Network Advanced

강사. 유효곤

(ugonfor@gmail.com)

본 수업의 강의자료는 이경문(gilgil, BoB멘토, 고려대 사이버국방학과 겸임교수)멘토님의 강의자료를 상당수 차용하였음을 밝힙니다.

Contents

- 네트워크란,review
- 과제 Review
  - Pcap programming
  - Socket programming
- 네트워크 보안
  - 호스트는 어떻게 라우터와 통신하는 가?
  - Arp (Address Resolution Protocol)
  - Arp Spoofing
- 네트워크 프로그래밍
  - Test
  - Demo

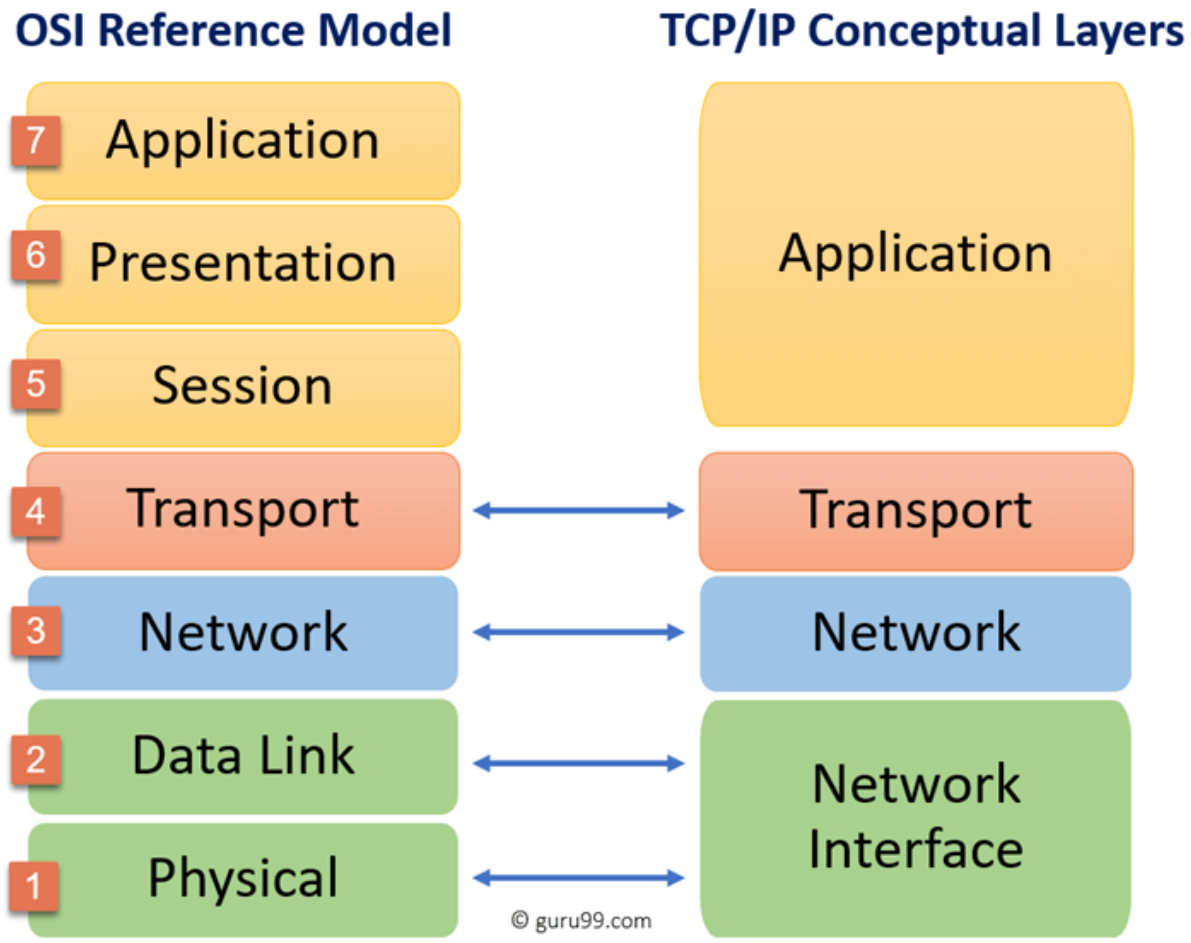
네트워크란, review

Network Model

Ethernet header, IP header, TCP/UDP header

Network Model

OSI reference Model / TCP.IP Model



Network Model

OSI reference Model / TCP.IP Model

OSI reference Model	TCP/IP Model	Layer Number	Protocol
Application	Application	L7(Firewall)	HTTP, SSH, Telnet, ···
Presentation			
Session			
Transport	Transport	L4(NAT)	TCP, UDP
Network	Network	L3(Router)	IP, IPv6, ARP, ICMP, ···
Data Link	Network Interface	L2(Switch)	Ethernet
Physical			

Ethernet, IP, TCP/UDP header

모든 프로토콜을 알아야 하는 가?

- Ethernet, IP, TCP/UDP 는 필수
- 나머지 프로토콜들은 필요에 따라 그때그때 배우면 됨.

프로토콜	목적
Ethernet	MAC 주소 정보를 통해 근거리 통신의 목적지 확인
IP	IP 주소 정보를 통해 장거리 통신의 목적지 확인
UDP	포트 정보를 통해, 목적지 기기의 포트 정보 확인
TCP	포트 정보를 통해, 목적지 기기의 포트 정보 확인 UDP에서 혼잡제어, 흐름제어, 데이터 유실 등을 고려한 프로토콜

