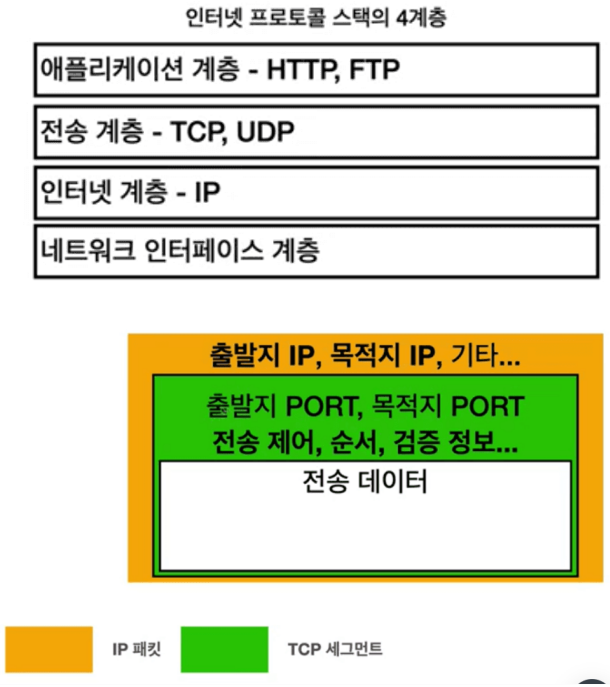
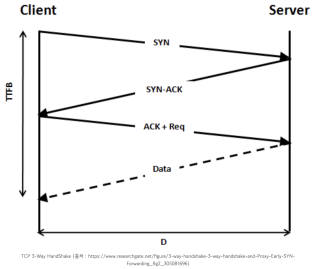
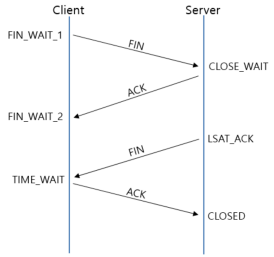
질문 및 개념	답변	중요도	관련 개념
			

TCP/IP 개념 및 설명	IP는 인터넷 프로토콜로 두 가지 역할 - 지정한 IP Address에 데이터 전달 - 패킷이라는 통신 단위로 데이터 전달 위 기능을 수행하는 프로토콜이지만 한계점을 가지고 있다 - 비연결성 : 패킷 받을 대상이 없거나 서비스 불능 상태여도 패킷 전송 - 비신뢰성 : 중산에 패킷이 사라기저가 패킷이 순서대로 오지 않을 가능성 - 프로그램 구분 : 같은 IP를 사용하는 서버에서 통신 애플리케이션이 둘 이상일 경우 위와 같은 IP 프로토콜의 한계를 해결해주는 것이 TCP 프로토콜 인터넷 프로토콜은 4계층이 있으며 이 순서를 통해 통신한다 1. 애플리케이션 계층의 프로그램에서 전송하고자 하는 **메시지를 생성**한다. 2. 그리고 해당 계층의 SOCKET 라이브러리를 통해 **전송계층에 전달**한다. 3. 전송계층에서 **TCP 정보를 생성**하고 **메시지 데이터를 포함하여 해당 내용을 인터넷 계층으로** 넘겨준다. 4. 인터넷 계층에서는 **IP 패킷을 생성**하고, **TCP 데이터를 포함하며 이 내용을 네트워크 인터페이스 계층으로** 전달시킨다. 5. 네트워크 인터페이스 계층은 **여러 장비를(LAN 카드) 통해 인터넷과 통신하며 서버에 데이터를 전송**한다. 4단계에서 TCP 데이터(세그먼트)를 포함하면서 한계점을 해결 (*인터넷 계층의 전송단위는 패킷, 전송계층의 전송단위는 세그먼트) TCP는 아래와 같은 특징 - 전송 제어 프로토콜(Transmission Control Protocol) - 연결지향(TCP 3 way handshake) - 데이터 전달 보증 - 순서 보장 - 신뢰할 수 있는 프로토콜 - 현재는 대부분이 TCP 를 사용한다. 여기서 중요한 것이 연결지향 3 way handshake 사진을 보면 SYN은 접속요청, ACK는 요청수락 1. 데이터 전송 2. 데이터 잘 받았다고 확인 3. 알았다고 확인 장점은 순서를 보장한다 패킷의 순서가 잘못되었다고 가정해보았을 때, 1. 패킷을 (1,2,3)으로 보냈다. 2. 패킷이 (1,3,2)로 도착했다. 3. 패킷을 2부터 다시 보내라고 요청한다.	중	
TCP와 UDP는 무엇이며 차이점은 무엇인가	TCP : 연결지향형 전송규약 - 흐름 중심 프로토콜, 통신을 주고받는 것을 중요시함 - 중간에 패킷이 손실되는 경우 재전송을 통해(SYN-ACK handshaking) 신뢰성을 보장함(느림) - 대부분의 통신에서 사용됨, 특히 파일이나 데이터 전송 시에 사용 - 데이터 경계 구분이 없음 (바이트 스트림 서비스) UDP : 비연결지향형 전송규약 - 데이터 중심 프로토콜, 주고받는 통신보다 데이터를 일방적으로 보내는 것을 중요시함 - 데이터 전송의 신뢰성 보장 X, (빠름) - P2P, 스트리밍, 전화에 사용	상	

