

TCP/IP 완벽 가이드

- 2-8부 TCP/IP 전송 계층 프로토콜-

김 지 혜(jihye@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

목 차

- 보충
 - ICMPv4 오류 메시지 유형
 - ICMPv4 정보 제공 메시지 유형
- TCP/IP 전송 계층 프로토콜
 - TCP 개요
 - TCP 원리와 일반 동작
 - TCP 기본 동작: 연결 수립, 관리와 종료
 - TCP 세그먼트 포맷과 데이터 송신
 - TCP 신뢰성과 흐름 제어 기능

목 차

- 보충
 - ICMPv4 오류 메시지 유형
 - ICMPv4 정보 제공 메시지 유형
- TCP/IP 전송 계층 프로토콜
 - TCP 개요
 - TCP 원리와 일반 동작
 - TCP 기본 동작: 연결 수립, 관리와 종료
 - TCP 세그먼트 포맷과 데이터 송신
 - TCP 신뢰성과 흐름 제어 기능

ICMPv4 오류 메시지 유형

- ICMPv4 목적지 접근 불가 메시지

- 메시지 하위 유형

코드값	메시지 하위 유형	설명
0	네트워크 접근 불가	지정된 네트워크로 전달될 수 없는 경우
1	호스트 접근 불가	지정된 네트워크로 전달됐지만, 호스트에는 전달되지 않는 경우
2	프로토콜 접근 불가	목적지 호스트에서 전송 프로토콜을 사용하지 못하는 경우
3	포트 접근 불가	TCP나 UDP 헤더 속 목적지 포트가 사용되지 않는 경우
4	DF(Don't Fragment)가 켜져 있음	IPv4 라우터는 데이터그램을 자동으로 단편화하지만, DF 플래그가 켜진 데이터그램은 출발지가 단편화 원치 않음을 의미
5	소스 라우팅 실패	라우터에 데이터그램의 소스 라우팅 옵션이 지정됐는데, 라우터가 그 경로로 포워딩할 수 없는 경우
6	알려지지 않은 목적지 네트워크	지정된 네트워크가 알려지지 않은 경우
7	알려지지 않은 목적지 호스트	지정된 호스트가 알려지지 않은 경우로, 보통 잘못된 주소를 의미

ICMPv4 오류 메시지 유형

• ICMPv4 목적지 접근 불가 메시지

• 메시지 하위 유형

코드값	메시지 하위 유형	설명
8	출발지 호스트 고립	더 이상 쓰이지 않음
9	목적지 네트워크로의 통신이 관리상 금지	목적지 장비가 위치한 네트워크로 데이터그램을 송신하는 것이 허용되어 있지 않은 경우
10	목적지 호스트로의 통신이 관리상 금지	목적지 장비가 위치한 네트워크로 데이터그램을 송신할 수 있지만, 특정 장비로 송신할 수 없는 경우
11	서비스 유형에 대한 목적지 네트워크 접근 불가	데이터그램 헤더의 서비스 유형 필드에 명시된 서비스 제공 불가, IP 주소에 지정된 목적지 네트워크에 접근 불가한 경우
12	서비스 유형에 대한 목적지 호스트 접근 불가	데이터그램 헤더의 서비스 유형 필드에 명시된 서비스 제공 불가, IP 주소에 지정된 목적지 호스트에 접근 불가한 경우
13	관리상 통신 금지	데이터그램이 메시지 내용에 의해 차단되어서 전달 불가한 경우
14	호스트 우선순위 위반	서비스 유형 필드의 우선순위 값이 허용되지 않아서, 첫 번째 홉 라우터에 의해 송신되는 경우
15	우선순위 차단	받은 데이터그램의 우선순위 값이 네트워크 상 허용된 최소값보다 작아서, 라우터가 송신하는 경우

