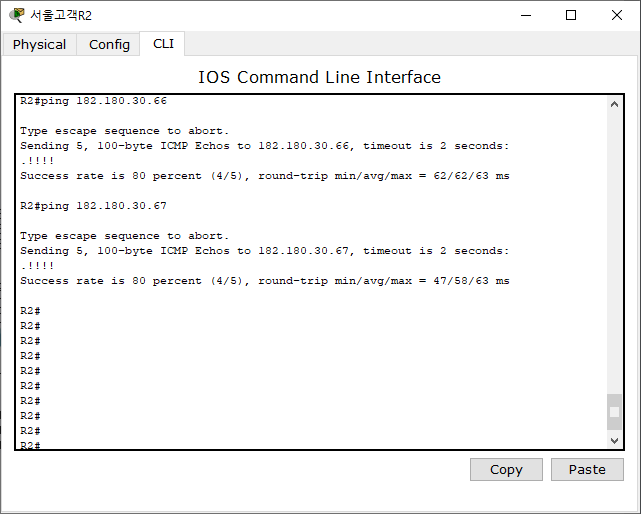
단계 02 R1 라우터에서 R4 라우터 시리얼로 Ping 통신을 한다

☞확인



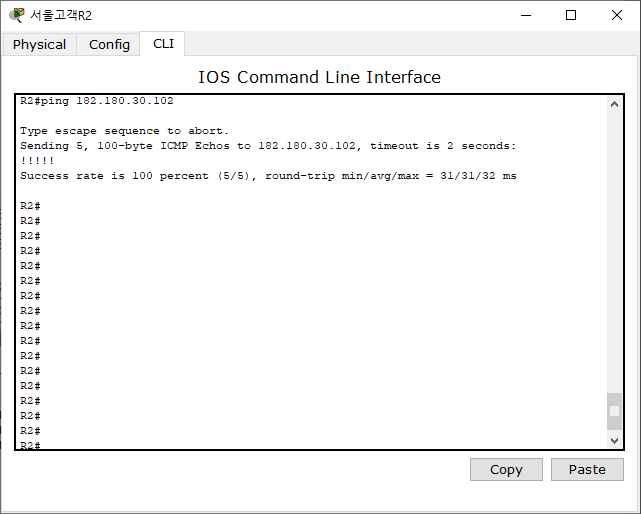
단계 03 R2 라우터에서 PC로 Ping 통신을 한다

☞확인



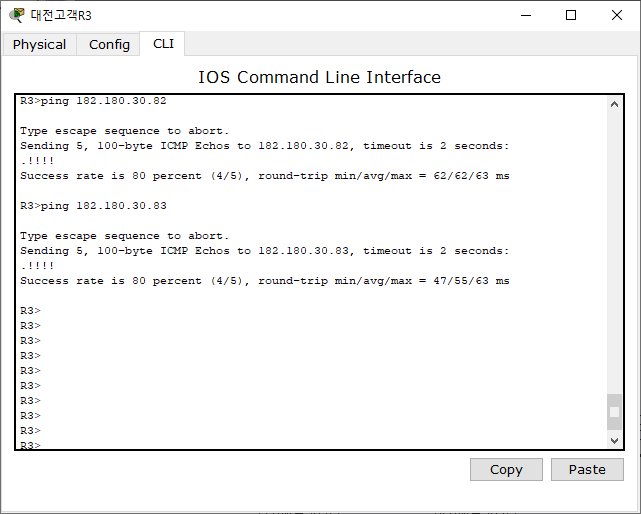
단계 04 R2 라우터에서 R5 라우터 시리얼로 Ping 통신을 한다

☞확인



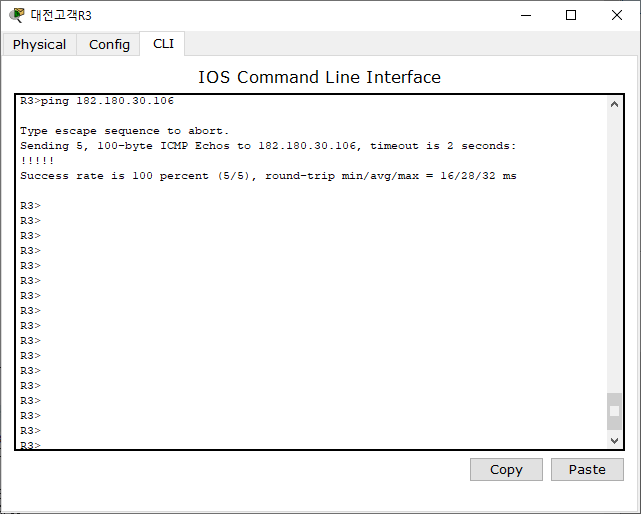
단계 05 R3 라우터에서 PC로 Ping 통신을 한다

☞확인



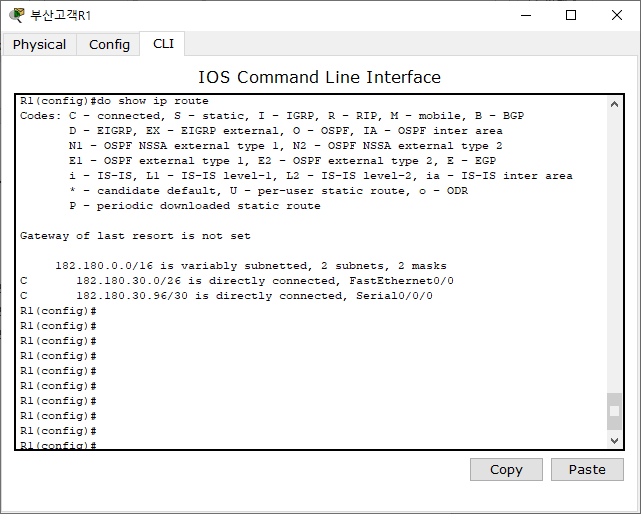
단계 06 R3 라우터에서 R6 라우터 시리얼로 Ping 통신을 한다

☞확인