과제 Review

Socket Programming

Pcap programming

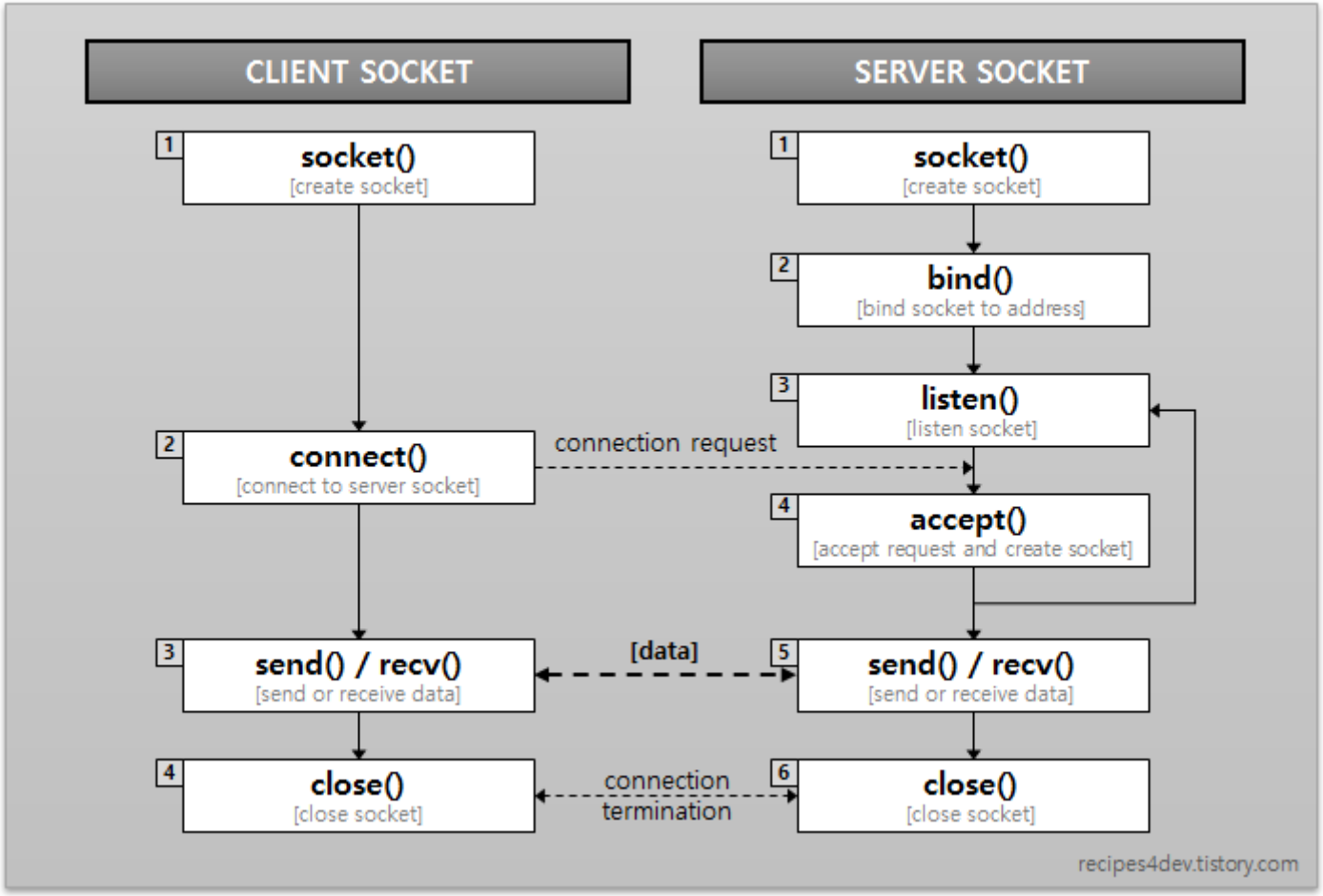
Socket Programming

소켓 프로그래밍

- code/socket에 주어진 소켓프로그래밍 예제를 확인해보자.
- Socket
  - 프로세스와 실제 네트워크를 연결해주는 **통로!**
  - 네트워크 프로그래밍 인터페이스(UC Berkeley에서 만든 Unix 표준 통신 인터페이스)
- 대부분의 웹 어플리케이션들이 Socket 인터페이스를 기반으로 만들어져있음

Socket Programming

소켓 프로그래밍



Pcap programming

Pcap 프로그래밍

- code/pcap에 주어진 pcap 프로그래밍 예제를 확인해보자.
- Pcap programming
  - libpcap을 다운 받아야 사용 가능하다.
    - sudo apt install libpcap-dev
  - 소켓과는 다르게 tcpdump(https://www.tcpdump.org/)에서 만든 **패킷 캡쳐** 라이브러리
  - 보통 네트워크 트래픽 관리를 할 때 이 라이브러리를 사용한다.
  - https://github.com/the-tcpdump-group/libpcap

Pcap programming

Pcap 프로그래밍

- https://www.tcpdump.org/pcap.html
- https://www.tcpdump.org/manpages/pcap.3pcap.html
- 위 사이트에서 여러 API들을 확인해볼 것

Description	Functions
pcap 핸들 열기	pcap_open, pcap_open_live, pcap_open_offline
pcap 핸들 닫기	pcap_close
packet 수신	pcap_next_ex
packet 송신	pcap_sendpacket

과제

과제설명

1. 소켓 프로그래밍

- code/socket 에 주어진 코드를 바탕으로 함.
- Client가 보낸 메시지를 relay하고 출력하는 server.cpp, client.cpp 작성

- ./server <port> [-e]
  - 옵션이 없을 경우에는 단순히 client가 보낸 메시지를 ./server에서 출력
  - -e 옵션이 주어지면, client가 보낸 메시지를 다시 client에게 전송
- ./client <IP address> <port>
  - 화면에 입력으로 서버로 메시지를 전송
  - 서버로 부터 오는 메시지를 recv해서 화면에 출력
    - 쓰레딩을 통해 구현하면 되지 않을까요?

