연세대학교
YONSEI UNIVERSITY

Project #3

- ARP Table Scanning -

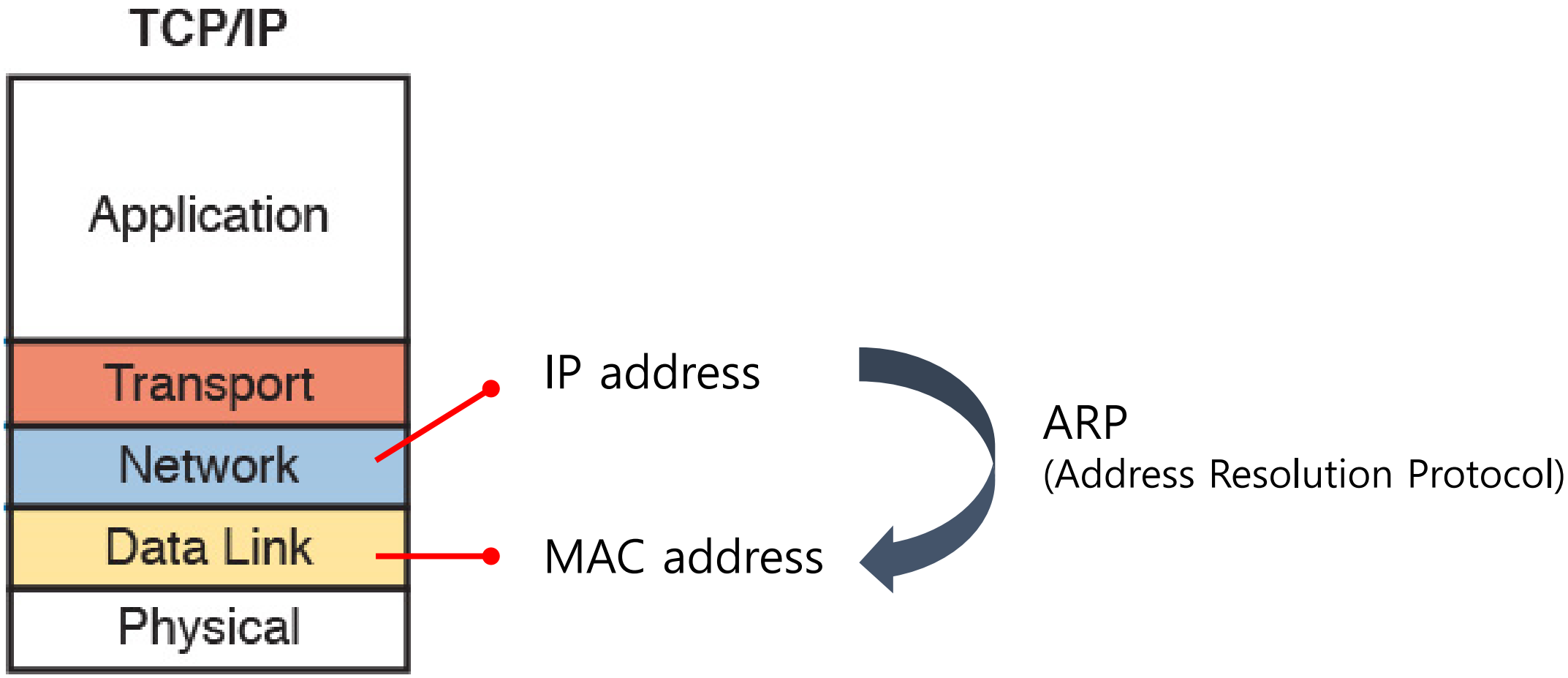
2023.11.29

과제 개요

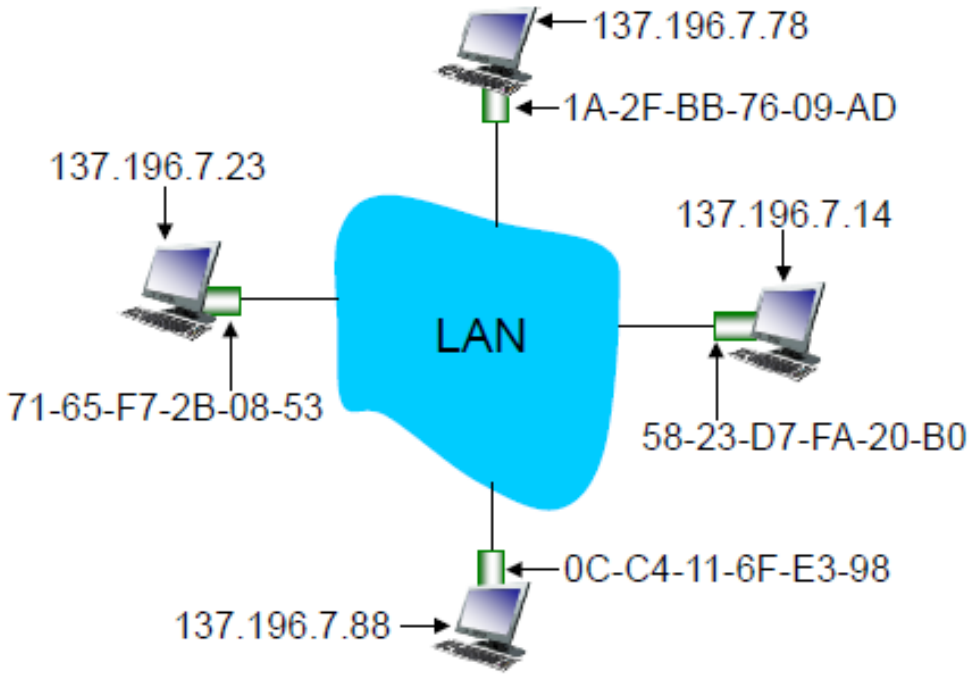
- 이동성 인식 기능 구현
  - ARP(Address Resolution Protocol) table scan을 통한 동일 subnet 내 기기들의 IP address 확인 기능 구현 (Python) 및 ARP 패킷 관찰 (Wireshark)

- Project #1, #2: server의 IP address를 직접 입력