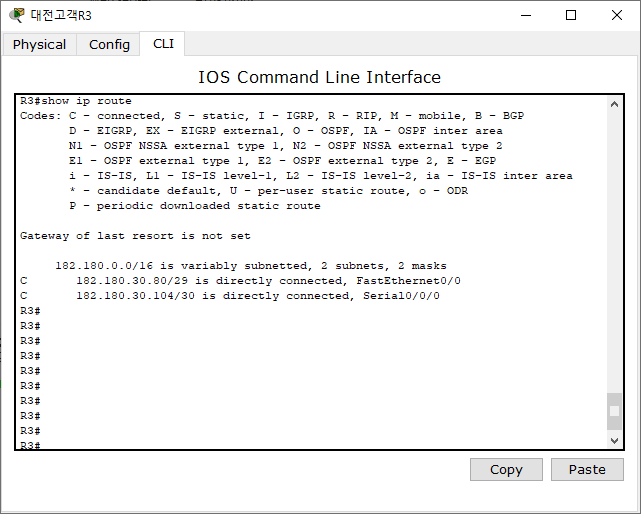


# 라우터에서 현재의 Routing Table 상태를 조회 해 보자

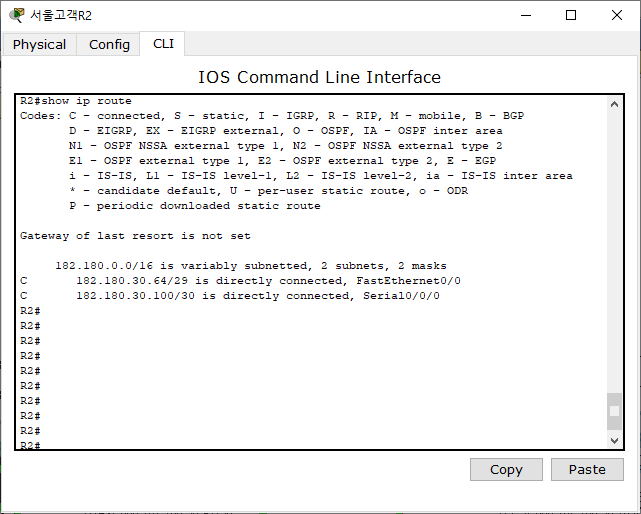
단계 01 부산 라우터에서 Routing Table 상태를 조회 한다



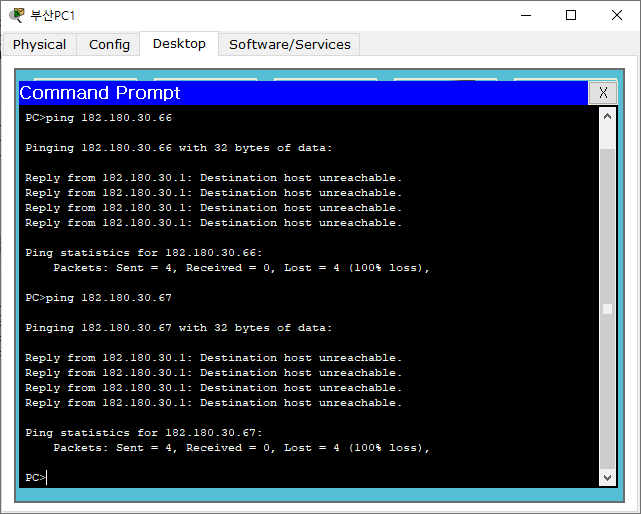
단계 02 대전 라우터에서 Routing Table 상태를 조회 한다



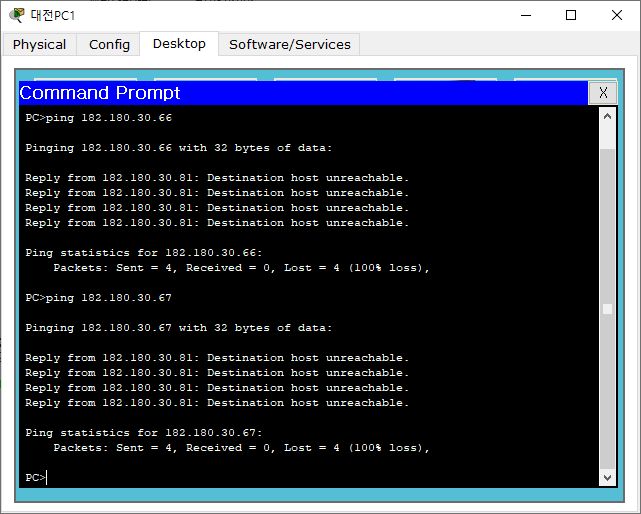
단계 03 서울 라우터에서 Routing Table 상태를 조회 한다



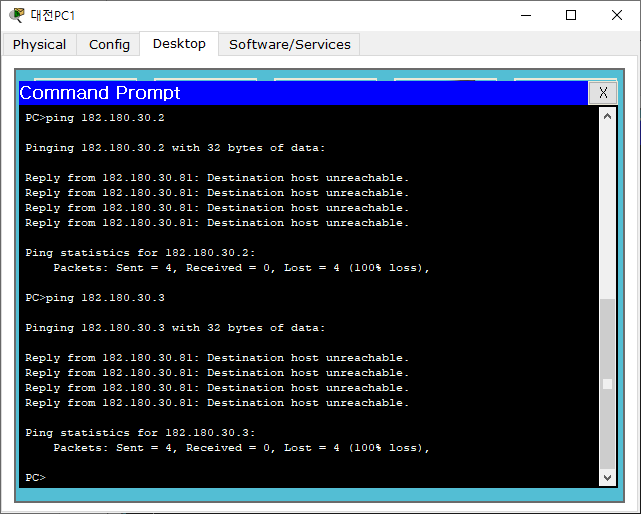
단계 04 부산지사 PC 에서 서울본사 PC 로 Ping 통신 확인



단계 05 대전지사 PC 에서 서울본사 PC 로 Ping 통신 확인