과제

과제설명

2. 패킷 캡쳐 프로그램

- code/pcap 에 주어진 코드를 바탕으로 함.
- 패킷 캡쳐 시 Ethernet – IP – TCP 로 구성된 패킷에 대해서만 , source MAC, IP, PORT 와 Destination MAC, IP, PORT 정보를 출력하는 패킷 캡쳐 프로그램 작성
- 헤더를 인터넷에서 잘 찾아서, 변형해서 사용하거나! 직접 만들어 사용할 것!
  - https://github.com/afabbro/netinet/blob/master/ip.h
  - https://github.com/afabbro/netinet/blob/master/tcp.h
  - https://sites.uclouvain.be/SystInfo/usr/include/net/ethernet.h.html

네트워크 보안

호스트는 어떻게 라우터와 통신하는 가?

Arp (Address Resolution Protocol)

Arp Spoofing

호스트는 어떻게 라우터와 통신하는 가?

ICMP를 통해 알아보자

google
IP : <IP>
Mac : <MAC>

Gateway
IP : <IP>
Mac : <MAC>

Me
IP : <IP>
Mac : <MAC>

ICMP				
	ETH		IP	
	SMAC	DMAC	SIP	DIP
Request				
Reply				

프로토콜	목적
Ethernet	MAC 주소 정보를 통해 근거리 통신의 목적지 확인
IP	IP 주소 정보를 통해 장거리 통신의 목적지 확인

호스트는 어떻게 라우터와 통신하는 가?

ICMP를 통해 알아보자

- Ping 8.8.8.8을 실행하면,
  - Gateway로 패킷이 전송됨
  - Gateway에서 패킷이 8.8.8.8로 전송됨
  - 8.8.8.8에서 Gateway로 패킷이 전송됨
  - Gateway에서 Me로 패킷이 전송됨

- Me는 Gateway의 Mac Address는 어떻게 아는 가? **ARP Table**에 저장되어 있음.
  - Arp Table: ip – mac address pair를 저장한 Table
  - 그럼, 처음부터 Gateway에 대한 정보가 Arp Table에 박혀있는 가? No.
  - 어떻게 Arp Table을 채울 수 있지? Arp Protocol

Arp (Address Resolution Protocol)

Arp Table을 채우는 방법

64	46.067305866	VMware_91:a3:83	Broadcast	ARP	42 Who has 172.30.1.254? Tell 172.30.1.8
65	46.072650493	Allradio_85:68:83	VMware_91:a3:83	ARP	60 172.30.1.254 is at 00:07:89:85:68:83

<table>
<tr><td colspan="2">Hardware type
(2bytes)</td><td>Protocol type
(2bytes)</td></tr>
<tr><td>Hardware
address length
(1bytes)</td><td>Protocol
address length
(1bytes)</td><td>Operation code
(2bytes)</td></tr>
<tr><td colspan="3">Source hardware address
(6bytes)</td></tr>
<tr><td colspan="3">Source protocol address
(4bytes)</td></tr>
<tr><td colspan="3">Target hardware address
(6bytes)</td></tr>
<tr><td colspan="3">Target protocol address
(4bytes)</td></tr>
</table>

Arp (Address Resolution Protocol)