- Project #3: 동일 subnet 내 기기들의 IP address를 scan하여 자동 입력

Address Resolution Protocol

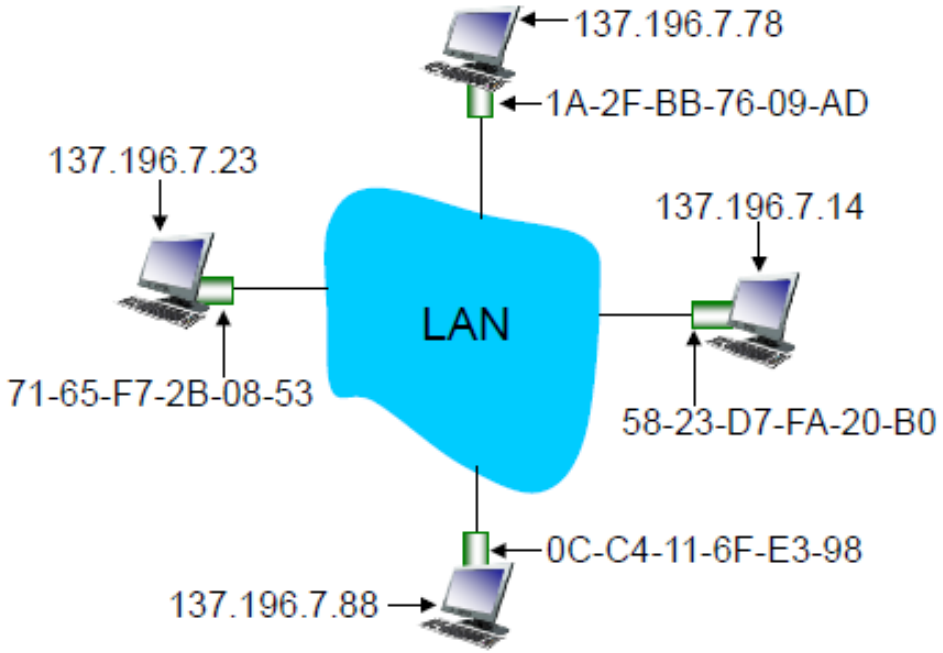


Address Resolution Protocol



- IP address
  - Host 가 움직이면 (다른 LAN으로 이동 시) 변경됨
- MAC address
  - Media Access Control Address
  - Network interface에 할당된 고유 식별 주소
  - 다른 LAN으로 이동해도 변경되지 않음