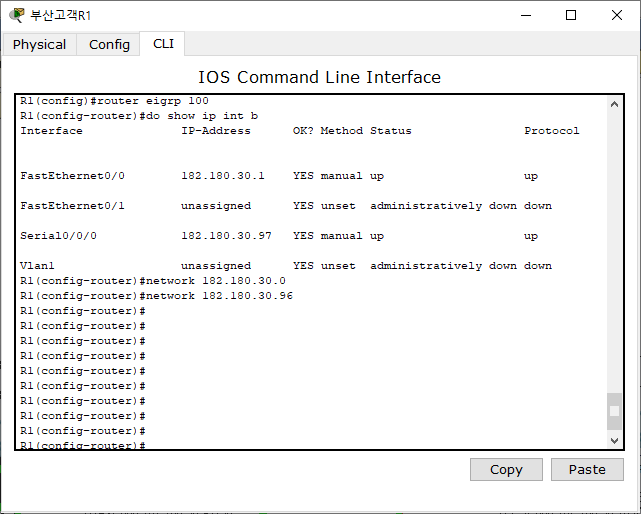
단계 06 대전지사 PC 에서 부산지사 PC 로 Ping 통신 확인



# 라우팅 프로토콜 설정

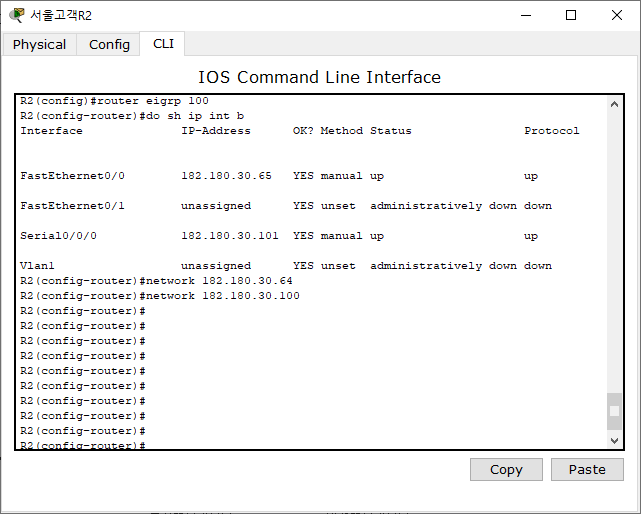
단계 01 R1에 라우팅 프로토콜을 설정한다

☞설정



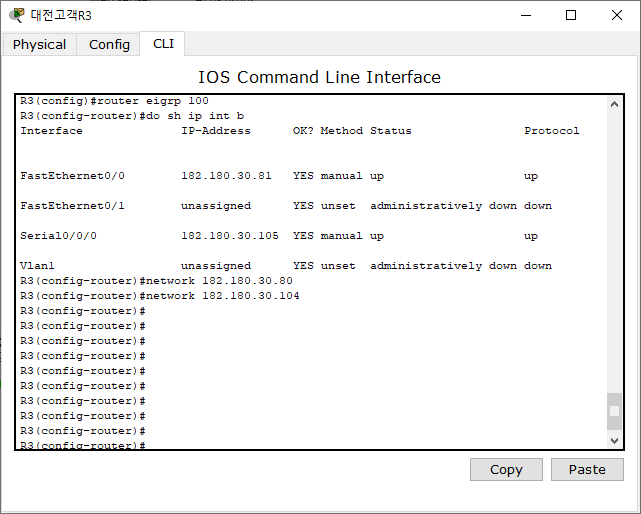
단계 02 R2에 라우팅 프로토콜을 설정한다

☞설정



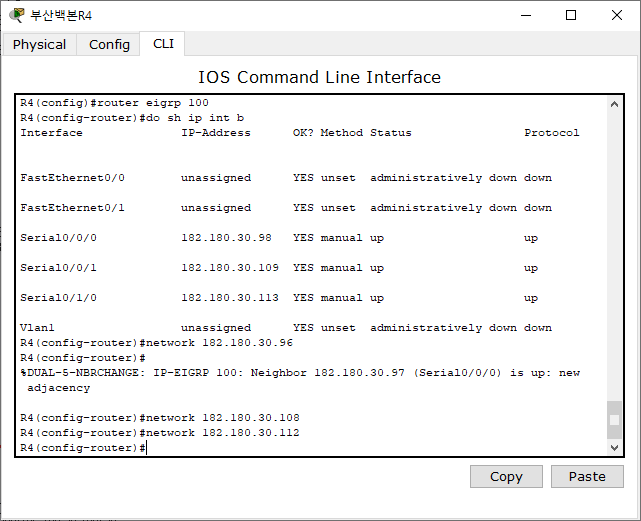
단계 03 R3에 라우팅 프로토콜을 설정한다

☞설정



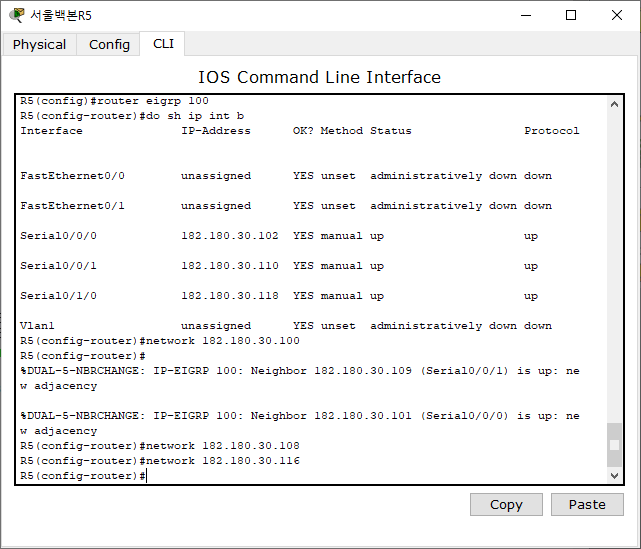
단계 04 R4에 라우팅 프로토콜을 설정한다

☞설정



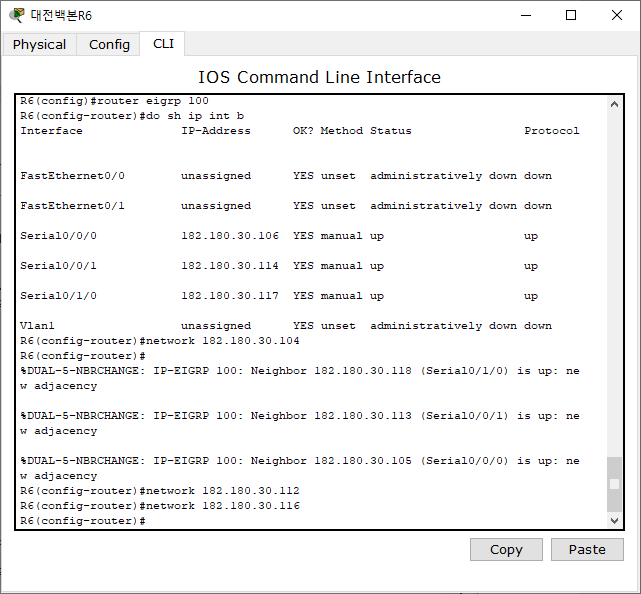
