### 네트워크 기초 ### // 책 추천 : 하루 3분 네트워크 교실

\* 네트워크

Network = Net(그물) + work(작업하다)

- 무언가가 무언가(종단,단말장치)와 무언가에 의해(유선,무선) 무언가(정보,데이터)를 주고받는 것

- 네트워크의 규모가 확장되거나 , 효율적인 정보 공유를 위해 규약( Protocol )이 필요

\* 데이터 전송 관계

- 요청(request)에 의한 응답(response) 관계

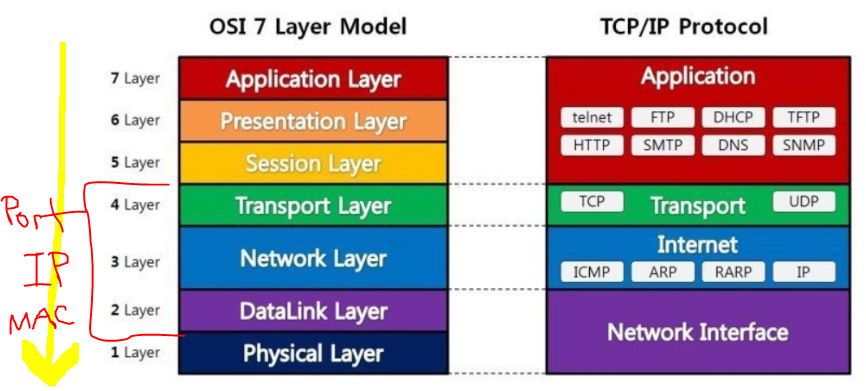
요청자 : 클라이언트 ( Client )

응답자 : 서버 ( Server )

\* 네트워크의 유형

- OSI 7계층과 TCP/IP 세분화 정도만 다름.

- LAN은 내부, WAN과 인터넷은 외부



1) LAN (Local Area Network): 로컬 에어리어 네트워크는 비교적 작은 지리적 범위 내에서 컴퓨터 및 기타 종단장치를 연결하는 네트워크입니다. 주로 집, 사무실, 학교 등 내부 네트워크에서 사용됩니다.

2) WAN (Wide Area Network): 원거리 에어리어 네트워크는 지리적으로 넓은 범위에 걸쳐 있는 네트워크를 의미합니다. 여러 LAN을 연결하거나 인터넷과 같은 글로벌 네트워크를 포함합니다.

3) Internet: 인터넷은 전 세계적으로 연결된 글로벌 네트워크로, 다양한 유형의 네트워크가 연결되어 정보 및 데이터를 공유하는 데 사용됩니다.

4) VPN (Virtual Private Network, 전용선): 가상 사설 네트워크는 공중 네트워크(인터넷)를 통해 안전하게 연결된 사설 네트워크처럼 사용하는 기술입니다. 원격 위치 또는 사용자가 안전하게 기업 네트워크에 접속할 수 있도록 합니다.

5) VLAN (Virtual LAN): 가상 LAN은 물리적으로 분리된 네트워크를 논리적으로 그룹화하여 관리하고 효율적으로 운영하기 위한 기술입니다. -> 보안, 자원 효율

6) WLAN (Wireless LAN): 무선 로컬 에어리어 네트워크는 무선 통신 기술을 사용하여 컴퓨터 및 장치를 연결하는 네트워크를 의미합니다. 주로 Wi-Fi를 통해 사용됩니다.

\* OSI 7 Layer

1) 물리 계층 (Physical Layer):

OSI 모델의 가장 하위 계층으로, 물리적 매체를 통해 데이터를 전송하는 역할을 합니다.

데이터 비트를 전기 신호, 광 신호 또는 무선 신호로 변환합니다.

예시 장비 및 기술: 케이블, 허브, 리피터

2) 데이터 링크 계층 (Data Link Layer):

데이터 링크 계층은 물리 계층에서 송수신되는 데이터 프레임을 관리하고, 오류 검출 및 수정을 수행합니다.

이 계층은 주소 지정 및 프레임의 흐름 제어를 관리하며, 네트워크 환경에서 데이터 프레임이 정확하게 전달되도록 합니다.

예시 장비 및 프로토콜: 스위치, 브리지, 이더넷, MAC 주소

3) 네트워크 계층 (Network Layer):

네트워크 계층은 패킷 라우팅과 경로 선택을 담당합니다. 이 계층은 송신자에서 수신자까지 데이터 패킷을 안정적으로 전달합니다.

라우터를 통해 패킷이 다른 네트워크로 라우팅되며, IP 주소를 사용하여 목적지를 식별합니다.

