제2장 네트워크 주소 체계

1. 포트 번호

- '2-1.네트워크 주소 체계.pcap' 파일을 와이어샤크로 실행한다.
- TCP, UDP 헤더 안에 포함된 주소
- 주소 크기: 16bit(2^16 = 0~65535)
- 클라이언트 입장: 서비스 요청 및 실행
- 서버 입장: 서비스 구분 및 제공
- 참고 사이트:
  https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

User Ports(1024-49151)
- PC에서 사용하는 포트
- mysql 3306

Dynamic/PrivatePort (49152-65535)
- PC에서 사용하는 포트, 동적/사설 포트

System Ports (0-1023)
- 서비스 예약용
- 예전에 개발되어 있던 서비스
- http 80

EX) IANA Port Number 사이트에서 프로토콜(서비스)를 검색할수 있다. **__**기억해야할것**__**

TCP		UDP	
http	**80**	**domain(dns)**	**53**
https(ssl)	**443**	bootps(dhcp server)	67
telnet	23	bootpc(dhcp client)	68
ssh	**22**	syslog	514
ftp	21	ntp	123
ftp-data	20	snmp	161
smtp	25	tftp	69
pop3	110		
mysql	3306		

ex) 클라이언트가 서버에게 요청을 했을때 다음은 무엇을 요청한것인가?

- SA = source address
- DA = destination address
  DA 53은 domain을 요구한다
- ***포트 번호를 보고 클라이언트가 뭐를 요구하는지 파악할 수 있다.***

******SA포트번호는 테이블 번호, DA포트번호는 메뉴판이라고 생각하면 편하다.****

Window에서 포트 번호 확인법:
cmd창에서 'netstat' 명령어를 통해 네트워크 연결 상태를 확인할 수 있다:

```
C:₩Users₩Administrator>netstat

활성 연결

  프로토콜  로컬 주소          외부 주소          상태
  TCP    192.168.11.181:49733   153:https          ESTABLISHED
  TCP    192.168.11.181:49755   134:https          TIME_WAIT
  TCP    192.168.11.181:49802   tp-in-f188:5228    ESTABLISHED
  TCP    192.168.11.181:49827   208.103.161.1:https  ESTABLISHED
  TCP    192.168.11.181:49832   27:https           ESTABLISHED
  TCP    192.168.11.181:49879   3:https            ESTABLISHED
  TCP    192.168.11.181:49893   110.93.158.140:https  ESTABLISHED
  TCP    192.168.11.181:49897   110.93.158.140:https  ESTABLISHED
  TCP    192.168.11.181:49935   218:https          TIME_WAIT
  TCP    192.168.11.181:49943   218:https          TIME_WAIT
  TCP    192.168.11.181:49946   211:https          TIME_WAIT
```

- ***여기서 상태가 ESTABLISHED 면 서버와 연결된 상태이다. 나머지는 연결이 안된거다.***

Ex1) 'netstat' 정보 확인을 이용한 네트워크 연결 상태 확인

프로토콜	로컬 주소	외부 주소	상태
TCP	192.168.10.27:49469	211.241.228.21:80	ESTABLISHED
TCP	192.168.10.27:49473	211.241.228.25:443	ESTABLISHED
TCP	192.168.10.27:49476	121.160.34.231:21	FIN_WAIT_2
TCP	192.168.10.27:49479	61.42.100.13:22	CLOSE_WAIT
TCP	192.168.10.27:49481	61.42.100.13:23	ESTABLISHED

- 클라이언트의 IP 주소: 192.168.10.27
- 클라이언트가 제공받고 있는 서비스 또는 연결된 서비스는 무엇인가? :
  - 클라이언트와 연결된 외부주소의 포트 번호를 볼때
  - 80 : http
  - 443 : https
  - 23 : telnet

Ex2) '192.168.10.27'은 서버인가? 클라이언트인가?

프로토콜	로컬 주소	외부 주소	상태
TCP	192.168.10.27:80	211.241.228.21:43511	ESTABLISHED
TCP	192.168.10.27:443	211.241.228.25:53122	ESTABLISHED

- system ports를 사용하고, 외부주소의 포트가 User Ports이므로 서버이다.