단계 05 R5에 라우팅 프로토콜을 설정한다

☞설정



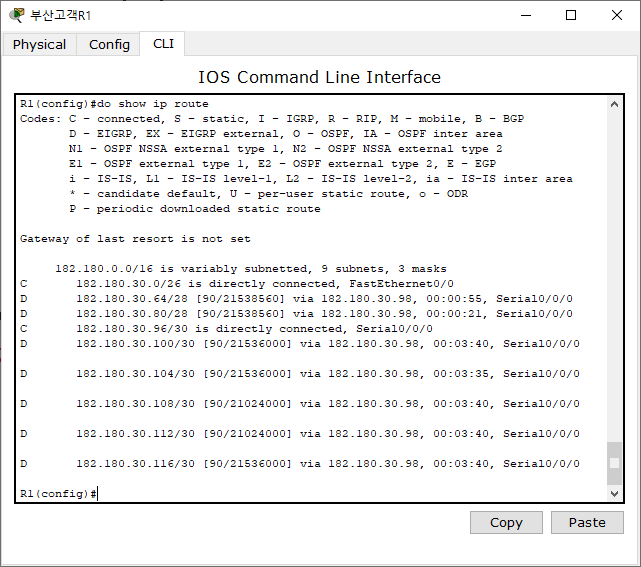
단계 06 R6에 라우팅 프로토콜을 설정한다

☞설정



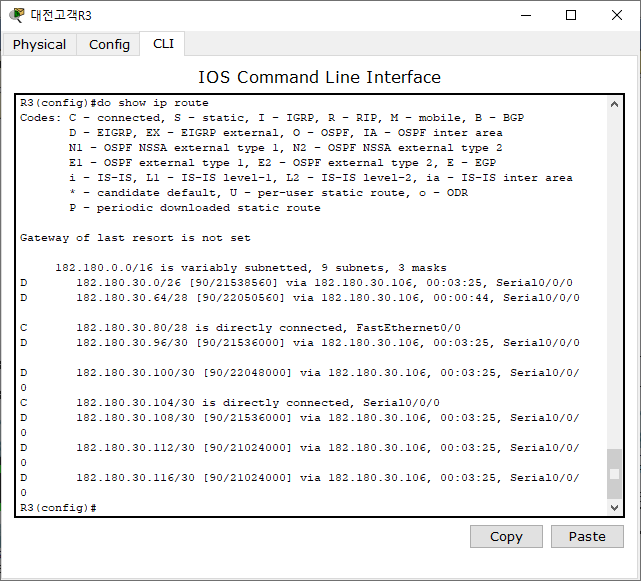
단계 07 부산지사 라우터에서 라우팅 테이블 조회

☞확인



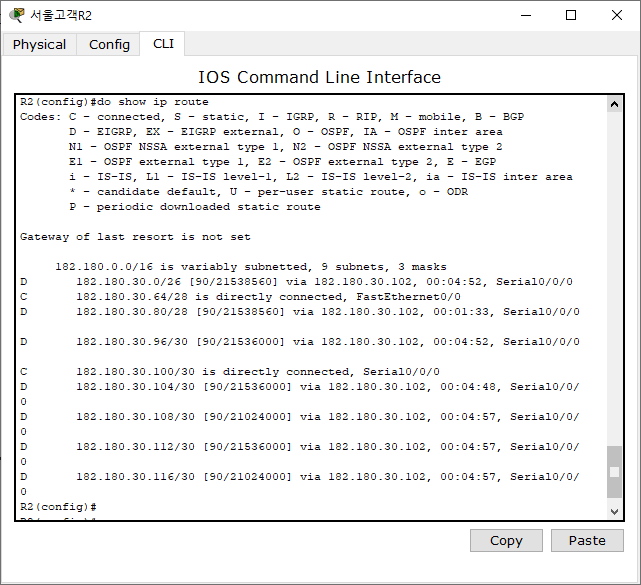
단계 08 대전지사 라우터에서 라우팅 테이블 조회

☞확인



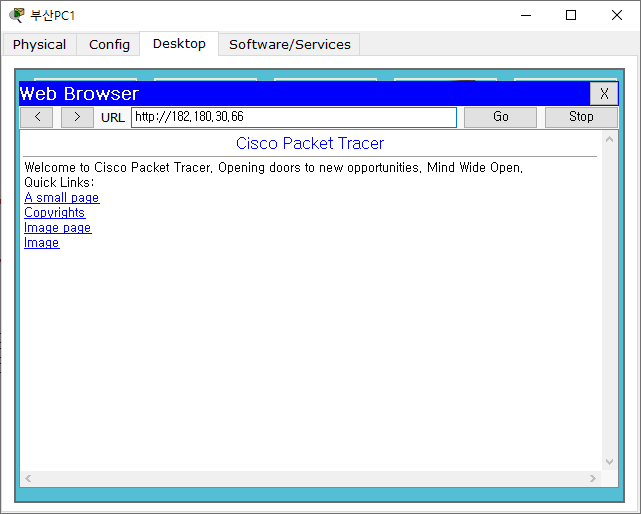
단계 09 서울본사 라우터에서 라우팅 테이블 조회

☞확인

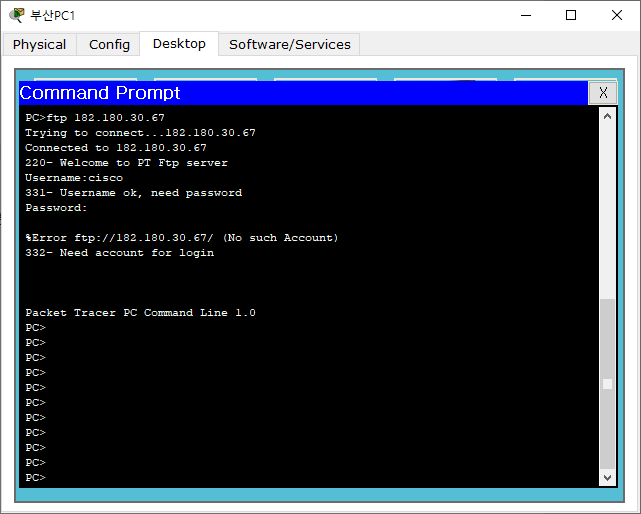


# 본사와 지사간 접속을 확인한다

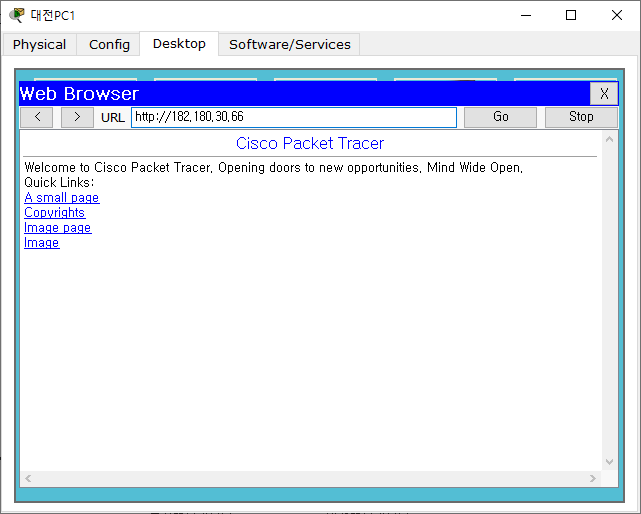