예시 프로토콜: IP, ICMP

4)전송 계층 (Transport Layer):

전송 계층은 데이터의 전송을 관리하며, 에러 검출 및 복구, 데이터의 순서화, 포트 번호를 통한 프로세스 식별을 수행합니다.

TCP (Transmission Control Protocol)와 UDP (User Datagram Protocol)는 이 계층에서 사용되며, 데이터 신뢰성 및 흐름 제어를 담당합니다.

5) 세션 계층 (Session Layer):

세션 계층은 통신 세션을 설정, 관리하고 종료합니다. 이 계층은 데이터의 동기화와 다중 통신 관리를 수행합니다. -> 연결 지속

예시 기술: API (Application Programming Interface), RPC (Remote Procedure Call)

6) 표현 계층 (Presentation Layer):

표현 계층은 데이터의 형식 변환, 데이터 압축, 데이터 암호화와 같은 데이터 표현과 관련된 작업을 담당합니다.

데이터를 응용 프로그램에서 이해할 수 있는 형식으로 변환하고, 데이터 보안을 유지합니다.

예시 기술: JPEG (이미지 압축), SSL/TLS (보안 프로토콜)

7) 응용 계층 (Application Layer):

OSI 모델의 최상위 계층으로, 사용자 및 응용 프로그램과 직접 상호 작용하는 계층입니다.

응용 프로그램은 이 계층을 통해 네트워크 서비스 및 기능을 사용할 수 있습니다.

예시 프로토콜: HTTP (웹 통신), FTP (파일 전송), SMTP (이메일)

\* TCP/IP

- 모델은 OSI 모델과 비슷한 네트워크 프로토콜 스택입니다.

- 이 모델은 4 ~ 5개의 계층으로 구성되어 있습니다

- TCP/IP 모델은 실제 인터넷 통신에서 널리 사용되며, OSI 모델보다 더 단순하고 실제 네트워크에서의 구현에 더 가깝습니다.

1) 네트워크 접속 계층 (Network Access Layer): OSI의 물리 계층과 데이터 링크 계층에 대응합니다. 이 계층은 하드웨어 인터페이스와 관련된 기능을 수행합니다.

2) 인터넷 계층 (Internet Layer): OSI의 네트워크 계층과 부분적으로 일치합니다. 이 계층은 IP 프로토콜을 사용하여 데이터 패킷의 라우팅과 전달을 담당합니다.

3) 전송 계층 (Transport Layer): OSI의 전송 계층과 동일한 역할을 수행하며, TCP와 UDP 프로토콜을 사용하여 데이터 전송을 관리합니다.

4) 응용 계층 (Application Layer): OSI의 응용 계층과 같은 역할을 합니다. 응용 프로그램과 네트워크 서비스 간의 상호 작용을 지원하며, HTTP, FTP, SMTP 등의 프로토콜을 사용합니다.

\* 데이터 전송 주소 체계

1) MAC 주소

- 로컬환경 내에서 데이터 전송 담당

- 변경이 불가능한 물리적인 주소

2) IP 주소

- 로컬(local)에서 리모트(remote)환경으로 데이터 전송 담당

- 변경이 가능한 논리적인 주소

- 공인 IP 주소 (Public IP)