Address Resolution Protocol



- A host sends the frames with IP address and MAC address of the destination node
- How to know MAC address?
  - Hosts and routers have ARP table

Neighbour	Linklayer Address	Expire (O)	Expire (I) Netif
10.0.0.1	0:c:29:12:34:56	2m25s	2m25s
10.0.0.41	0:c:29:65:43:21	39s	39s
10.0.0.47	0:c:00:00:00:01	1m14s	1m14s
10.0.0.53	ab:cd:ef:81:6:72	2m32s	2m32s
10.0.0.58	fe:dc:ba:11:e2:6e	1m51s	1m51s

- If the ARP table doesn't have an entry for the destination node?
  - Broadcast

과제 설명

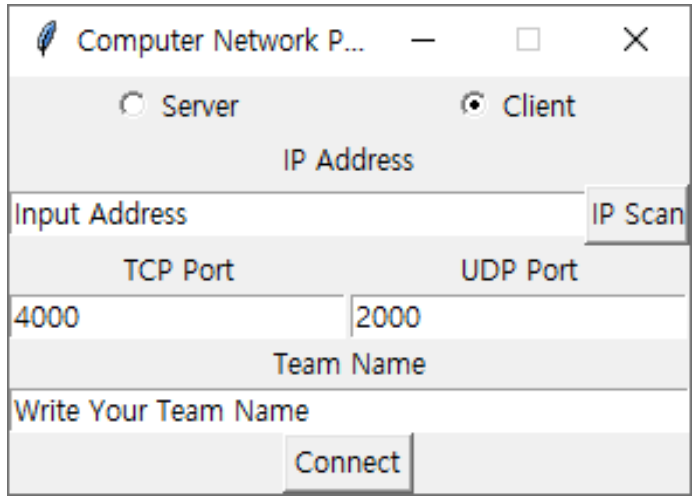
1. ARP Table Scan을 통한 주변 기기 IP address 확인 기능
   - 외부 Library 사용하여 ARP 패킷 발생
     - netifaces, psutil: gateway의 ip address 및 네트워크 인터페이스 이름 확인
     - scapy: layer 2 (link layer)에서의 ARP 패킷 생성 및 확인
   - ARPTable class의 get_ARP_table() 함수를 완성