ICMPv4 오류 메시지 유형

- ICMPv4 송신 속도 낮춤 메시지

- 정의

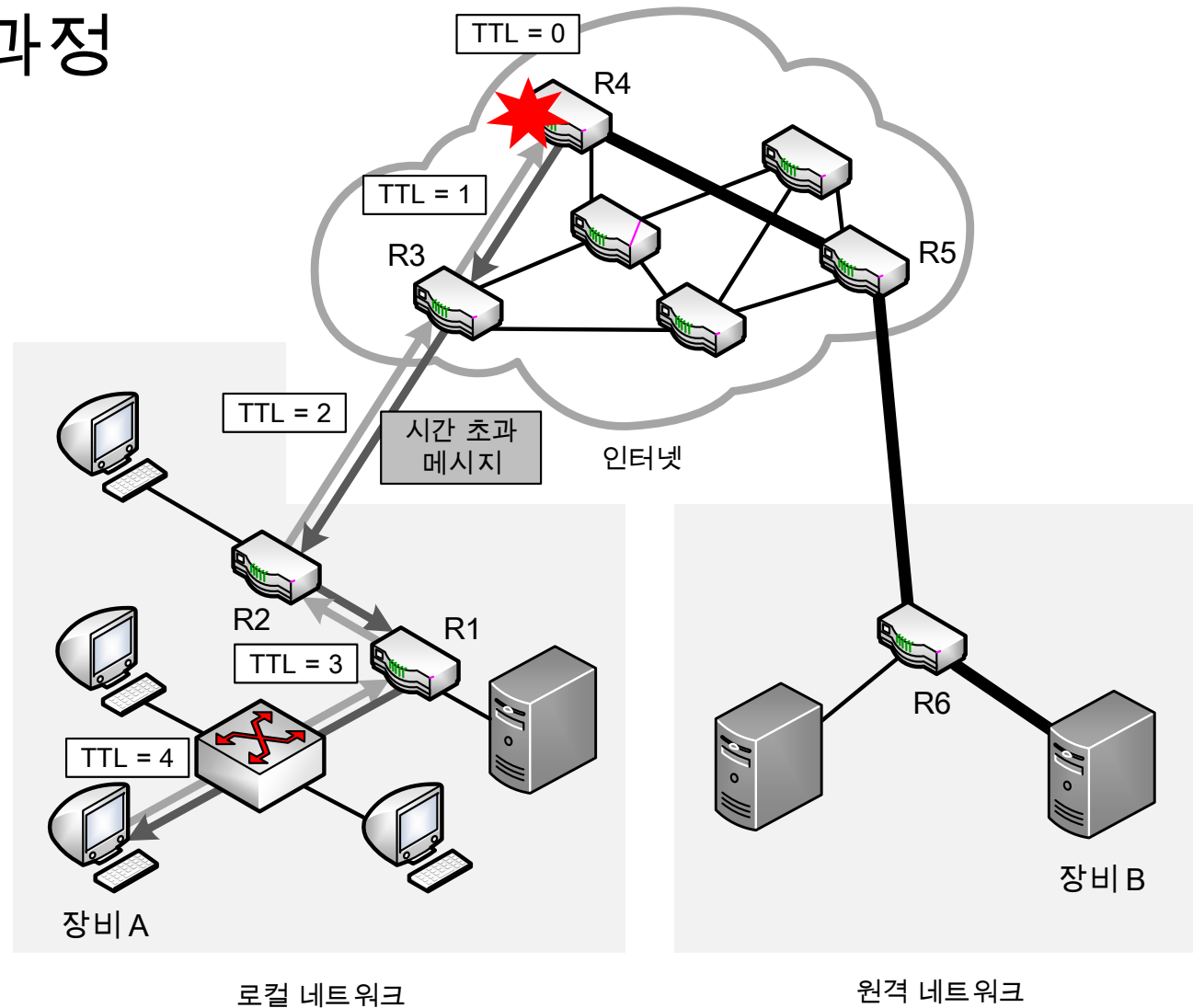
- 수신 측 버퍼 공간이 부족한 경우, 송신 측에게 송신 속도를 낮출 것을 요구하는 메시지

- 버퍼 공간의 부족

- 송신 장비의 처리 속도가 수신 장비보다 빠른 경우
 - 송신 장비의 데이터 전송 속도를 수신 장비의 처리량에 따라 조절해야 함
- 하나의 목적지 장비가 여러 출발지 장비에서 온 데이터그램을 받는 경우
 - e.g., 짧은 시간 동안 많은 검색

ICMPv4 오류 메시지 유형

- ICMPv4 시간 초과 메시지
- TTL 만료 과정



목 차

- 보충
 - ICMPv4 오류 메시지 유형
 - ICMPv4 정보 제공 메시지 유형
- TCP/IP 전송 계층 프로토콜
 - TCP 개요
 - TCP 원리와 일반 동작
 - TCP 기본 동작: 연결 수립, 관리와 종료
 - TCP 세그먼트 포맷과 데이터 송신
 - TCP 신뢰성과 흐름 제어 기능