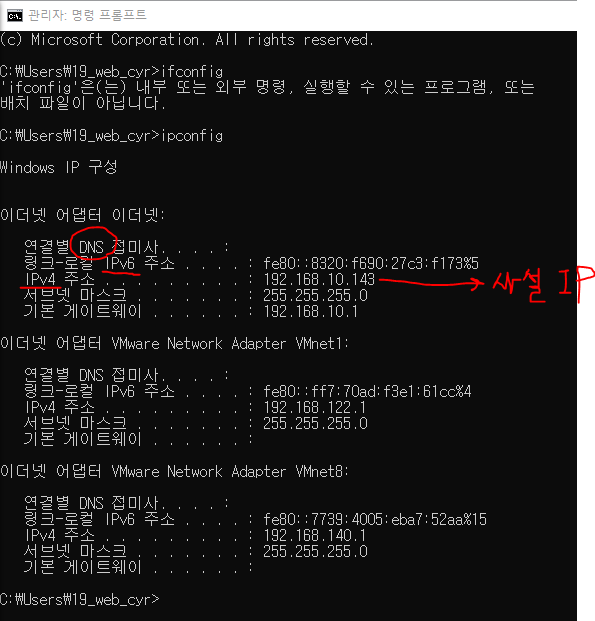
> 웹 브라우저에서 '내 아이피 주소’ 검색으로 확인

ISP업체에서 할당한 인터넷이 가능한 주소, 공인 IP 네트워크 정보는 ISP업체 라우터 장비에 등록

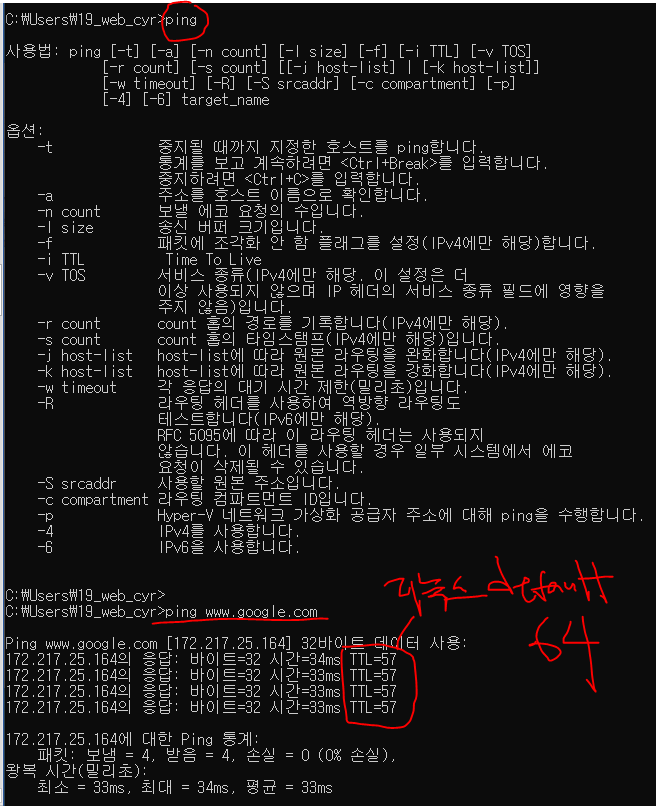
@ISP (Internet Service Provider) : 인터넷 서비스 제공자 Ex) kt,lg,sk,등

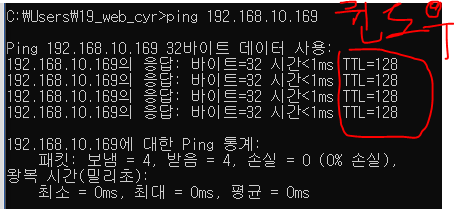
- 사설 IP 주소 (Private IP)