2. IP 주소

- IP 헤더 안에 포함된 주소
- 주소 크기: 32bit(2^32개 = 4,294,967,296)
    - 2012년 2월에 ipv4주소 고갈
    - 우리나라는 1억몇천개 정도 가지고 있다. ‘
    - IPv6 128bit = 2^128 (간 단위)
- ***로컬 환경에서 리모트 환경으로 데이터 전송 담당***
- 변경이 가능한 논리적인 주소(만들어서/설정해서 사용하는 주소)
- LAN이 아닌 다른 네트워크(WAN)으로 보낼때는 IP가 필수이다.
- IP 주소검색: https://xn--c79as89aj0e29b77z.xn--3e0b707e/
    - 나라, 할당한 회사 등을 알 수 있다.

3. MAC 주소

- ETH 헤더 안에 포함된 주소
- 주소 크기: 48bit(2^48개)
- ETH 로컬 환경 내에서 데이터 전송 담당
- **00-e0-4c**-14-62-ba
  [----------]
  OUI 24bit: 랜카드 업체(이더넷 장치 업체)가 IEEE 기관으로부터 임대받은 주소
    - ex)
        - cisco (00-00-0C)
- 변경 불가능한 물리적인 주소
- MAC 주소 조회 사이트: https://aruljohn.com/
    - 나라, 제조업체 등을 알 수 있다.

Ex) 시스템 주소 관련 예제

C:₩Users₩Administrator>**ipconfig /all**

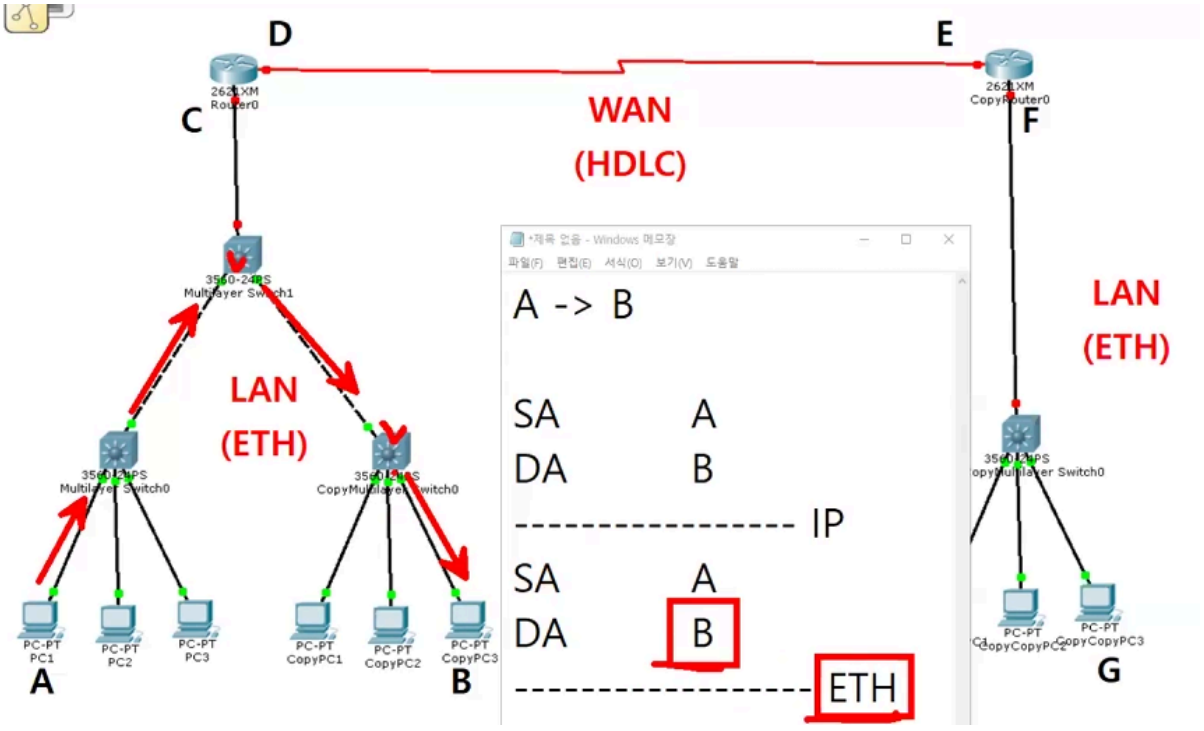
```
이더넷 어댑터 이더넷:

   연결별 DNS 접미사. . . . :
   설명. . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   물리적 주소 . . . . . . . . : 00-D8-61-6E-30-B4
   DHCP 사용 . . . . . . . . . : 예
   자동 구성 사용. . . . . . . : 예
   링크-로컬 IPv6 주소 . . . . : fe80::b069:5b58:6879:a6ac%14(기본 설정)
   IPv4 주소 . . . . . . . . . : 192.168.10.27(기본 설정)
   서브넷 마스크 . . . . . . . : 255.255.255.0
   임대 시작 날짜. . . . . . . : 2022 년 4 월 13 일 수요일 오전 9:18:08
   임대 만료 날짜. . . . . . . : 2022 년 4 월 13 일 수요일 오전 11:18:06
   기본 게이트웨이 . . . . . . : 192.168.10.1
   DHCP 서버 . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . : 100718689
   DHCPv6 클라이언트 DUID. . . : 00-01-00-01-27-BE-97-9A-00-D8-61-6E-30-B4
   DNS 서버. . . . . . . . . . : 168.126.63.1
                                 168.126.63.2
   Tcpip 를 통한 NetBIOS. . . . : 사용
```