ICMPv4 정보 제공 메시지 유형

- ICMPv4 타임스탬프 요청과 응답 메시지
 - 문제점
 - 타임스탬프 필드를 사용해도 시간 동기화가 어려움
 - 데이터그램별로 송신하는 데 걸리는 시간이 다름
 - 데이터그램을 수신하는 데 무한한 시간이 걸릴 수 있음
 - 라우터가 데이터그램을 버리기도 함
 - 해결 방안
 - 네트워크 시간 프로토콜(NTP, Network Time Protocol) 사용
 - 네트워크 상 연결된 모든 장비 간 시간 정보를 동기화하기 위한 프로토콜

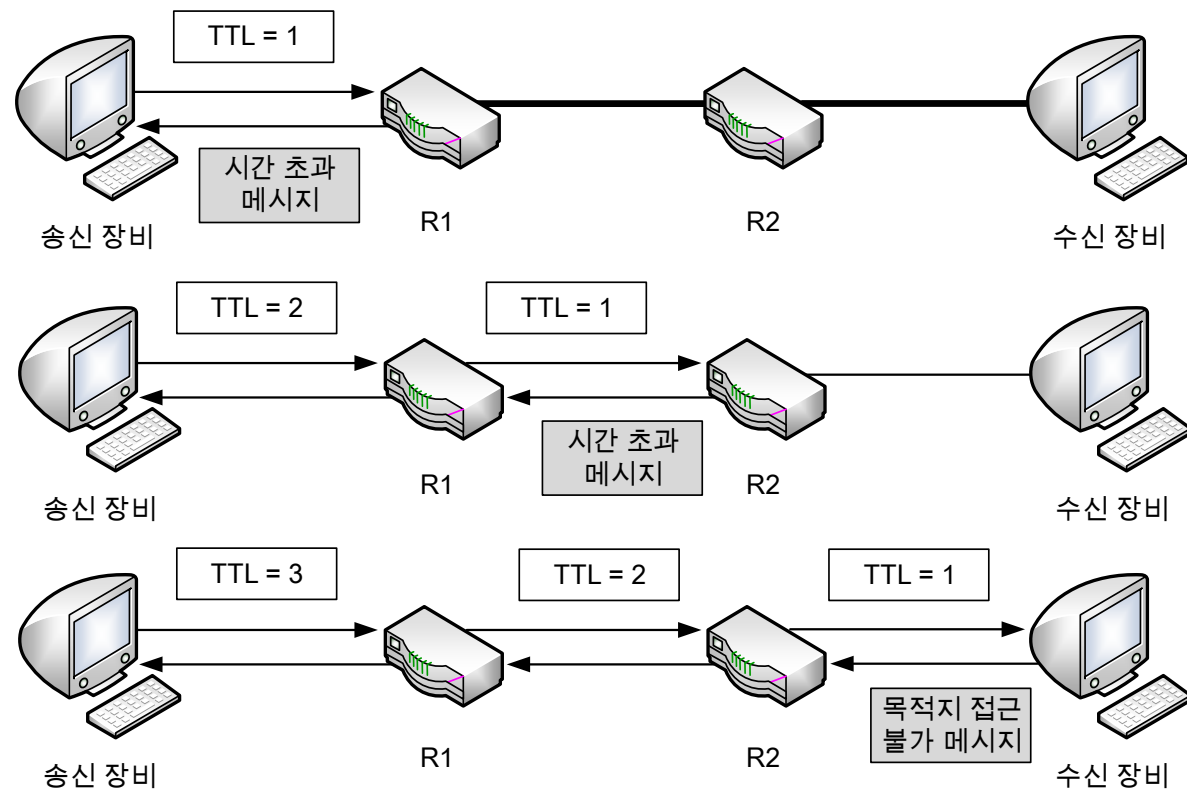
ICMPv4 정보 제공 메시지 유형

- ICMPv4 경로 추적(Traceroute) 메시지

- 정의

- 목적지까지의 라우팅 경로를 추적하기 위해 쓰이는 메시지

- Traceroute 동작 원리



목 차

- 보충
 - ICMPv4 오류 메시지 유형
 - ICMPv4 정보 제공 메시지 유형
- TCP/IP 전송 계층 프로토콜
 - TCP 개요
 - TCP 원리와 일반 동작
 - TCP 기본 동작: 연결 수립, 관리와 종료
 - TCP 세그먼트 포맷과 데이터 송신
 - TCP 신뢰성과 흐름 제어 기능

TCP 개요

- TCP(Transmission Control Protocol)
 - 정의
 - 네트워크의 정보 전달을 통제하는 프로토콜
 - 역사
 - 초기 TCP(Transmission Control Program)
 - 데이터그램 전송, 라우팅, 연결, 신뢰, 데이터 흐름 관리
 - 3계층과 4계층 기능을 함께 사용해야 했음
 - 3계층 기능만 필요한 경우에 문제가 됨
 - 계층화와 모듈화라는 핵심 개념 위반
 - TCP(Transmission Control Protocol)와 IP(Internet Protocol)로 분리하기로 결정