단계 1 부산지사 PC에서 서울 본사 WEB 서버로 접속한다



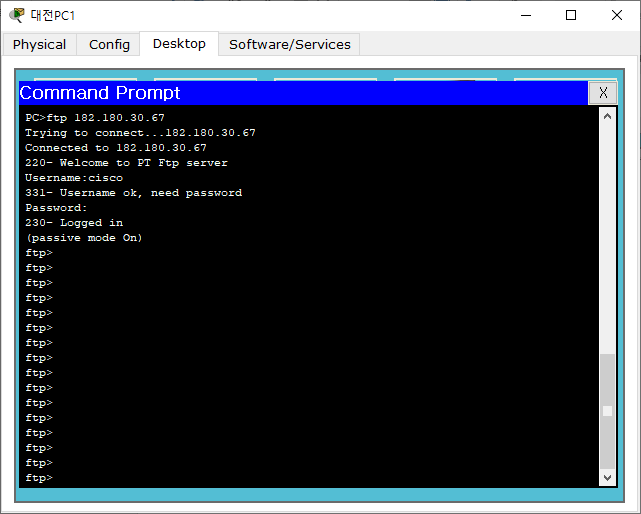
단계 2 부산지사 PC에서 서울 본사 FTP 서버로 접속한다



단계 3 대전지사 PC에서 서울 본사 WEB 서버로 접속한다



단계 4 대전지사 PC에서 서울 본사 FTP 서버로 접속을 한다



# ▣ 확장 ACL Extend Access Control List(EACL) 설정

확장 ACL을 적용하여 특정 서버에 접근을 차단하도록 해보자

☞ 부산지사의 182.180.30.2/26 PC는 서울 본사의 WEB 서버에 접근 할 수 없다

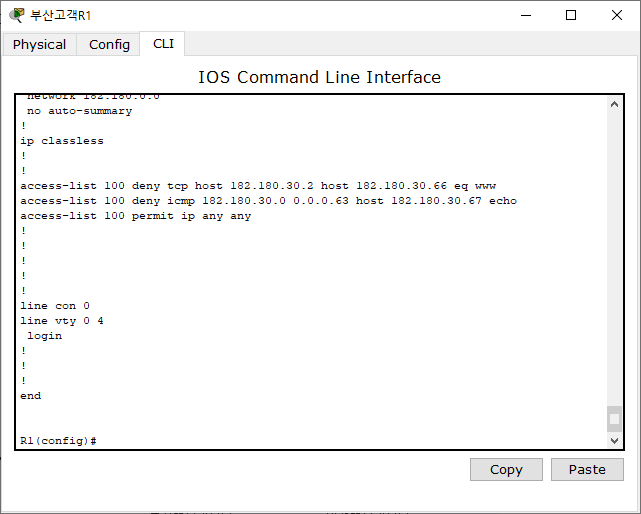
☞ 부산지사의 모든 PC는 서울 본사의 FTP 서버에 PING 통신 할 수 없다