- 현재 PC는 수동 IP 설정 방식인가? 아님 DHCP 서비스 방식인가?
    - DHCP 사용
- PC IP 주소와 서브넷 마스크는 어떻게 되는가?
    - 192.168.10.27
    - 255.255.255.0
- 게이트웨이 주소?
    - 192.168.10.1
- DNS 서버 주소?
    - 168.126.63.1
- MAC 주소?
    - 00-D8-61-6E-30-B4
- MAC 주소 검색 후 어느 회사 제품파악:
    - Micro-Star
- PC(시스템/호스트)를 구분할때 IP 주소, MAC 주소 중에 어떤 주소가 구분이 정확한가?
    - MAC주소

데이터 전송 체계 (그림예제)

ex) 같은 네트워크 일 경우우

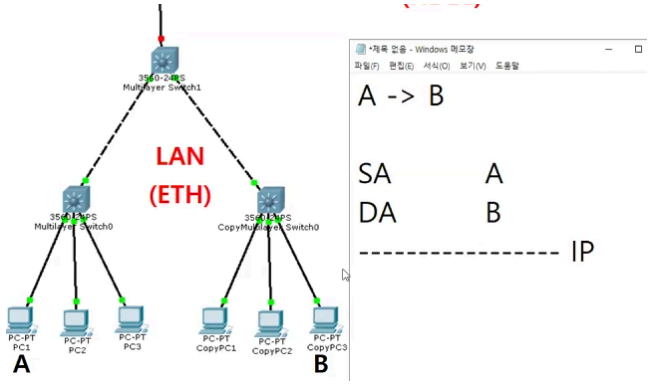


A⇒ B (A에서 B로 데이터를 전송. 같은 네트워크이다.)
SA A
DA B
—----------IP
SA A
DA B
—----------ETH (Mac Address)