TCP 개요

• TCP 특징

특징	설명
연결형과 양방향	<ul style="list-style-type: none">통신 전 연결 수립과 장비 간 양방향 송·수신
다중 연결과 종단 식별	<ul style="list-style-type: none">연결된 두 장비의 소켓 쌍으로 종단 식별<클라이언트 IP 주소>:<포트 번호>, <서버 IP 주소>:<포트 번호>
신뢰성 보장	<ul style="list-style-type: none">모든 데이터가 목적지에 도달할 수 있도록 함무결성 검사를 통해 필요한 경우 재전송 처리
승인	<ul style="list-style-type: none">수신 여부에 대한 승인 메시지 전송
스트림 기반	<ul style="list-style-type: none">한 번에 한 바이트씩 연속적으로 전송되는 바이트 열데이터의 중복이나 손실 없이 종단 간 데이터 전송 보장

TCP 개요

- TCP가 수행하는 기능 (1/2)
 - 주소 지정과 다중화
 - 포트를 이용한 주소 지정
 - 포트와 주소로 여러 프로세스를 연결하는 다중화
 - e.g., 동일한 IP 주소로 메일 전송(SMTP)과 파일 전송(FTP) 동시에 가능
 - 연결 수립, 유지, 종료
 - 장비의 데이터 이동을 위한 연결 협상
 - 데이터 처리와 전송
 - 애플리케이션에서 데이터를 패키징하여 목적지 장비로 전달
 - 목적지 장비에서 패키징으로 풀어 애플리케이션으로 전달

TCP 개요

- TCP가 수행하는 기능 (2/2)
 - 신뢰성과 전송 품질 서비스
 - 송신된 데이터가 목적지에 도달하지 않거나, 잘못된 순서로 전송되지 않음
 - 흐름 및 혼잡 제어
 - 흐름 제어
 - 송신 측과 수신 측의 데이터 처리 속도 차이를 해결하기 위한 방식
 - 송신 측의 데이터 전송량 제어
 - 혼잡 제어
 - 송신 측의 데이터 전달과 네트워크의 데이터 처리 속도 차이를 해결하기 위한 방식
 - 송신 측의 데이터 전송 속도 제어

TCP 개요

- TCP가 수행하지 않는 기능
 - 애플리케이션 사용 명시
 - TCP는 전송 프로토콜만 정의
 - 애플리케이션 프로토콜로 TCP 사용 방식 명시
 - 보안 제공
 - 데이터의 인증이나 프라이버시를 보장하지 않음
 - 이를 해결하기 위해 IPsec 같은 수단 사용
 - 메시지 경계 유지
 - 스트림 구조이기에 메시지 경계 명시는 애플리케이션 몫
 - 실제 통신 보장
 - 통신을 방해할 경우 TCP는 재전송만 가능

목 차

- 보충
 - ICMPv4 오류 메시지 유형
 - ICMPv4 정보 제공 메시지 유형
- TCP/IP 전송 계층 프로토콜
 - TCP 개요
 - TCP 원리와 일반 동작
 - TCP 기본 동작: 연결 수립, 관리와 종료
 - TCP 세그먼트 포맷과 데이터 송신
 - TCP 신뢰성과 흐름 제어 기능

TCP 원리와 일반 동작

- TCP 포트와 연결

- 포트(Port)

- 장비 내의 여러 프로세스 중 실제로 데이터를 받아야 하는 프로세스 위치를 알려주는 고유한 숫자 번호

- 소켓(Socket)

- 프로세스가 데이터를 주고 받으려면 반드시 열어야 하는 창구 같은 것
 - 프로토콜, IP 주소, 포트 번호로 이루어짐

- TCP 연결은 동시에 맺을 수 있음

- 연결 식별을 위해 두 종단에 해당하는 소켓 쌍 이용
 - <클라이언트 IP 주소>:<포트 번호>, <서버 IP 주소>:<포트 번호>

TCP 원리와 일반 동작

- TCP 데이터 처리: 스트림 동작
 - 애플리케이션으로 송신하는 데이터는 바이트 스트림 처리
 - 애플리케이션에서 수신하는 데이터는 스트림으로 간주
- TCP 데이터 패키징: 세그먼트
 - 수신한 스트림을 IP를 위해 분리한 메시지의 형태
 - 세그먼트 크기 결정 방법
 - 최대 세그먼트 크기(MSS, Maximum Segment Size) 결정
 - 연결 수립 과정 중에 결정
 - 연결이 먼저 수립된 경우, 수신 가능한 데이터 크기로 결정

