

Project #3

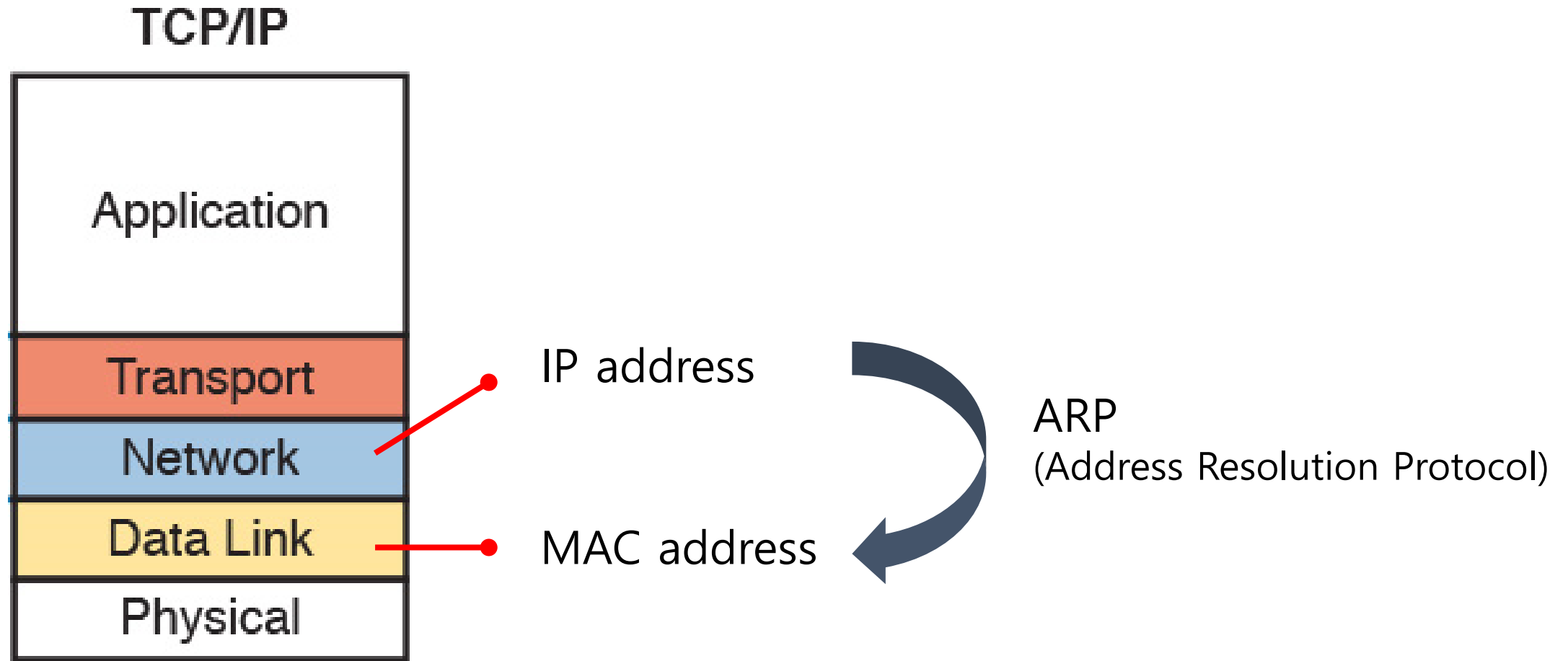
- ARP Table Scanning -

2023.11.29

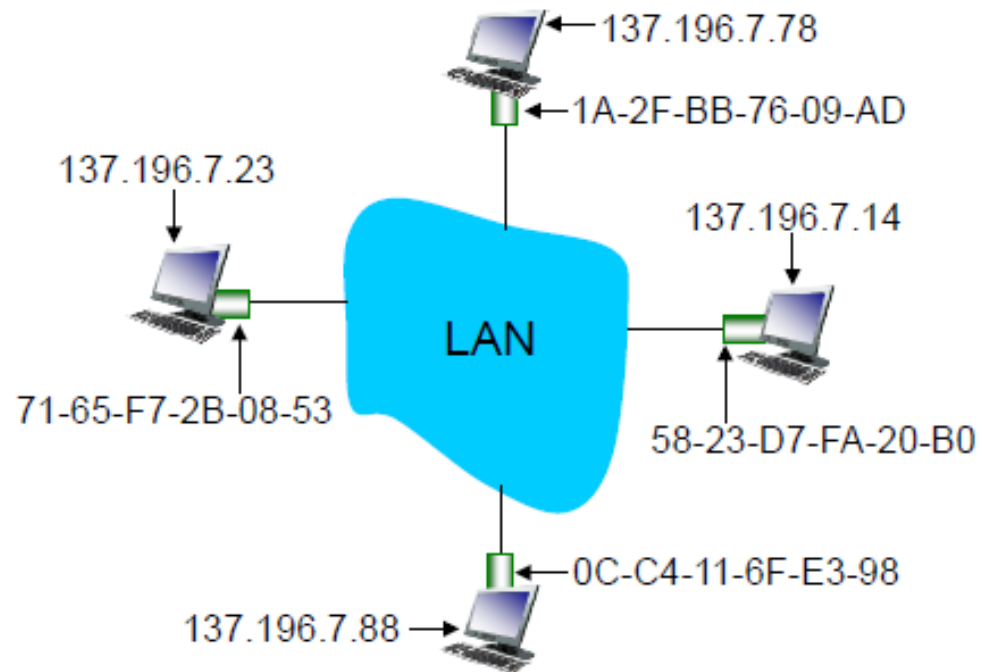
과제 개요

- 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

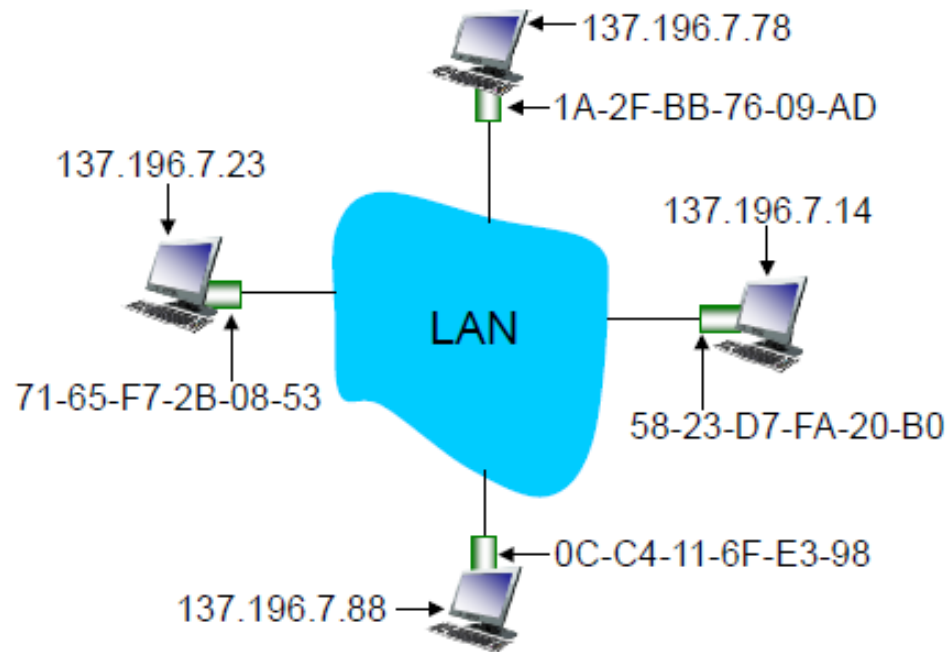


Address Resolution Protocol



- 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, wlan0, 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

Computer Network P... — □ ×

☐ Server ☒ Client

IP Address

Input Address IP Scan

TCP Port UDP Port

4000 2000

Team Name

Write Your Team Name

Connect

ARP Scanning — □ ×

scan ip range interface name

165.132.106.1/24 이더넷

ARP Table Scanning...