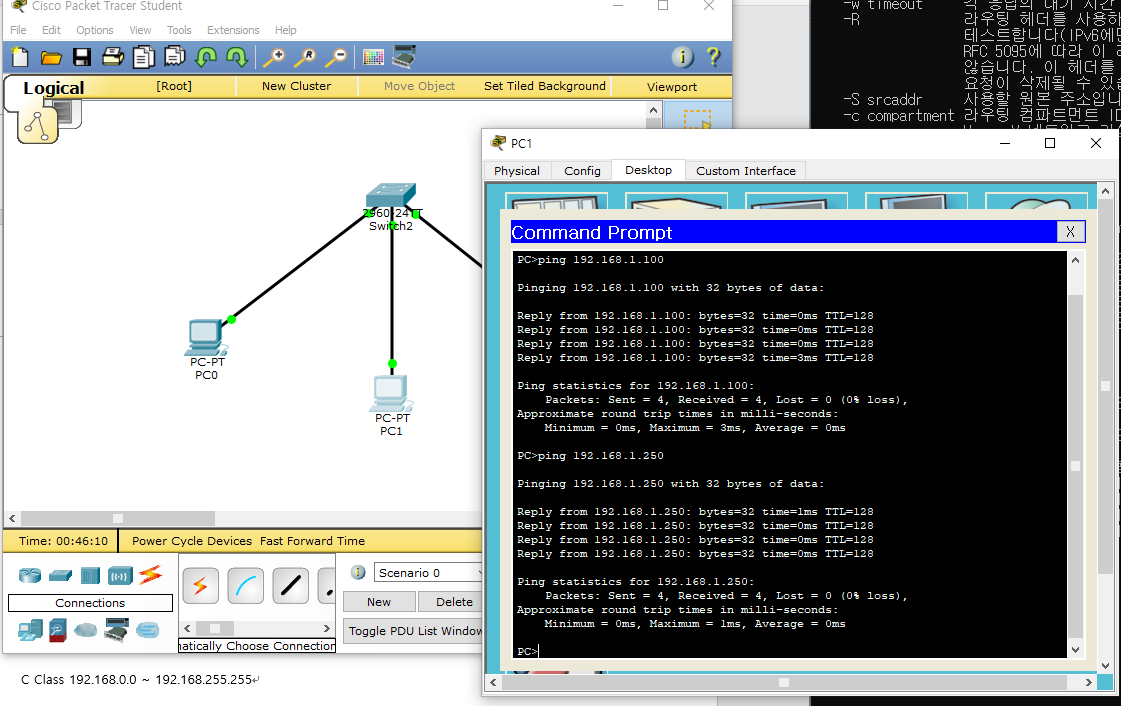
> Window command : 'ipconfig'로 확인

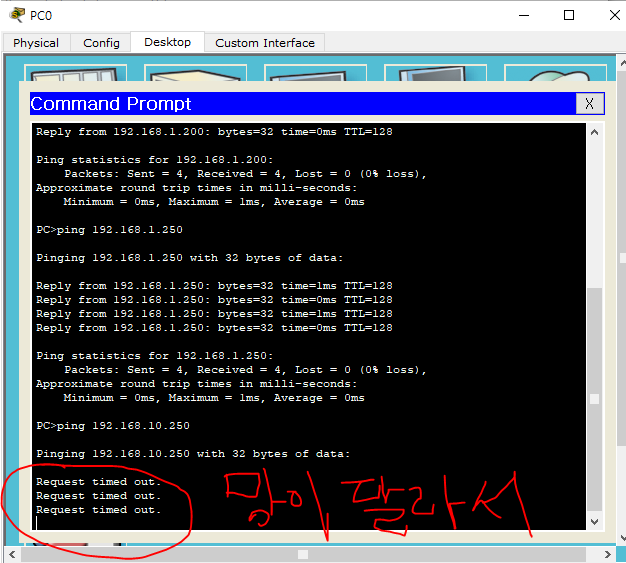


ISP업체 임대와 상관없이 내부용으로 사용하는 주소 , 사설 IP 네트워크 정보는 ISP업체 라우터 장비에 등록 x









[ 사설 IP 주소 대역 ] (외부와는 연결 X) 여기 해당하지 않으면 public id

A Class 10.0.0.0 ~ 10.255.255.255

B Class 172.16.0.0 ~ 172.31.255.255

C Class 192.168.0.0 ~ 192.168.255.255

- 서브넷 마스크 (Subnet Mask)

- 공통비트 '1'표기 -> 네트워크 아이디 ( 네트워크 식별자 )

- 공통비트 '0'표기 -> 호스트 아이디 ( 호스트 식별자 )