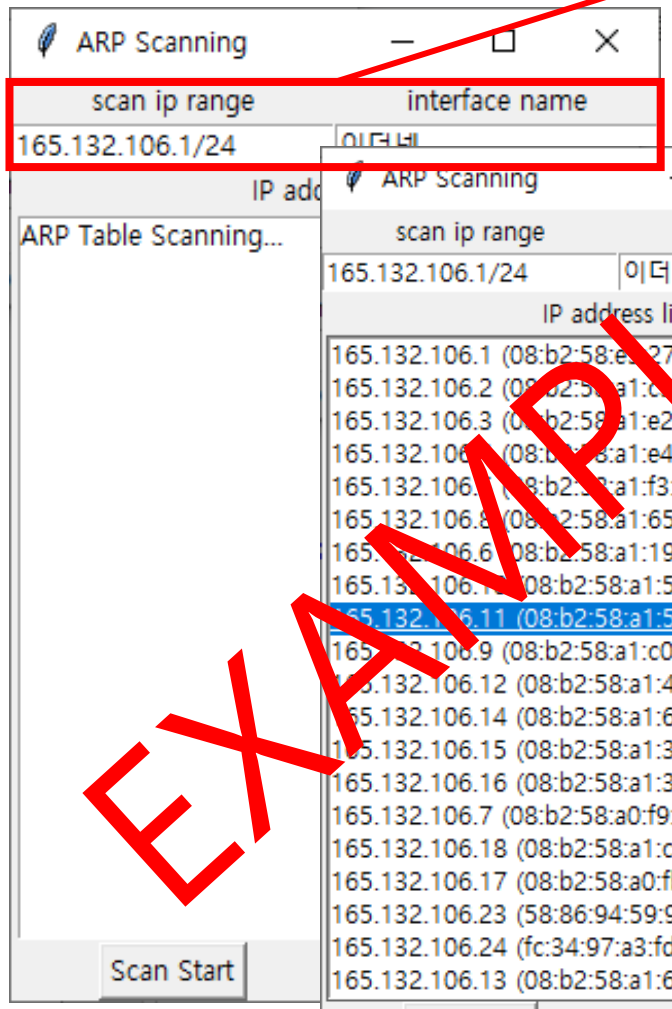
```
def get_ARP_table(self, interface:str, ips:str) -> int:
    # interface: 네트워크 인터페이스의 이름 ex) en0, wl0, 이더넷 등
    # ips: 탐색할 ip의 범위 ex) 192.168.0.1/24는 192.168.0.0 ~ 192.168.0.255까지 256개 ip 범위를 탐색
    # interface와 ips는 ARP scanning 창으로부터 사용자의 입력값을 받아서 설정됨

    self.ARP_table = list()
    self.interface = interface

    # todo: scapy의 srp를 사용해 ARP response를 get
    ans = None

    for snd, rcv in ans:
        # todo: arp response (ans)로부터 ip address와 mac address를 get
        ip_addr = None
        mac_addr = None
        self.ARP_table.append((ip_addr, mac_addr))
```