TCP와 UDP는 무엇이며 차이점은 무엇인가	<table><tr><th>프로토콜 종류</th><th>TCP</th><th>UDP</th></tr><tr><td>연결 방식</td><td>연결형 서비스 (패킷 교환 방식)</td><td>비연결형 서비스 (데이터그램 방식)</td></tr><tr><td>전송 순서</td><td>전송 순서 보장</td><td>전송 순서가 바뀔 수 있음</td></tr><tr><td>수신 여부 확인</td><td>수신 여부를 확인함</td><td>수신 여부를 확인하지 않음</td></tr><tr><td>통신 방식</td><td>1:1 통신</td><td>1:1 OR 1:N or N:N 통신</td></tr><tr><td>신뢰성</td><td>높다</td><td>낮다</td></tr><tr><td>속도</td><td>느리다</td><td>빠르다</td></tr></table>	상
TCP 3-WAY-HANDSHAKE	3-Handshaking : TCP에 쓰이는 연결 설정 - SYN/SYC : 통신 요청 데이터 - ACK : 응답 데이터 - SYN_RCV : 통신 요청 받음 이는 TCP/IP 통신 기법 중 하나로, TCP/IP 프로토콜을 이용하여 통신하기 전에 정확한 전송을 보장하고자 연결이 잘 되어있는지 확인하는 것이다. 보통 데이터 송수신 시작 전에 이뤄지고 순서는 크게 3단계로 진행된다. 먼저, 클라이언트는 서버에게 접속요청을 위한 SYN 패킷을 보낸다. 클라이언트는 SYN을 보낸 후 SYN/ACK 응답을 기다리는 SYN-SENT 상태가 된다. 그 다음, 서버가 Listen 상태일 경우에 SYN을 수신받는다. 이후 요청수락인 ACK와 SYN flag 패킷을 보낸다. 이 때, 서버는 SYN-RECEIVED 상태가 된다. 마지막으로 클라이언트는 ACK를 서버에게 보내고 이 이후부터는 연결상태로 되어 데이터를 송수신한다. 	중	
TCP 4-Way HandShake	TCP 3-Way HandShake 와는 반대로 데이터 송수신이 끝나고, 클라이언트와 서버 간 연결을 종료하기 위해 수행하는 것 이다. 먼저, 클라이언트가 서버에게 FIN Flag를 전송한다. 클라이언트가 전송하고나서 FIN-WAIT 상태가 된다. 다음으로, 서버가 FIN Flag를 받고, 클라이언트에게 ACK를 보낸다. 이 때, 서버는 CLOSE_WAIT 상태가 된다. 그럼 클라이언트는 다음 FIN Flag를 받기 전까지 TIME-OUT 상태가 되고, 남은 데이터를 받으며 종료할 준비를 한다. 데이터를 모두 보낸 서버는 이제 연결종료의 의미인 FIN Flag를 클라이언트에게 전송한다. 클라이언트는 이를 받고 ACK 메세지를 서버에 전송한다. 서버는 이러한 ACK 메세지를 받고 CLOSED 하는 것으로 클라이언트와 서버 간 통신은 마무리된다.  TCP 4-Way HandShake 과정 (출처 : https://steffen-lee.tistory.com/31)	하	

TCP 헤더에 대해 설명하세요	송신 측과 수신 측의 포트 번호, 연결 정보가 기록된 제어 비트, 오류를 검출할 때 사용되는 체크섬, 몇 번째 데이터인지 알려주는 시퀀스 번호, 몇 번째 데이터까지 수신했는지 알려주는 ACK 번호, 윈도우 크기 등이 헤더에 저장되어 있습니다.	하	
라우팅 알고리즘에 대해 설명하세요	라우팅 알고리즘이란 통신할 때 최적의 경로를 찾아 데이터를 전송하는 알고리즘 입니다. 이를 위해 능동적으로 라우팅을 수행하는 장비인 라우터가 사용됩니다. 대표적인 라우팅 알고리즘으로는 다익스트라 알고리즘과 벨만포드 알고리즈이 있습니다. 다익스르타 알고리즘은 방문하지 않은 노드 중에서 최단 거리가 가장 짧은 노드를 선택하는 알고리즘이고, 벨만포드 알고리즘은 매번 모든 노드를 확인하면서 거리가 가장 짧은 노드를 선택하는 알고리즘입니다.	하	
공인 IP와 사설 IP의 차이에 대해 설명하세요	공인 IP는 ISP(인터넷 서비스 공급자)가 제공하는 IP 주소로, 유일한 주소이며 외부에 공개되어 있습니다. 사설 IP는 IPv4의 주소 부족으로 인해 서브넷팅된 iP주소로 사설 IP만으로는 인터넷에 직접 접속할 수 없고, 라우터를 통해서만 인터넷에 접속할 수 있습니다.	하	