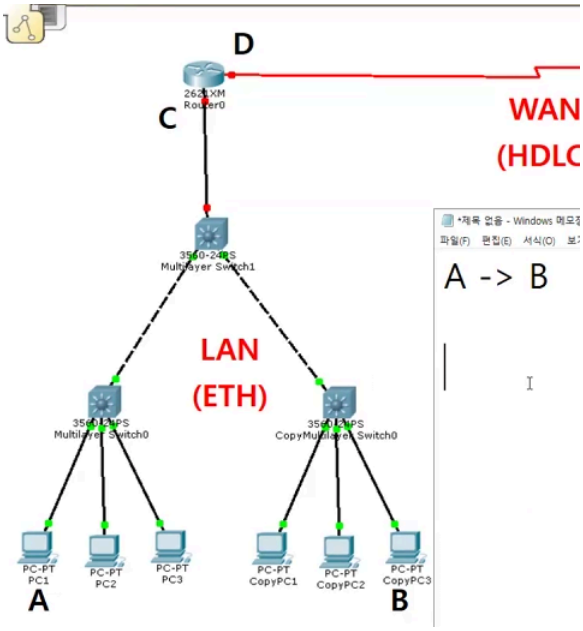
****** 스위치라는 장비는 기본적으로 ETH 헤더만 본다.***

- ***ETH 헤더의 목적지를 확인해서 맞는 방향으로 전기 신호를 보낸다.***

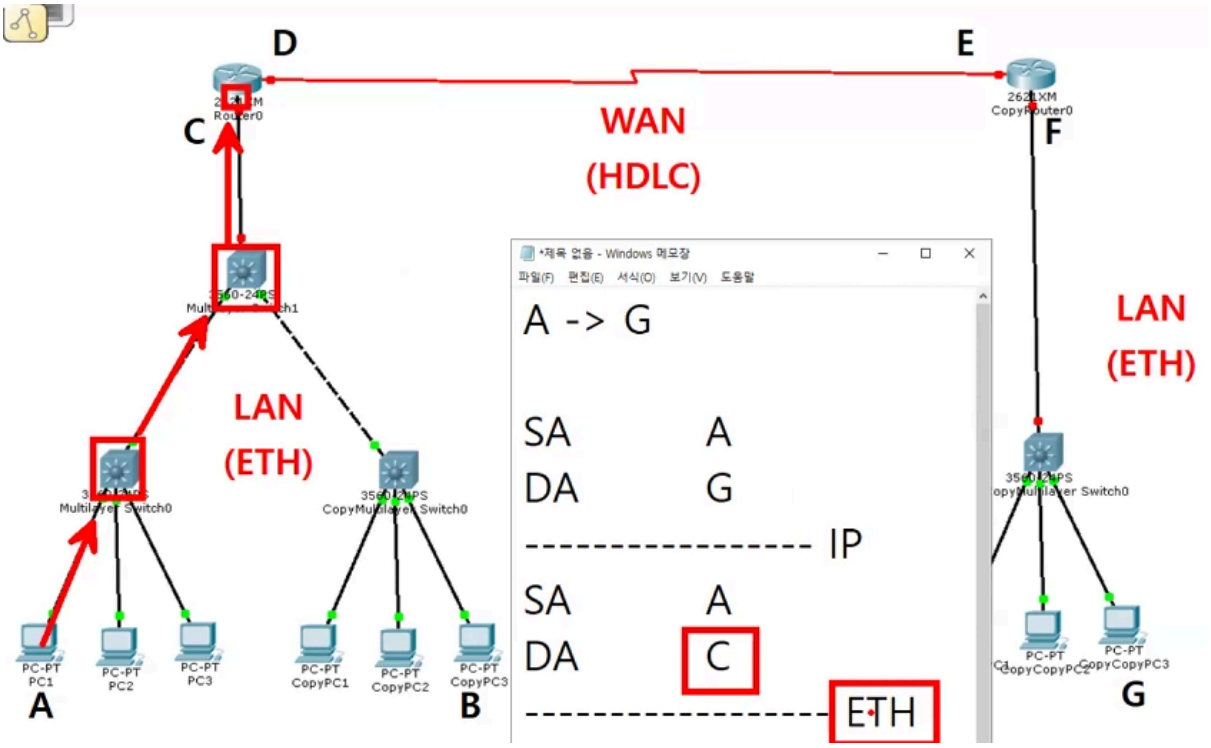
A PC에서 출발 → 스위치에서 목적지로 이동(ETH 헤더 이용) → 목적지 PC 도착
목적지에 도달했을때 B PC는 ETH 헤더를 확인 한 뒤 ETH를 뜯어낸다 (decapsulation)



마지막으로 PC가 IP 헤더를 확인 한 뒤, IP를 뜯어낸다 (decapsulation)