NID와 PID

IP Subnet Mask Network ID Host ID

---------------------------------------------------------------------------

192.168.6.254 255.255.255.0 192.168.6 .254

192.168.6.254 255.255.0.0 192.168 .6.254

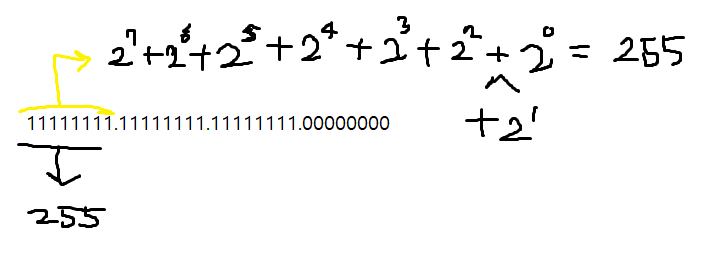
192.168.6.254 255.0.0.0 192. .168.6.254

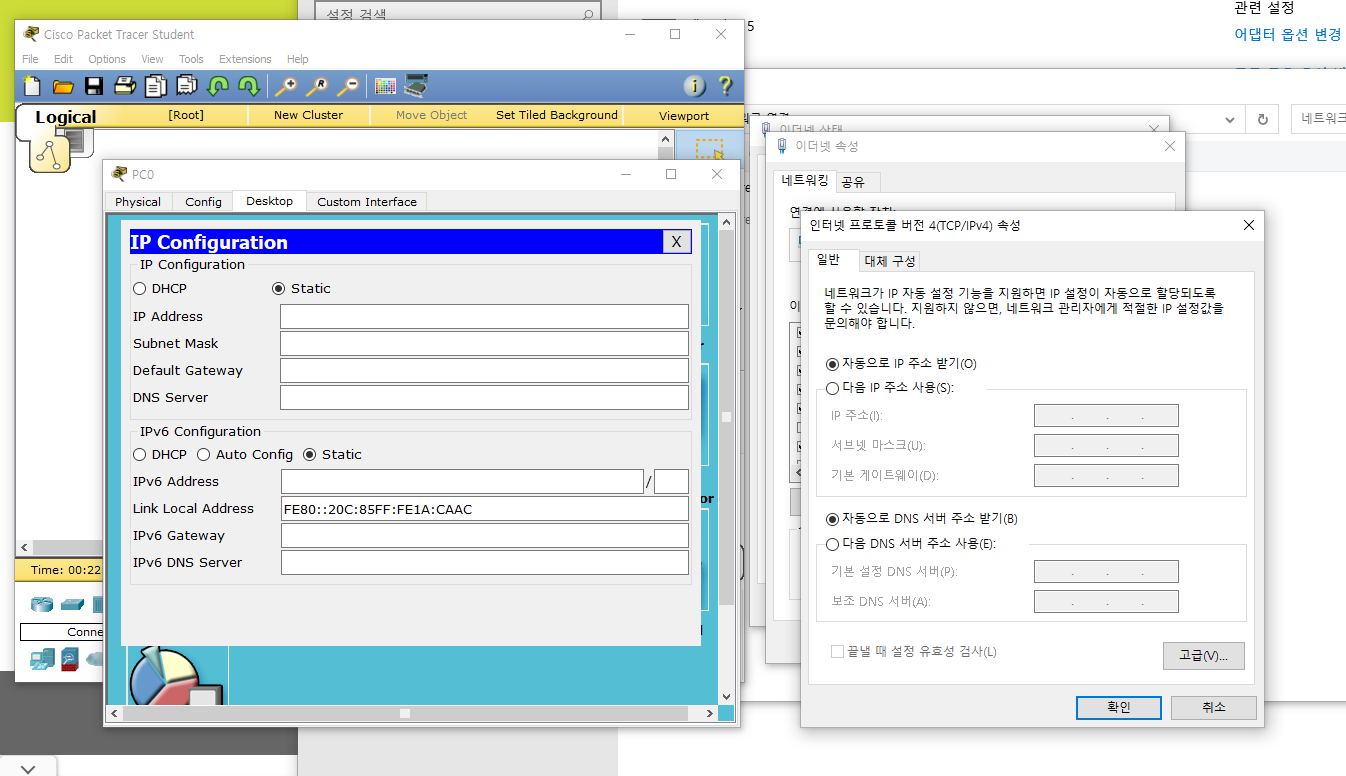
- IP 주소 클래스 ( 0.0.0.0 ~ 255.255.255.255 )

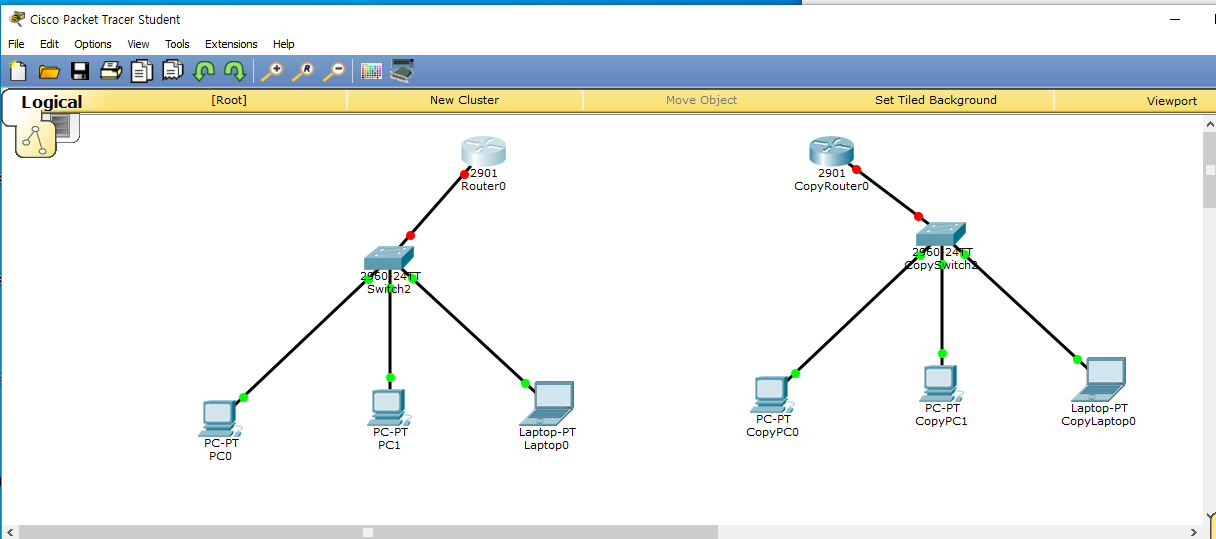
경우의 수 256개 X 256개 X 256개 X 256개 = 4,294,967,296 개의 주소