ARP를 통해 알아보자

Gateway
IP : <IP>
Mac : <MAC>

You
IP : <IP>
Mac : <MAC>

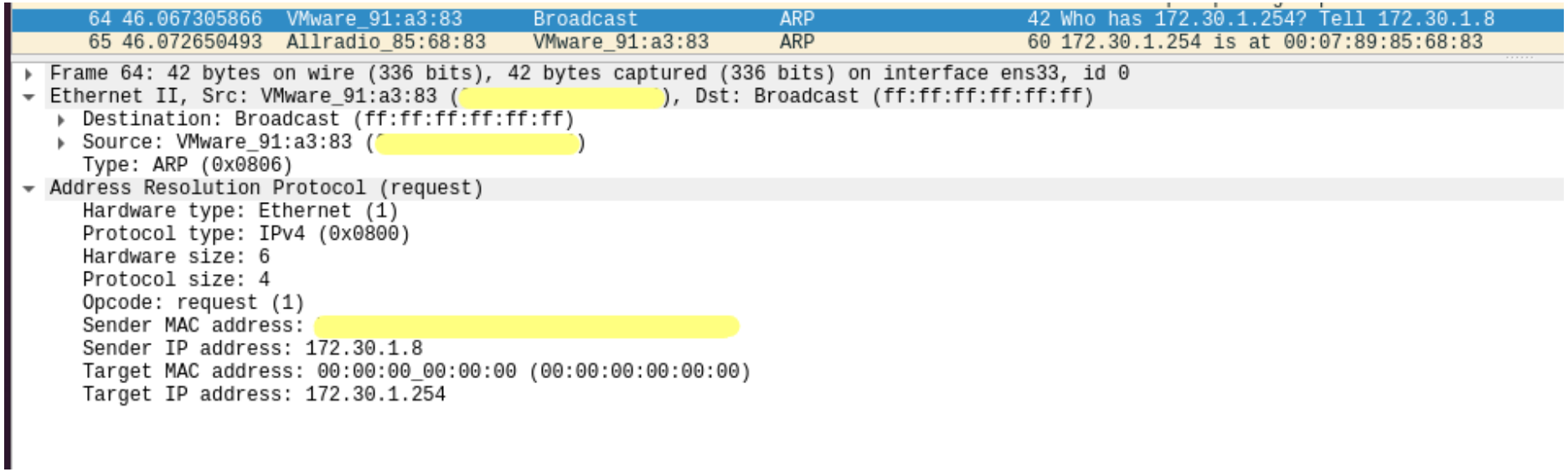
Me
IP : <IP>
Mac : <MAC>

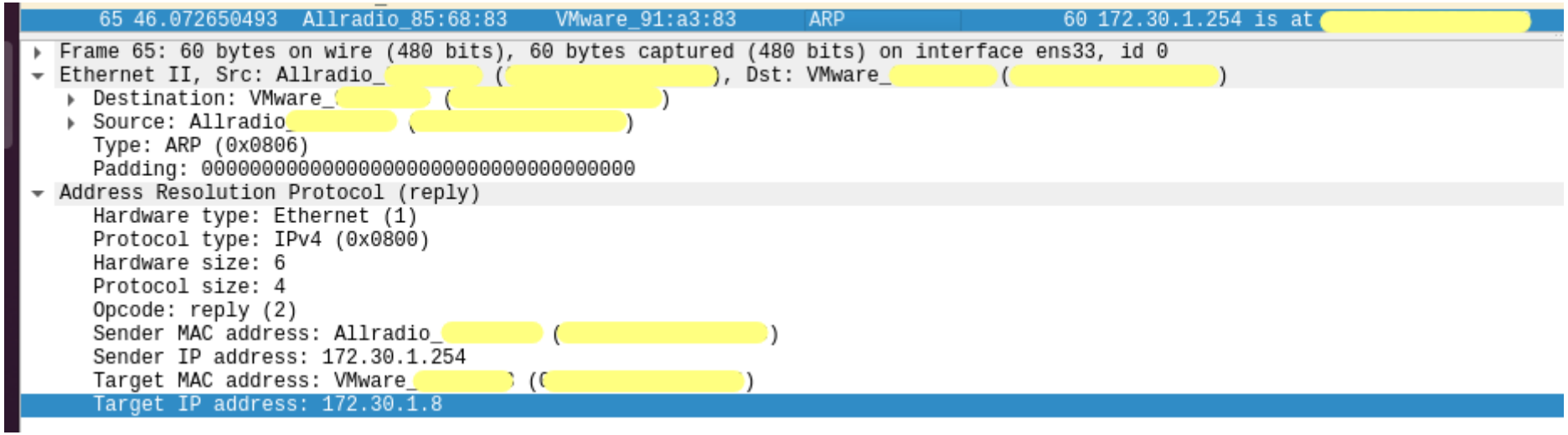
ARP						
	ETH		ARP			
	SMAC	DMAC	SMAC	SIP	TMAC	TIP
Request						
Reply						