☞ 대전지사의 182.180.30.82/28 PC는 서울 본사의 WEB 서버에 접근 할 수 없다

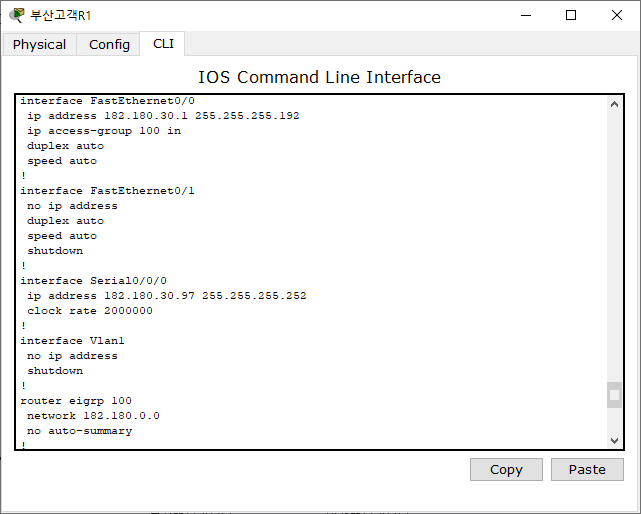
☞ 부산지사의 모든 PC는 서울 본사의 WEB 서버에 PING 통신 할 수 없다