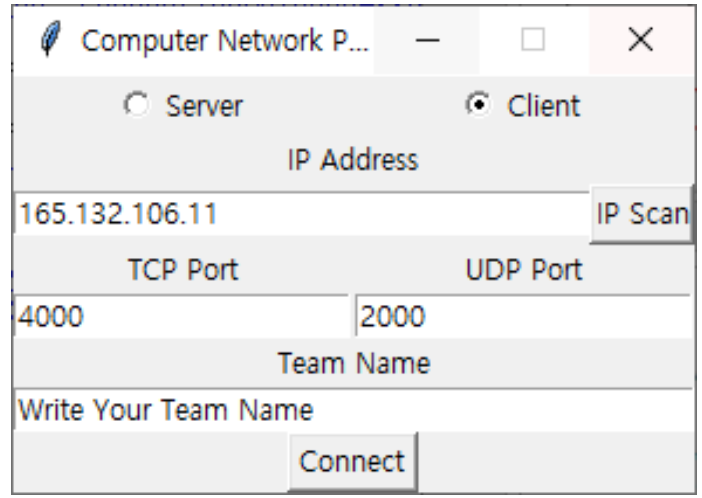
과제 설명

기본 코드인 default_ip_nif()로부터 router의 ip 및 interface name을 반환하여 자동으로 입력됨

-> 직접 입력할 필요 없음

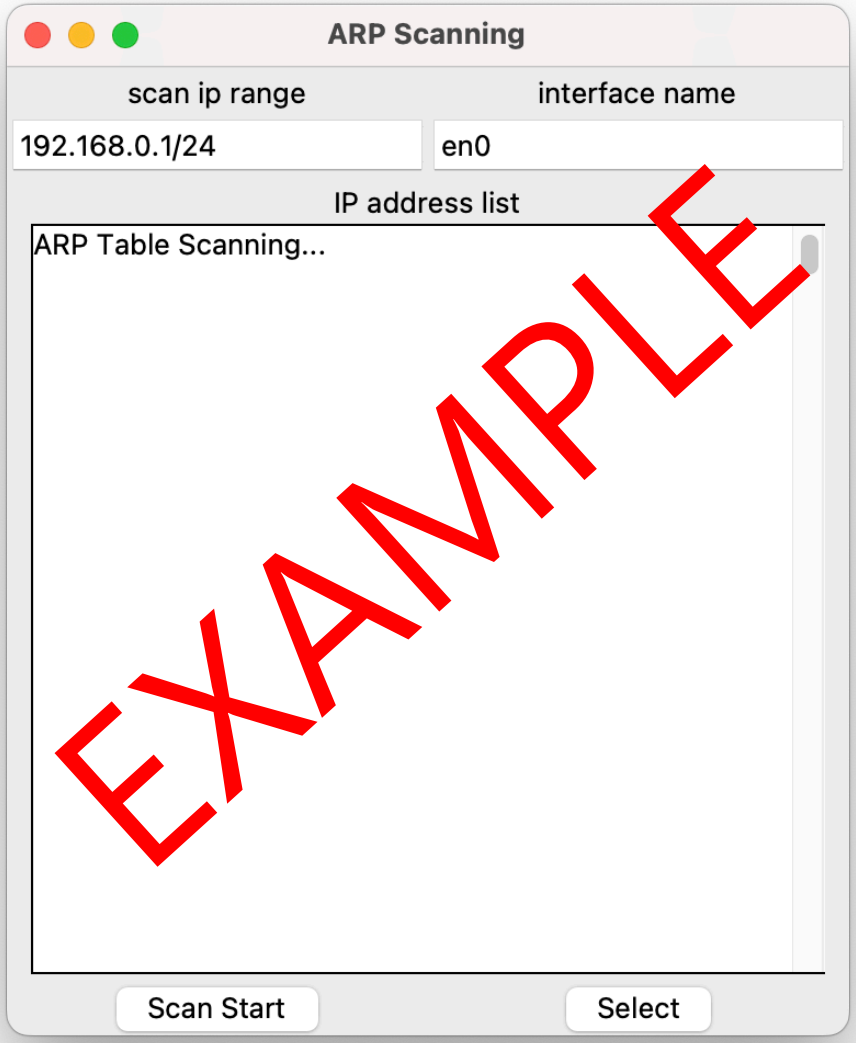


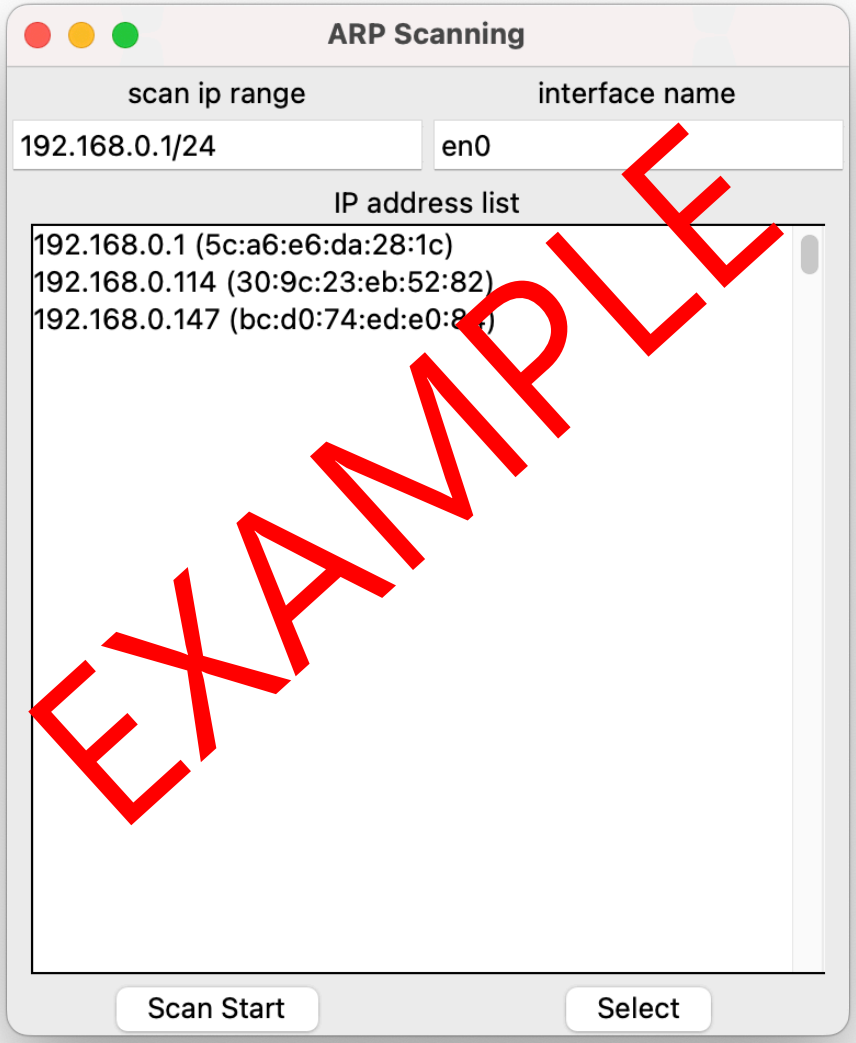




EXAMPLE

과제 설명

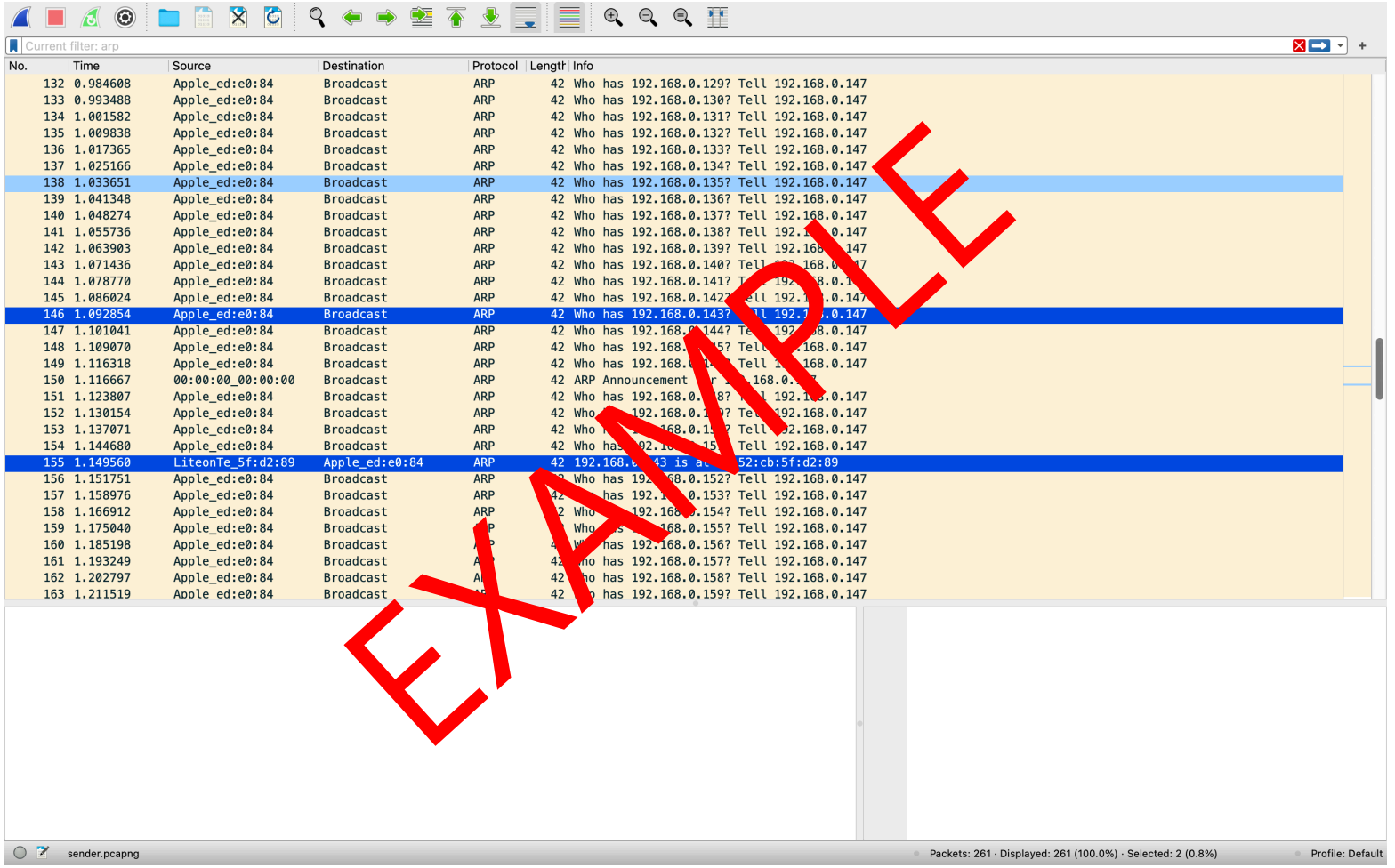

ARP Scanning
scan ip range
interface name
192.168.0.1/24
en0
IP address list
ARP Table Scanning...
Scan Start
Select
EXAMPLE


ARP Scanning
scan ip range
interface name
192.168.0.1/24
en0
IP address list
192.168.0.1 (5c:a6:e6:da:28:1c)
192.168.0.114 (30:9c:23:eb:52:82)
192.168.0.147 (bc:d0:74:ed:e0:8
Scan Start
Select
EXAMPLE

과제 설명

2. Wireshark를 통한 ARP 패킷 관찰