개수 부족 -> 공유기를 쓰는 이유이자, 공인 IP와 사설 IP가 있는 이유, IPv6가 있는 이유

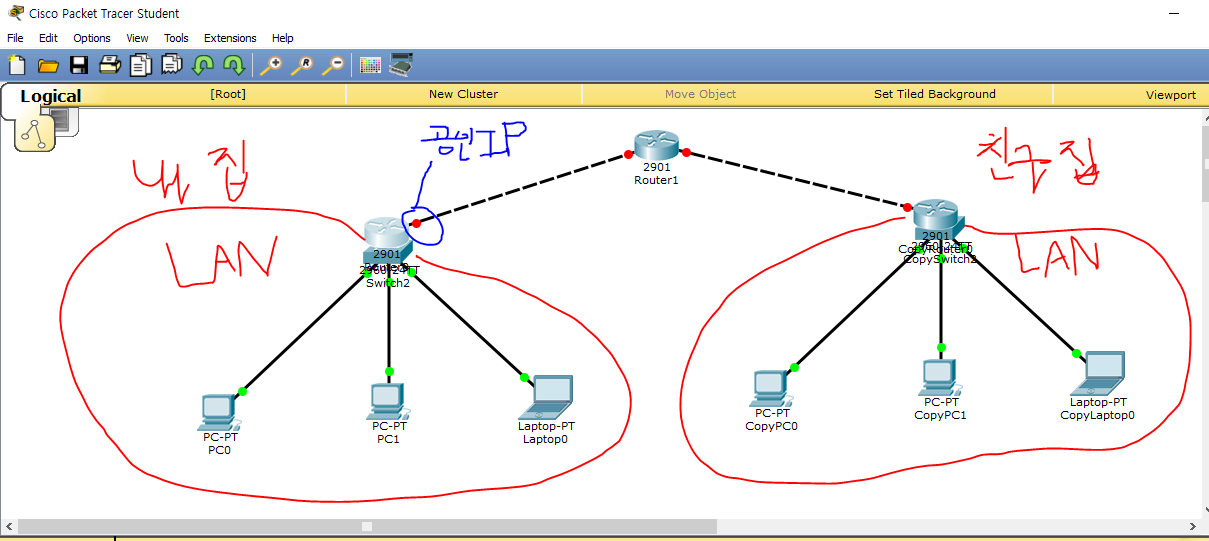
IPv6는 16진수를 사용함(0~9, a~f)











\* 유니케스트 주소

- 장치에 설정하는 주소

A Class ( 0 ~ 127 )

- 기본 서브넷마스크 : 255.0.0.0

- 네트워크당 IP주소 개수 : 2^24개

B Class ( 128 ~ 191 )

- 기본 서브넷마스크 : 255.255.0.0

- 네트워크당 IP주소 개수 : 2^16개

C Class ( 192 ~ 223 )

- 기본 서브넷마스크 : 255.255.255.0

- 네트워크당 IP주소 개수 : 2^8개

\* 멀티케스트 주소

- 장치에 사용할 수 없음

- 멀티캐스트 트래픽을 위한 목적으로 사용됩니다.

D Class ( 224 ~ 239 )

\* 실험 및 예비 목적으로 예약

- 장치에 사용할 수 없음

- 일반적인 네트워크 운영에는 사용되지 않음

E Class ( 240 ~ 255 )

+@유니케스트 -> 1 : 1 통신

@멀티케스트 -> 1 : 특정 그룹 통신

@브로드케스트 -> 1 : 전체 통신

- 현재는 CIDR (Classless Inter-Domain Routing)와 함께 더 유연한 주소 할당 방식을 사용

3) Port 번호

- 네트워크 통신에서 프로세스나 서비스를 식별하기 위한 번호

- TCP/IP 네트워크에서는 Port 번호를 사용하여 데이터가 어떤 프로그램으로 전송되어야 하는지 결정

- TCP (Transmission Control Protocol)

연결 지향 프로토콜: TCP는 연결을 설정하고 유지한 후 데이터를 안정적으로 전송하기 위한 연결 지향 프로토콜

데이터 전송 전에 3-way 핸드셰이크를 통해 연결을 설정

신뢰성: TCP는 데이터의 신뢰성을 보장하기 위해 재전송 및 에러 검출 및 복구 메커니즘을 제공

데이터가 손실되거나 손상되었을 때 다시 전송하고, 데이터가 순서대로 도착하도록 보장

흐름 제어와 혼잡 제어: TCP는 네트워크의 트래픽 흐름을 관리하고 혼잡 상태를 감지하며 조절하는 기능을 한다.

네트워크에서의 과도한 혼잡을 방지하고 안정적인 데이터 전송을 가능하게 한다.