프로토콜	목적
Ethernet	MAC 주소 정보를 통해 근거리 통신의 목적지 확인
IP	IP 주소 정보를 통해 장거리 통신의 목적지 확인

Arp (Address Resolution Protocol)

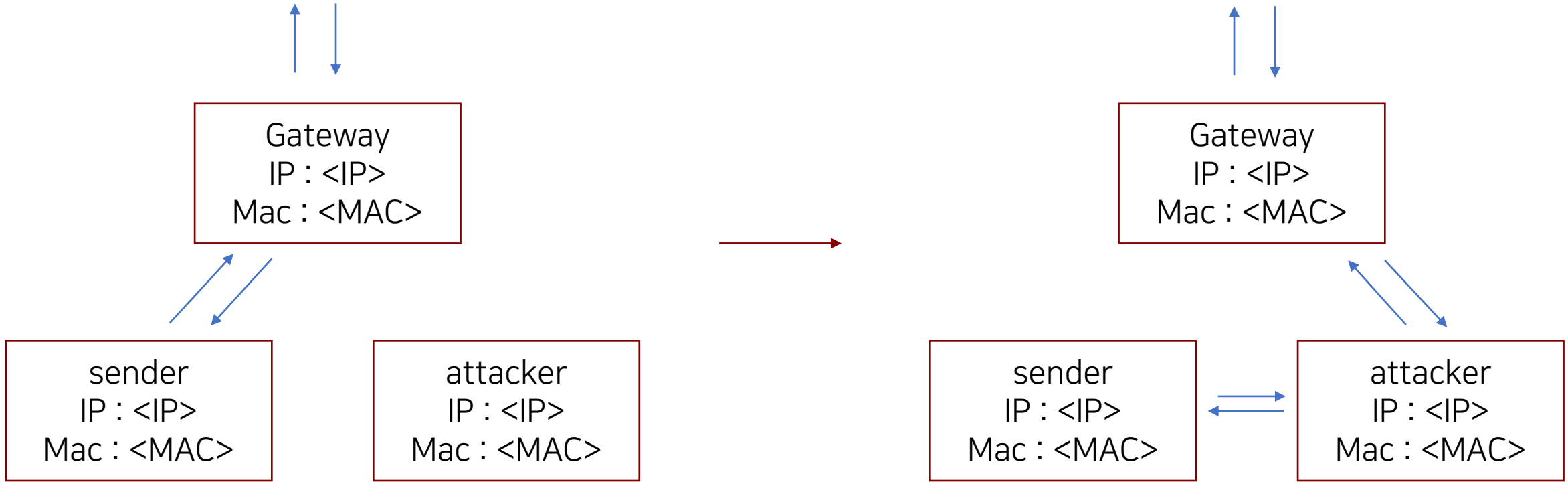
Wireshark를 통해 실제로 확인해보자.





Arp (Address Resolution Protocol)

Arp spoofing



네트워크 프로그래밍

Test

Demo

네트워크 프로그래밍

Test

- Code/Arp/Test 확인
- Wireshark와 함께 확인해보기

네트워크 프로그래밍

Demo

- Code/Arp/Demo 확인
- 옆에 친구들과 패킷을 날려보며 확인

-

- 7주간 수업 듣느라 수고하셨습니다 :)
- 설문조사 해주세요~
- https://forms.gle/yDw7tMgCPzXp157g9