TCP 원리와 일반 동작

- TCP 데이터 식별: 순서 번호
 - 데이터가 순서대로 목적지에 도달했는지 확인
 - 수신한 세그먼트는 순서 번호를 이용하여 원본 데이터 스트림으로 재조합
 - 손실된 데이터 확인 시 재전송

TCP 원리와 일반 동작

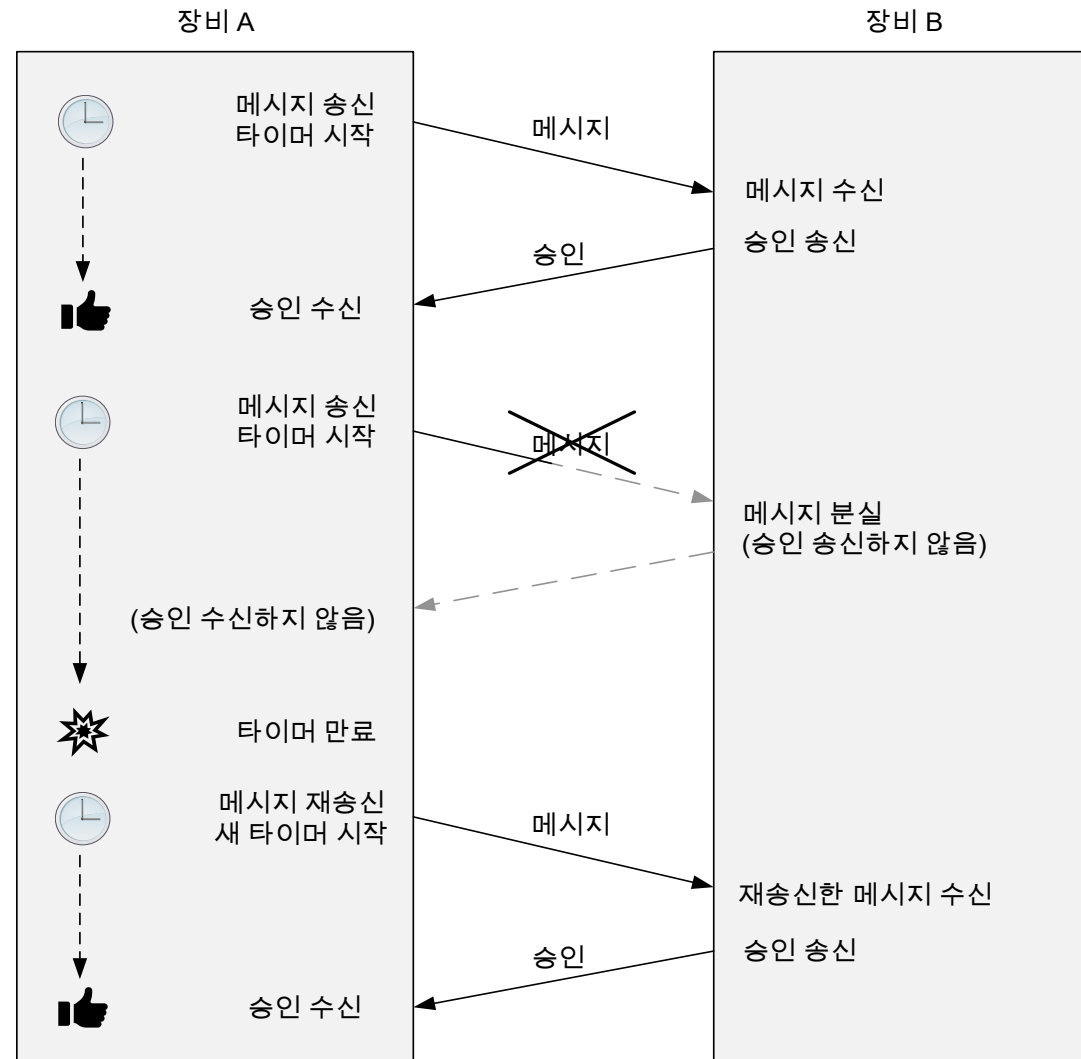
- TCP 슬라이딩 윈도우 승인 체계
 - 두 개의 장비 간 데이터그램 흐름 제어를 위한 방법
 - PAR(Positive Acknowledgment with Retransmission)을 개선하고 수정한 구조
- 사용하는 이유
 - 신뢰성 보장
 - 송신 데이터의 목적지 도달 여부 확인
 - 도달하지 못한 경우 데이터 재전송
 - 긍정 승인(PAR) 사용
 - 데이터 흐름 제어
 - 수신 장비가 처리 가능한 속도로 데이터 송신을 관리
 - 개선된 PAR 사용