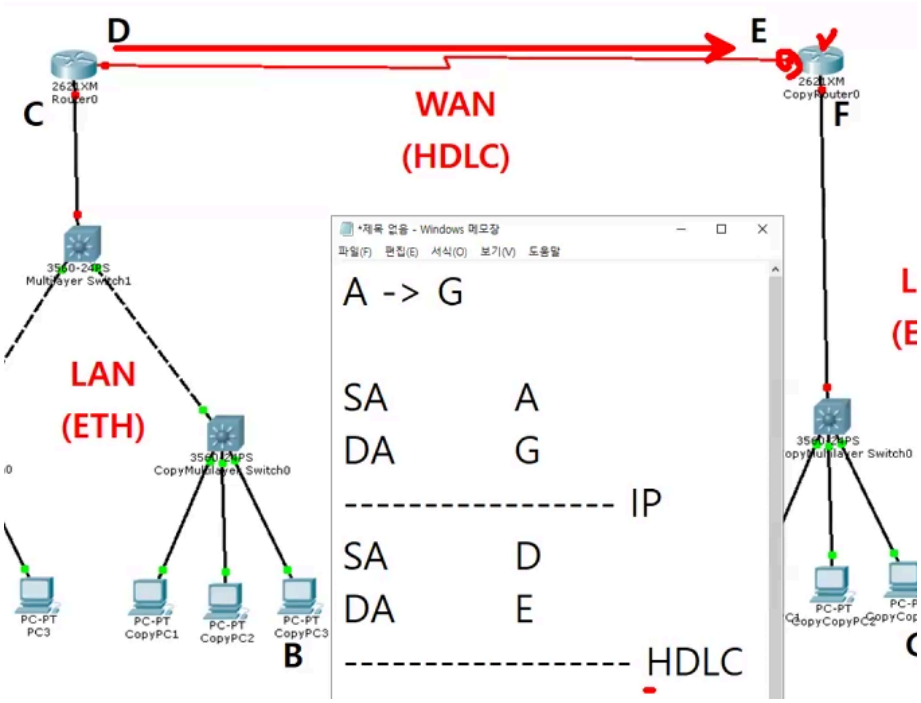
ex) 다른 네트워크 일 경우 (A → G)
ETH은 같은 네트워크에서 데이터를 전송하려고 만들어진거기 때문에 다른네트워크로 엑세스를 못한다. 그러므로, 현재 네트워크의 게이트웨이 까지만 설정한다.



데이터가 게이트웨이까지 이동하면 ETH의 목적지가 자기한테 온걸 확인 한 후 뜯어낸다 (decapsulation)

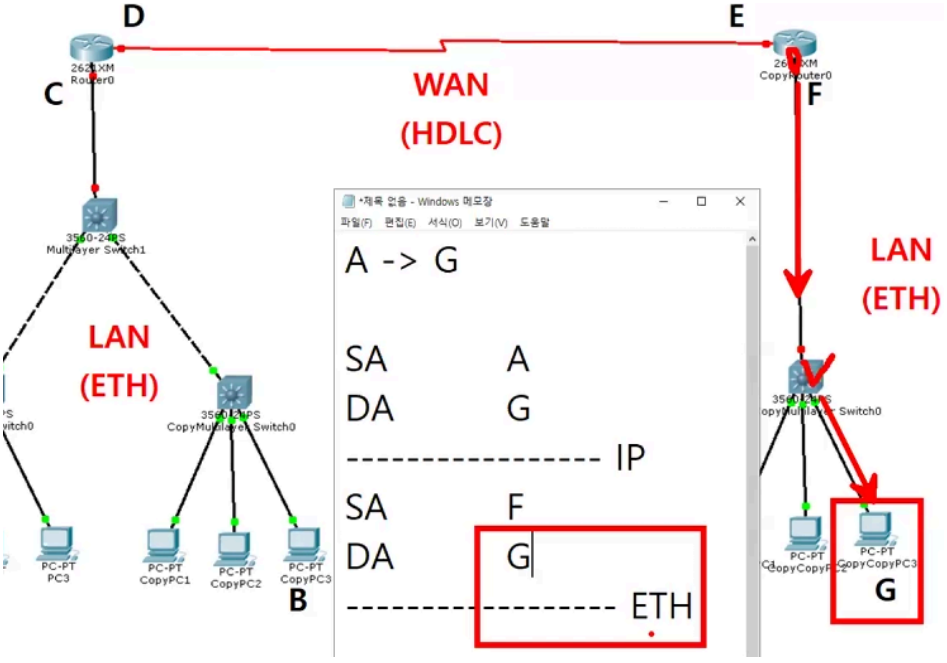
다른 네트워크끼리 데이터 전송을 하려면 WAN을 사용한다. 여기서는 HDLC 프로토콜을 사용하므로 새로 HDLC 프로토콜을 덮어씌워준다.

여기서 출발지는 현재 있는 게이트웨이, 목적지는 보내는 다른 네트워크의 게이트웨이 이다. 이 예제에서는 D, E이다.