- UDP (User Datagram Protocol)

비연결성 프로토콜: UDP는 연결을 설정하지 않고 데이터를 전송하는 비연결성 프로토콜

연결 설정과 관리에 드는 오버헤드가 없어 TCP보다 빠른 데이터 전송이 가능

신뢰성 부족: UDP는 데이터의 전달 신뢰성을 보장하지 않으며, 데이터가 손실될 수 있고

데이터가 순서대로 도착하지 않을 수 있습니다.

흐름 제어와 혼잡 제어 부재: UDP는 흐름 제어와 혼잡 제어를 제공하지 않으므로 데이터가 네트워크 혼잡에 의해 손실될 수 있음

- 포트 범위는 0에서 65535까지 사용한다. (전 세계 표준)

System Port ( Well Known Port ) > (0 - 1023)

User Port ( Registered Port ) > (1024 - 49151)

Dynamic/Private Port > (49152 - 65535)

netstat –ant (커맨드에서 옵션 부분 의미 : all numeric tcp)



[System Port 예시]

HTTP(TCP 80): www에서 hypertext정보를 주고받을 수 있는 프로토콜

HTTPS(TCP 443): http에서 보안이 강화된 프로토콜

telnet(TCP 23): 원격터미널 제어를 하기 위한 프로토콜

**SSH(TCP 22): telnet에서 암호화된 보안이 강화된 프로토콜 (원격 제어)**

FTP(TCP 21): 파일전송을 위한 프로토콜 (인증 및 로그인) -> 제어

FTP-data(TCP 20): 파일전송을 위한 프로토콜 (데이터 전송) -> 파일 전송

SMTP(TCP 25): 이메일을 송신하기 위한 프로토콜

POP3(TCP 110): 이메일을 수신하기 위한 프로토콜

**DNS(UDP 53): IP주소를 도메인이름으로 변환하는 프로토콜 (구매 가능)**

**Domain Name Service**

DHCP(UDP 67): IP주소를 중앙에서 관리 및 할당하는 프로토콜 (서버)

Dynamic Host Configuration Protocol

DHCP(UDP 68): IP주소를 중앙에서 할당받는 프로토콜 (클라이언트)

NTP(UDP 123): 시간동기화를 위한 프로토콜

syslog(UDP 514): 컴퓨팅에서 syslog는 메시지 로깅의 표준

\* 네트워크 주소 변환(Network Address Translation, NAT)

NAT는 IPv4의 주소 부족 문제를 해결하기 위한 방법으로서 고려되었으며,

주로 비공인(사설, local) 네트워크 주소를 사용하는 망에서 외부의 공인망

(public, 예를 들면 인터넷)과의 통신을 위해서 네트워크 주소를 변환하는 것이다.

즉 내부 망에서는 사설 IP 주소를 사용하여 통신을 하고, 외부망과의 통신시에는

NAT를 거쳐 공인 IP 주소로 자동 변환한다.

장점:

1. 공인 IP 주소 1개에, 여러 개의 비공인 주소를 매핑할 수 있어 비용절감 효과가 있다.

2. 사설 IP 주소를 사용함으로써 외부에서 볼 때 내부의 망 구조를 알 수 없어 보안 효과가 있다.

단점:

외부망과의 통신시 주소 변환을 거쳐야 하므로 느려지며, 사용자가 많을수록 속도 저하가 커진다.