TCP 원리와 일반 동작

• TCP 슬라이딩 윈도우 승인 체계

• 긍정 승인(PAR)

- 신뢰성 보장을 위해 사용
- 첫 메시지에 대한 승인을 받기 전까지 다음 메시지 전송 불가



TCP 원리와 일반 동작

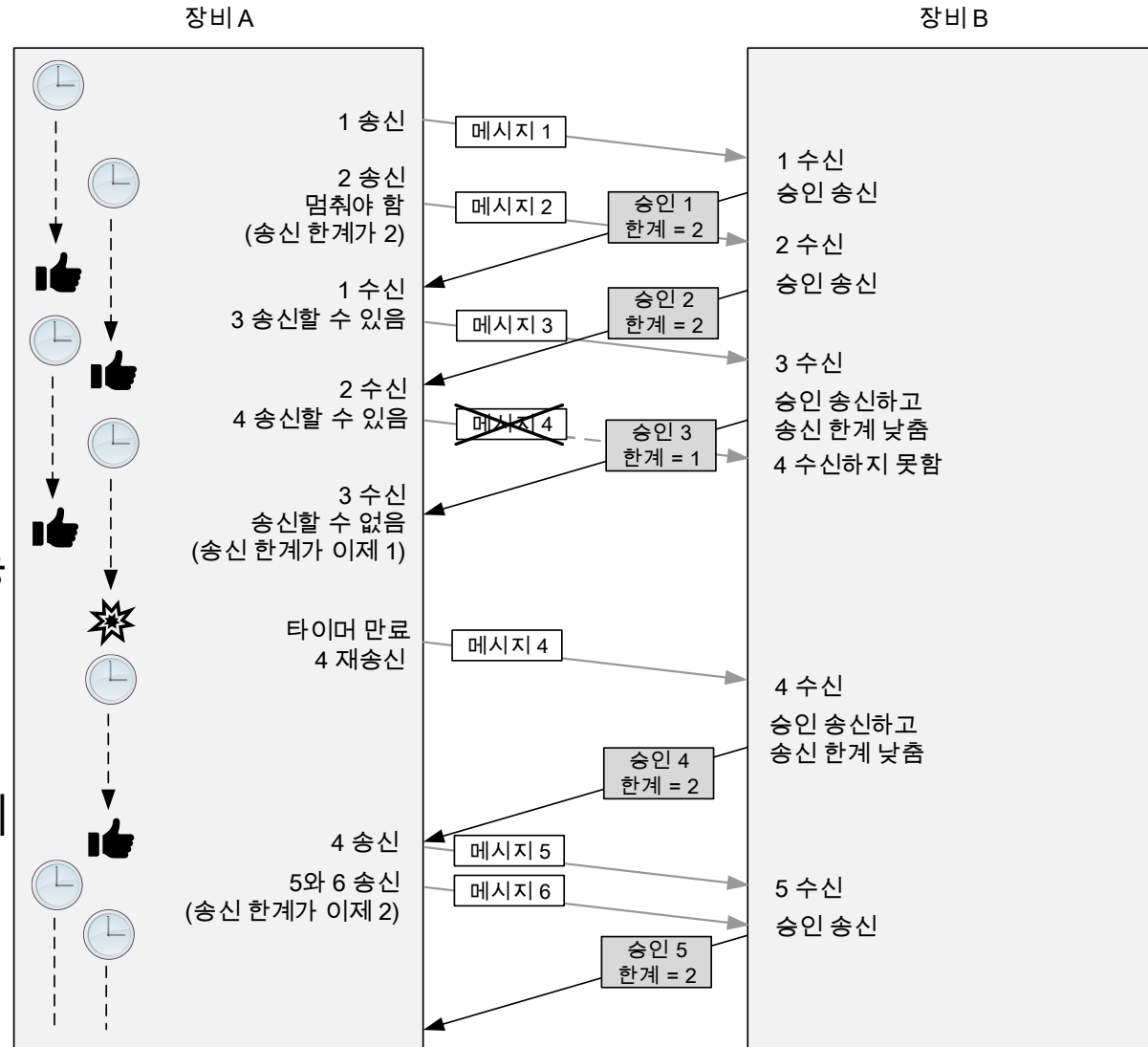
• TCP 슬라이딩 윈도우 승인 체계

• 개선된 PAR

- 송신 장비가 여러 메시지 동시에 송신 가능

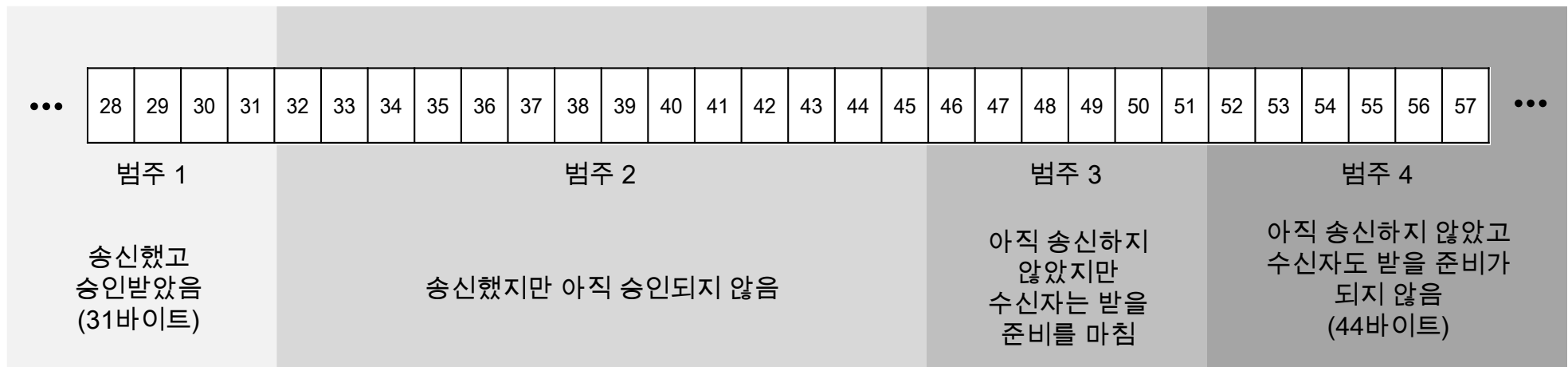
• 개선 사항

- 순서 번호
 - 개별적으로 승인 가능
 - 동시에 여러 메시지 수신 가능
- 송신 제한 필드
 - 수신 가능한 메시지의 최대 수 지정 가능
 - 메시지 송신 속도를 제한함으로써 흐름 제어