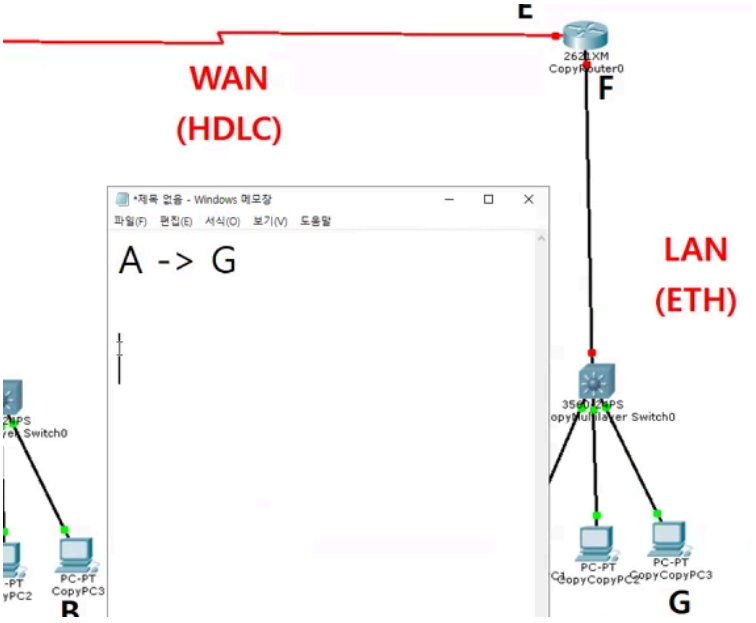


다른 네트워크의 게이트웨이에 도착했을때, 자기 자신한테 도착한게 맞으므로 HDLC헤더를 decapsulation 한다. 그러나 IP는 자기한테 온 것이 아니므로 목적지를 다시 정해줘야한다.

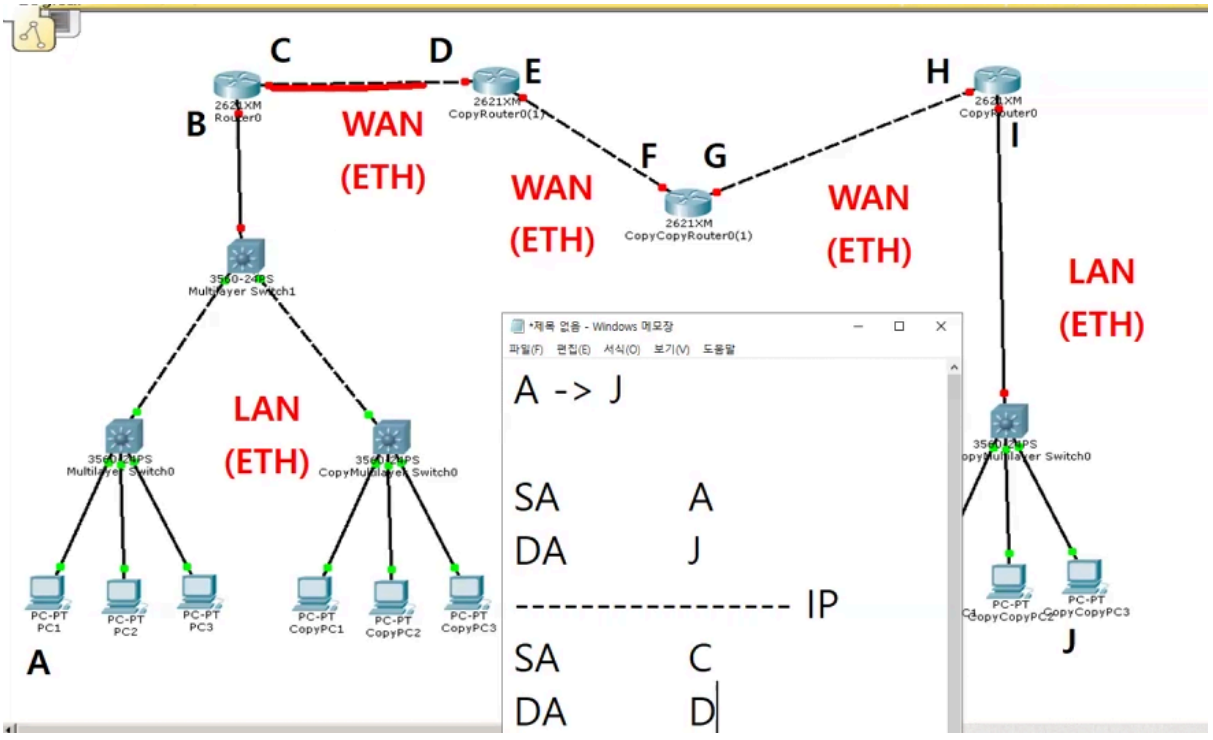
이제 목적지의 PC가 같은 네트워크에 있기 때문에 다시 ETH 헤더를 encapsulation 한다. 출발지는 F(현 네트워크의 게이트웨이), 목적지는 G(PC) 이다.