   - Wireshark 패킷 캡처 시작 후 pj_3를 통해 ARP 패킷을 발생시켜 관찰
   - Scan 중일 경우
     - ARP 패킷이 주기적으로 발생 (ms 단위)
     - "Who has xxx.xxx.xxx.xxx? Tell xxx.xxx.0.Y" query 패킷과 그에 대한 response 패킷 (일반적으로 Y는 2~255 사이의 값)

과제 설명



제출 방법

- 팀원 중 한 명만 제출
- 유의사항
  - ✓ pj_1.py와 pj_2.py 파일을 동일 directory에 위치
  - ✓ 학교 등 외부 - 테더링 이용 권장
  - ✓ 집 – 공유기 이용 가능
- 제출 파일
  - ✓ Project 압축 파일 (파일명: 팀이름_zip)
  - ✓ 보고서 (파일명: 팀이름_pdf): 다음 슬라이드 참고
- 제출 마감
  - ✓ 12월 20일 (수) 23시 59분
  - ✓ 단, 질문은 20일 (수) 18시까지만 가능

제출 방법

- **보고서 작성 내용**

  1) 구현 환경 및 코드에 대한 설명

  3) 정상 동작 스크린샷 (ARP table scanning 기능)

  4) Wireshark를 사용해 sender (ARP packet 발생시킨 host)와 receiver (ARP packet 수신한 host) 각각의 ARP 패킷 관찰 스크린샷