IP address list

165.132.106.1 (08:b2:58:a1:c7:f0)

165.132.106.2 (08:b2:58:a1:c7:01)

165.132.106.3 (08:b2:58:a1:e2:4)

165.132.106.4 (08:b2:58:a1:e4:81)

165.132.106.5 (08:b2:58:a1:f3:c1)

165.132.106.6 (08:b2:58:a1:65:41)

165.132.106.7 (08:b2:58:a1:19:41)

165.132.106.8 (08:b2:58:a1:5c:81)

165.132.106.9 (08:b2:58:a1:c0:01)

165.132.106.10 (08:b2:58:a1:4b:81)

165.132.106.11 (08:b2:58:a1:63:41)

165.132.106.12 (08:b2:58:a1:3a:01)

165.132.106.13 (08:b2:58:a1:39:41)

165.132.106.14 (08:b2:58:a0:f9:41)

165.132.106.15 (08:b2:58:a1:ce:81)

165.132.106.16 (08:b2:58:a0:fb:01)

165.132.106.17 (58:86:94:59:9e:95)

165.132.106.18 (fc:34:97:a3:fd:ca)

165.132.106.19 (08:b2:58:a1:60:81)

Scan Start

Computer Network P... — □ ×

☐ Server ☒ Client

IP Address

165.132.106.11 IP Scan

TCP Port UDP Port

4000 2000

Team Name

Write Your Team Name

Connect

과제 설명

ARP Scanning

scan ip range

192.168.0.1/24

interface name

en0

IP address list

ARP Table Scanning...

Scan Start

Select

ARP Scanning

scan ip range

192.168.0.1/24

interface name

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:e0:84)

Scan Start

Select

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

Current filter: arp

No.	Time	Source	Destination	Protocol	Length	Info
132	0.984608	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.129? Tell 192.168.0.147
133	0.993488	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.130? Tell 192.168.0.147
134	1.001582	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.131? Tell 192.168.0.147
135	1.009838	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.132? Tell 192.168.0.147
136	1.017365	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.133? Tell 192.168.0.147
137	1.025166	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.134? Tell 192.168.0.147
138	1.033651	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.135? Tell 192.168.0.147
139	1.041348	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.136? Tell 192.168.0.147
140	1.048274	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.137? Tell 192.168.0.147
141	1.055736	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.138? Tell 192.168.0.147
142	1.063903	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.139? Tell 192.168.0.147
143	1.071436	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.140? Tell 192.168.0.147
144	1.078770	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.141? Tell 192.168.0.147
145	1.086024	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.142? Tell 192.168.0.147
146	1.092854	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.143? Tell 192.168.0.147
147	1.101041	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.144? Tell 192.168.0.147
148	1.109070	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.145? Tell 192.168.0.147
149	1.116318	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.146? Tell 192.168.0.147
150	1.116667	00:00:00_00:00:00	Broadcast	ARP	42	ARP Announcement for 192.168.0.147
151	1.123807	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.148? Tell 192.168.0.147
152	1.130154	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.149? Tell 192.168.0.147
153	1.137071	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.150? Tell 192.168.0.147
154	1.144680	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.151? Tell 192.168.0.147
155	1.149560	LiteonTe_5f:d2:89	Apple_ed:e0:84	ARP	42	192.168.0.143 is at 52:cb:5f:d2:89
156	1.151751	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.152? Tell 192.168.0.147
157	1.158976	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.153? Tell 192.168.0.147
158	1.166912	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.154? Tell 192.168.0.147
159	1.175040	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.155? Tell 192.168.0.147
160	1.185198	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.156? Tell 192.168.0.147
161	1.193249	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.157? Tell 192.168.0.147
162	1.202797	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.158? Tell 192.168.0.147
163	1.211519	Apple_ed:e0:84	Broadcast	ARP	42	Who has 192.168.0.159? Tell 192.168.0.147

sender.pcapng Packets: 261 · Displayed: 261 (100.0%) · Selected: 2 (0.8%) Profile: Default

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

Q&A