# 확장 ACL 설정 및 접속 확인

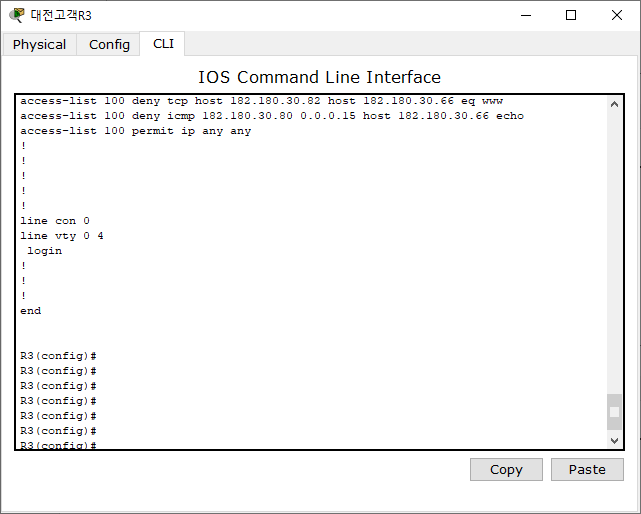
단계 1 부산고객 라우터에 확장 ACL 100번 리스트를 작성한다



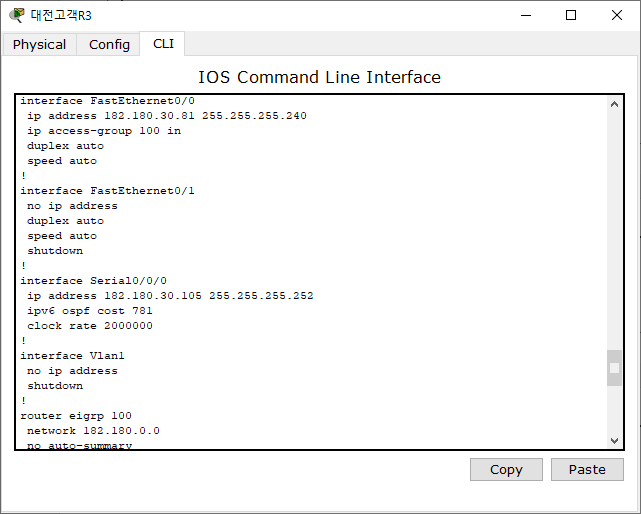
단계 2 부산고객 라우터에 확장 ACL 100번 리스트를 적용한다



단계 3 대전고객 라우터에 확장 ACL 100번 리스트를 작성한다

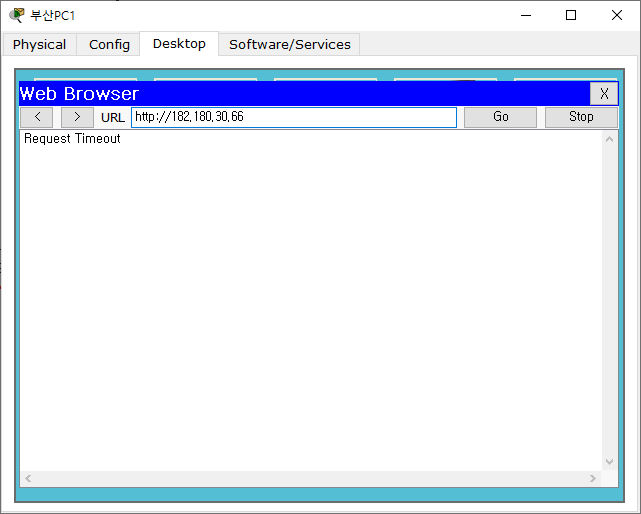


단계 4 대전고객 라우터에 확장 ACL 100번 리스트를 적용한다

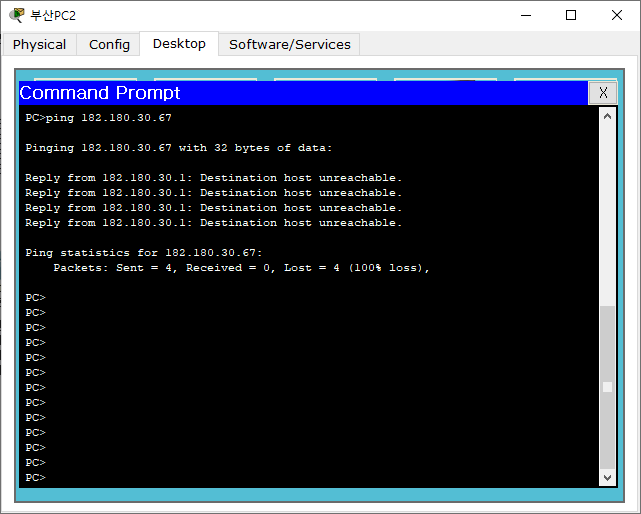


# 본사와 지사간 접속을 확인한다

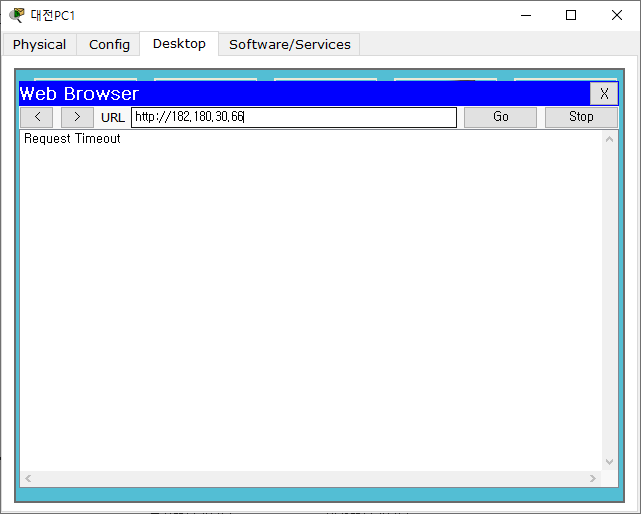
단계 1 부산지사의 182.180.30.2/24 PC 에서 서울 본사 WEB 서버로 접속을 한다



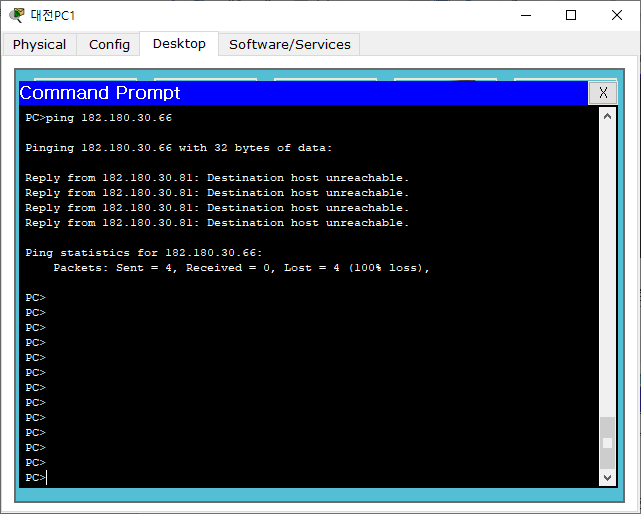
단계 2 부산지사 모든 PC에서 서울본사로 FTP 서버로 PING 통신을 한다