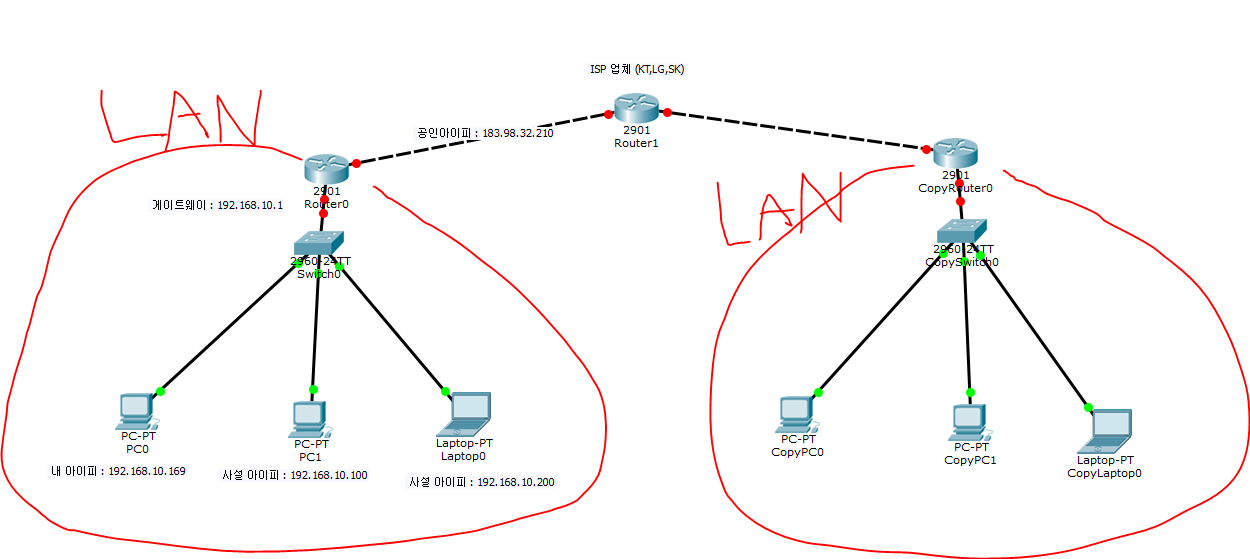
이러한 NAT 기능은 보통 라우터나 방화벽 등에 설치하며, 라우팅 정책에 따라 사설 IP 주소와 변환될 IP 주소를 static하게 혹은 dynamic하게 매핑할 수 있으며 테이블로 관리된다.

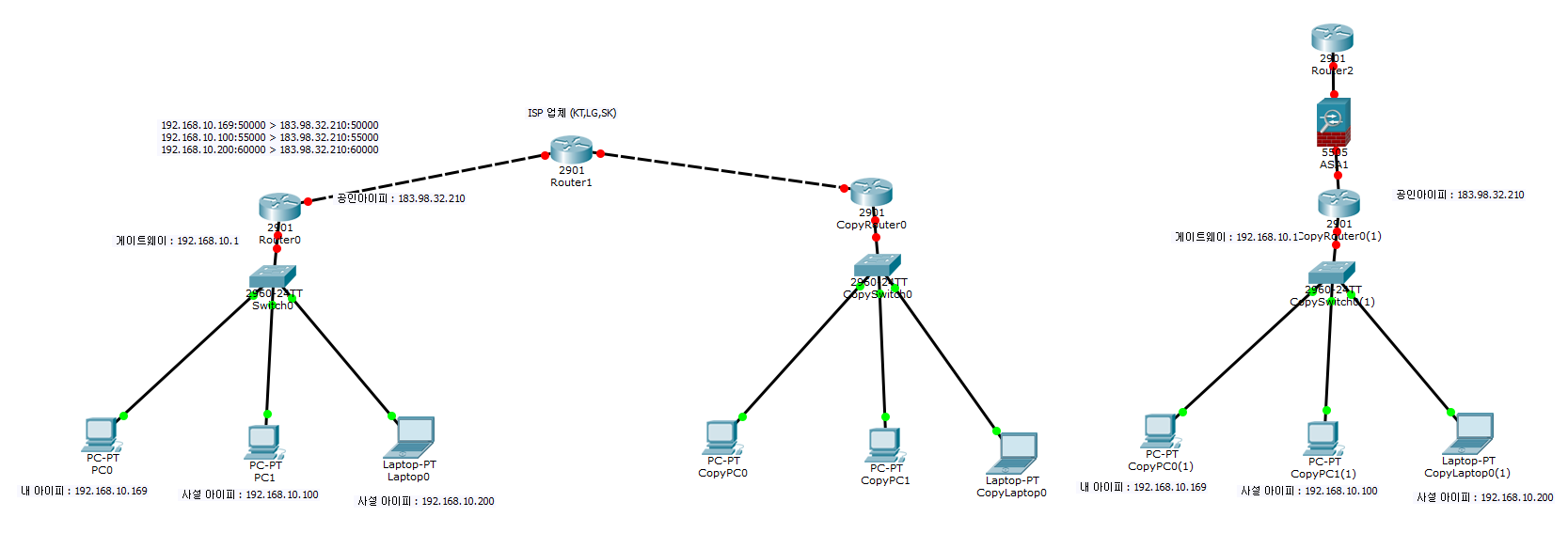
1. 사설 IP 주소를 정적인 하나의 공인 IP 주소로 매핑

2. 사설 IP 주소를 임의의 공인 IP 주소들 중에서 어떤 하나와 매핑

3. 사설 IP 주소에 특정 TCP 포트를 더한 것을 하나의 공인 IP 주소로 매핑

4. 공인 IP 주소를 사설 IP 주소 중의 하나로 (순서는 라운드 로빈 방식을 사용) 매핑 할 수 있다.





- 아키텍처 정의서