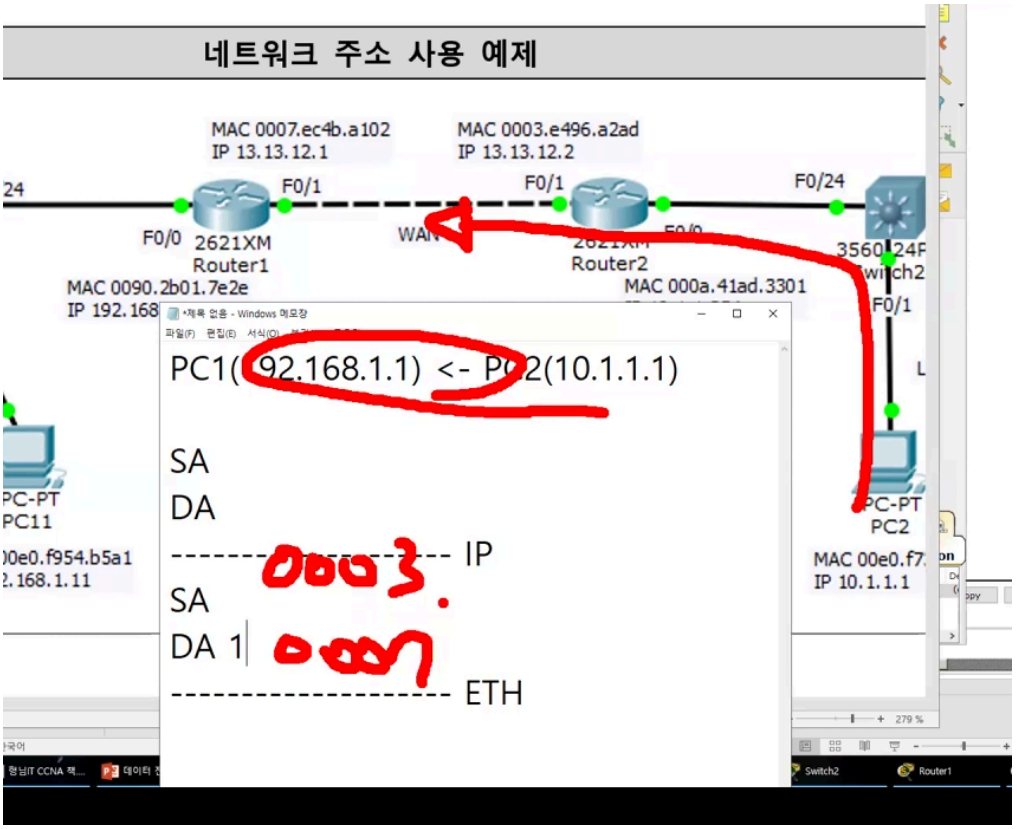
데이터가 스위치를 통해 G에 도달했을때 PC는 ETH헤더를 확인한후 자기한테 온 것이 맞으면 Decapsulation 한다.
마지막으로 IP 헤더를 확인 한 후 맞으면 Decapsulation 한다.