  5) Mobility에 따른 IP address 및 ARP table 확인

  5-1) 장소 A에 있을 때

  - Wireless network interface를 disable 시키기 전과 disable 시킨 후 다시 enable 시켰을 때의 IP address 및 ARP table 변화 확인 (스크린샷 및 간단한 설명)

  5-2) 장소 A에서 B로 이동했을 때

  - 장소 이동 후 IP address 및 ARP table 변화 확인 (스크린샷 및 간단한 설명)
    - ✓ 방법 1) 물리적으로 다른 장소로 이동하여 새로운 공유기에 연결
    - ✓ 방법 2) 하나의 모바일 기기의 테더링을 활성화시켜 공유기로 설정 -> 연결된 기기 중 하나의 기기를 모바일 기기와 거리가 멀어지게 하거나, 연결을 끊고 다른 공유기에 연결

  5-3) 5-1과 5-2의 IP address 및 ARP table 변화에 대한 차이점 및 이유 간단히 서술 (200자 이내)

❖ 장소 A: 기존에 머물러 있던 장소(ex. 교내, 집 등) / 장소 B: 새롭게 이동한 장소(ex. 세브란스, 외부 커피숍 등)

❖ 단, 교내에서의 이동은 불가

연세대학교
YONSEI UNIVERSITY

Q&A