단계 3 대전지사의 182.180.30.82/24 PC에서 서울 본사 WEB 서버로 접속한다

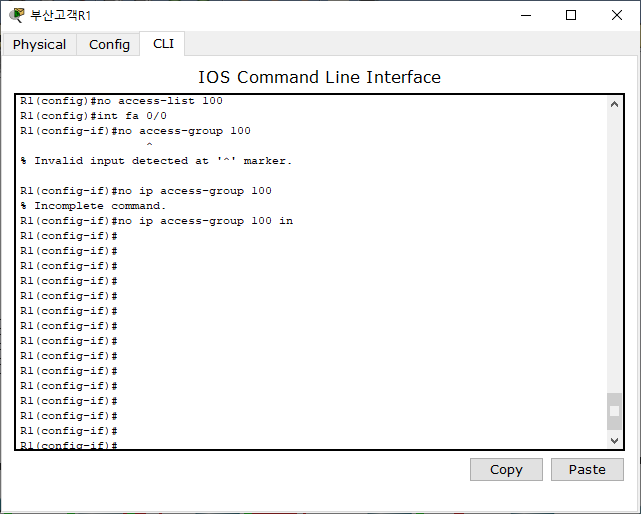


단계 4 대전지사의 모든 PC에서 서울 본사로 WEB 서버로 PING 통신을 한다

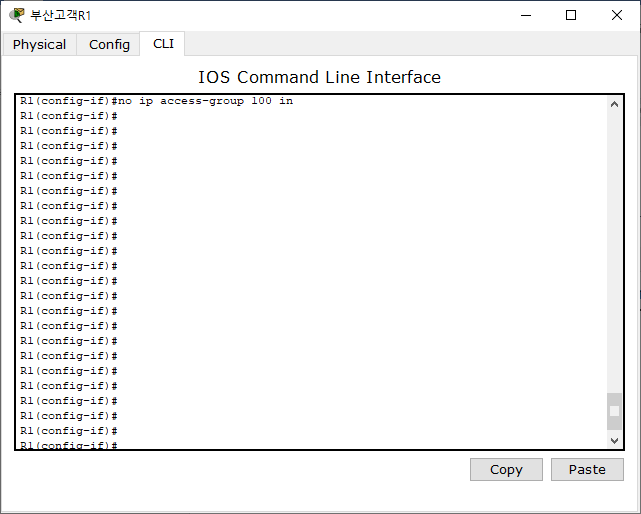


# 확장 ACL 해제 한다

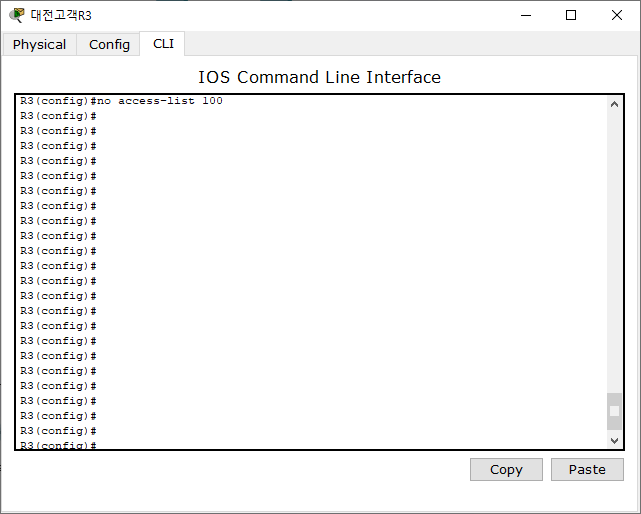
단계 1 확장 ACL 100번 리스트를 제거 한다



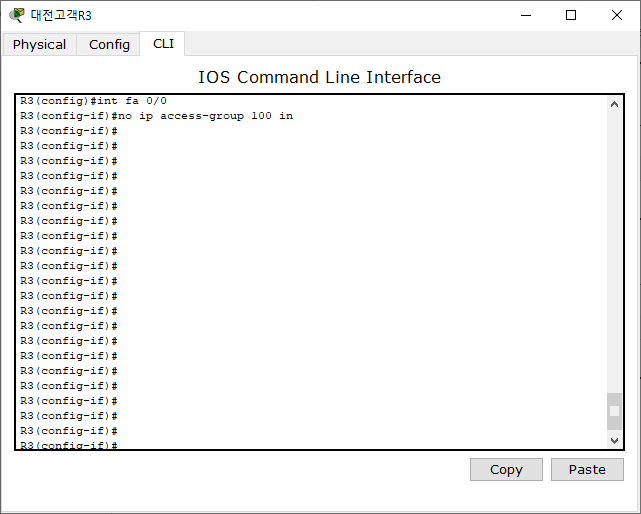
단계 2 확장 ACL 100번 리스트를 적용을 해제 한다



단계 3 확장 ACL 100번 리스트를 제거 한다

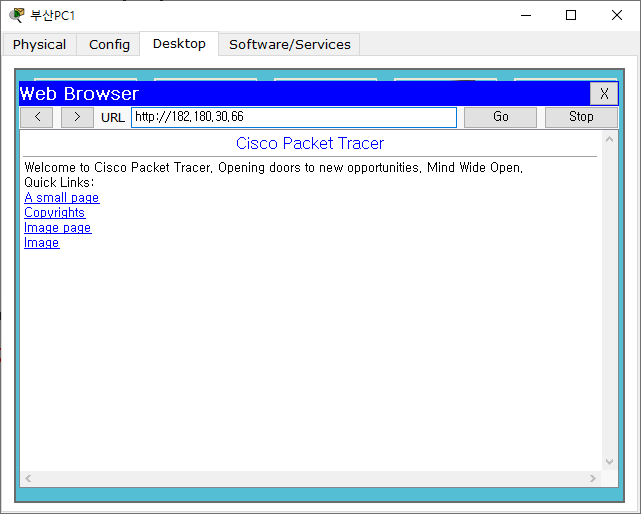


단계 4 확장 ACL 100번 리스트를 적용을 해제 한다

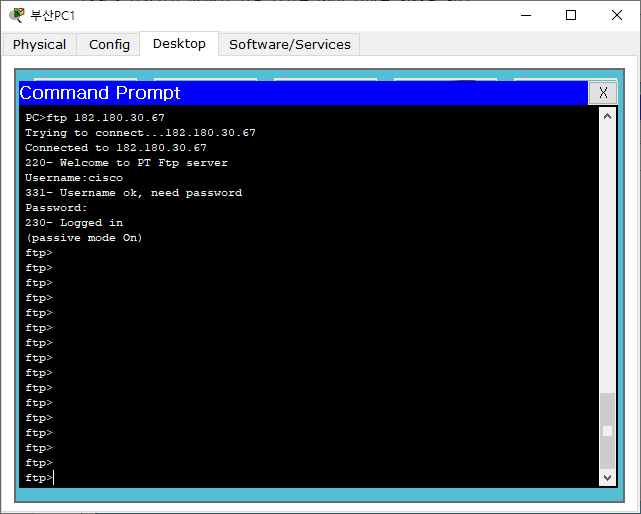


# 본사와 지사간 접속을 확인한다

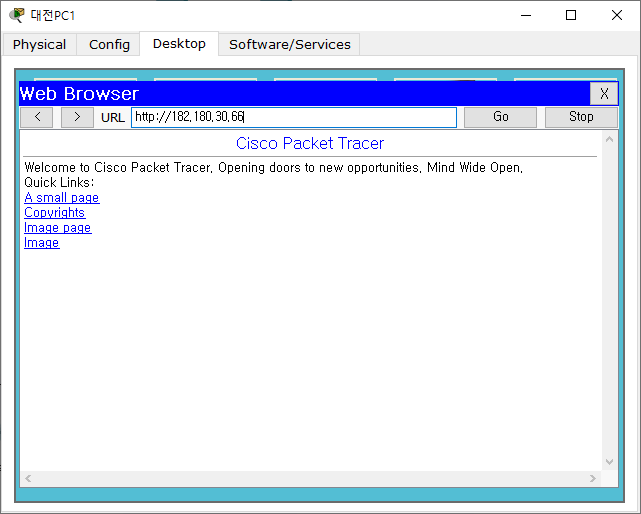
단계 1 부산지사 PC에서 서울 본사로 WEB 서버로 접속을 한다



단계 2 부산지사 PC에서 서울 본사로 FTP 서버로 PING 통신을 한다



단계 3 대전지사 PC에서 서울 본사로 WEB 서버로 접속을 한다



단계 4 대전지사 PC에서 서울 본사로 FTP 서버로 PING 통신을 한다