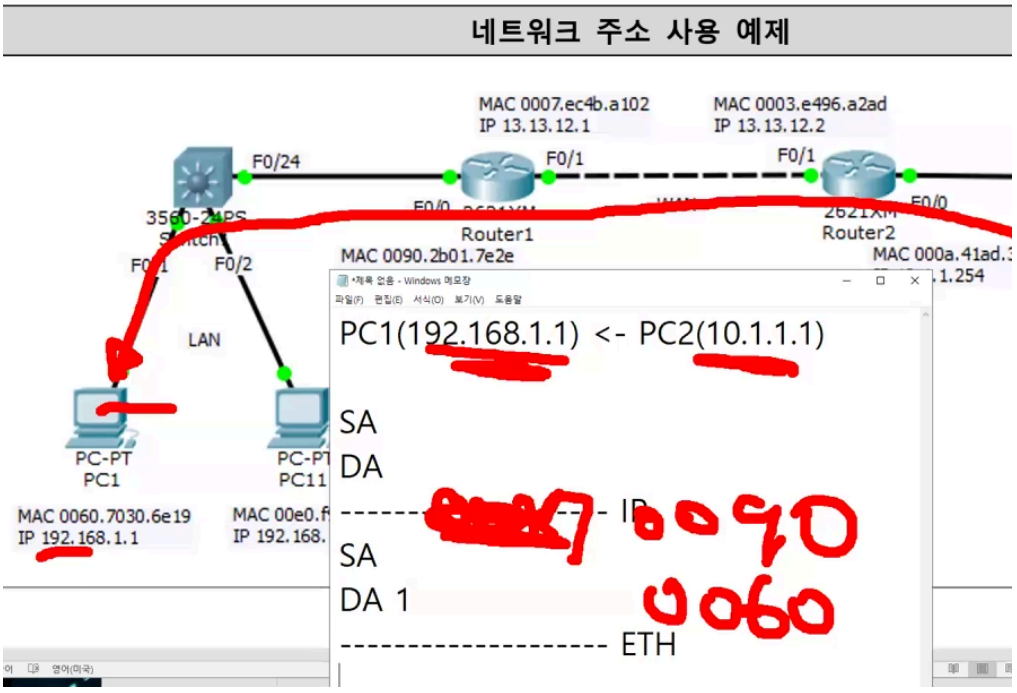


ex) 이런 경우에는 WAN끼리 이동할때마다 decap, encap을 해 줘야한다.
WAN, LAN 둘다 같은 ETH을 사용하지만 다른 정보를 가지고있다.

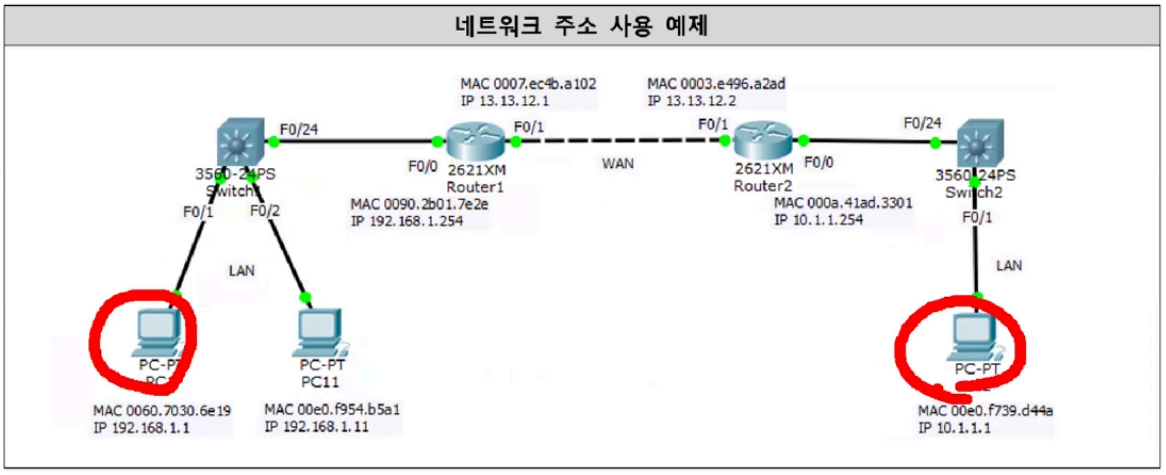


ex) 시험 문제중에 현 주소를 이야기해라:





'2-2.네트워크 주소 사용 예제.pkt' 파일을 실행한다.



PC1 → PC2로 데이터를 전송할때 출발지, 목적지 MAC은?

- SA 0060
- DA 0090

스위치 장비는 ETH 헤드까지만 본다

ETH 프로토콜은 같은 네트워크 안에서만 데이터를 전송할 수 있다.

다른 네트워크로 데이터를 전송할때는 ETH(LAN), IP. HDLC(WAN) 프로토콜을 함께 사용한다.

IP는 외부 통신네트워크로 보내기 위해서 만들어졌다.

다른 네트워크로 나가기 위해서는 라우터를 거쳐야 하는데, 다른 네트워크로 연결하는 통로를 게이트웨이(Gateway)라고 한다.