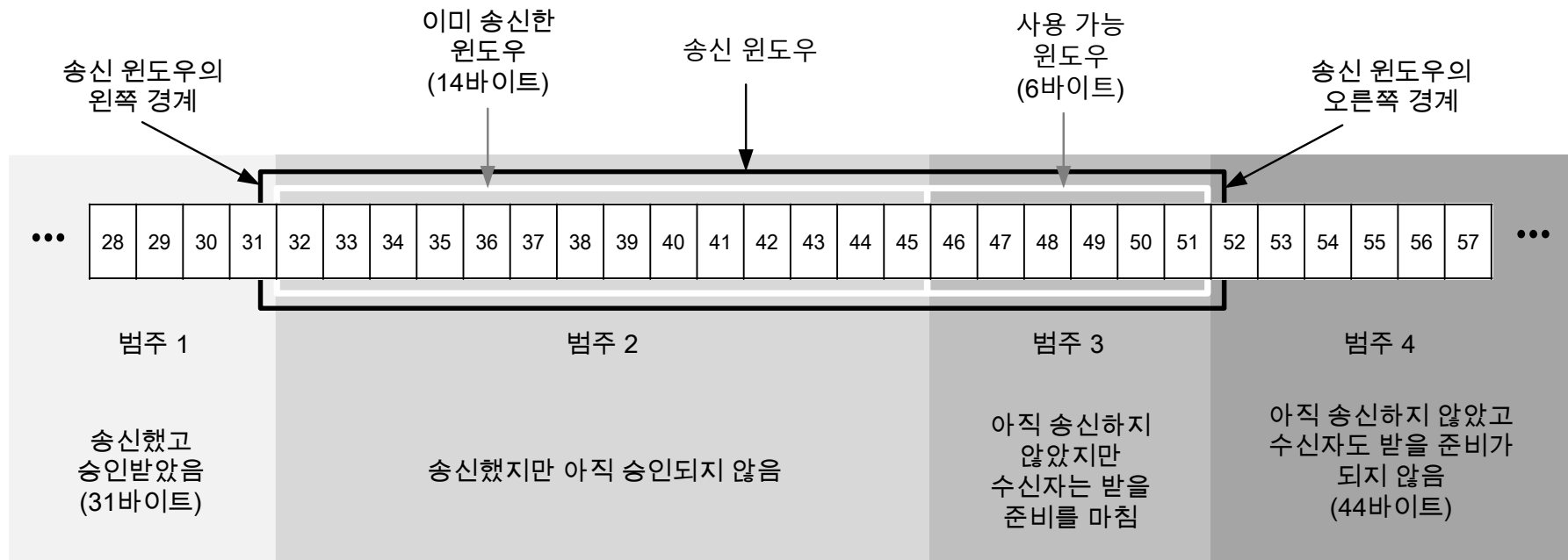
TCP 원리와 일반 동작

- TCP 슬라이딩 윈도우 승인 체계
 - TCP 전송 스트림 바이트 상태
 - 송신했고 승인받은 바이트
 - 송신했지만 승인되지 않은 바이트
 - 송신하지 않았지만 수신자는 받을 준비를 마친 바이트
 - 송신하지 않았고 수신자가 받을 준비도 되지 않은 바이트



TCP 원리와 일반 동작

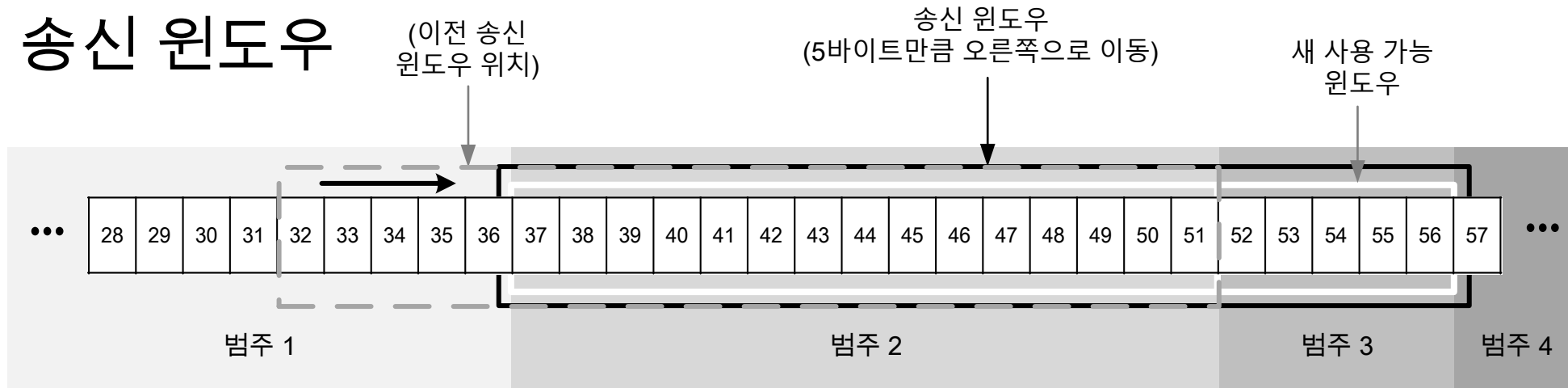
- TCP 슬라이딩 윈도우 승인 체계
 - 윈도우 크기
 - 송신 윈도우(Send Window)
 - 승인을 받기 전에 한 번에 송신 가능한 데이터 수
 - 사용 가능 윈도우(Usable Window)
 - 송신 윈도우에서 데이터 송신에 추가 사용이 가능한 남은 데이터 수



TCP 원리와 일반 동작

- TCP 슬라이딩 윈도우 승인 체계

- 송신 윈도우



- 빠진 승인 처리

- 세그먼트 각각에 대한 승인을 보내지 않음
 - 수신 장비의 실제 수신 세그먼트도 재전송해야 함
- 전송 완료 시간 할당 및 재전송 기능

목 차

- 보충
 - ICMPv4 오류 메시지 유형
 - ICMPv4 정보 제공 메시지 유형
- TCP/IP 전송 계층 프로토콜
 - TCP 개요
 - TCP 원리와 일반 동작
 - TCP 기본 동작: 연결 수립, 관리와 종료
 - TCP 세그먼트 포맷과 데이터 송신
 - TCP 신뢰성과 흐름 제어 기능

TCP 기본 동작

- TCP 동작 방식: 유한 상태 머신(FSM, Finite State Machine)
- 특징
 - 연결 수립, 관리, 종료 과정을 표현
 - 주로 한 장비가 연결 수립이나 종료를 시작, 다른 장비가 응답
- 기본 FSM 개념

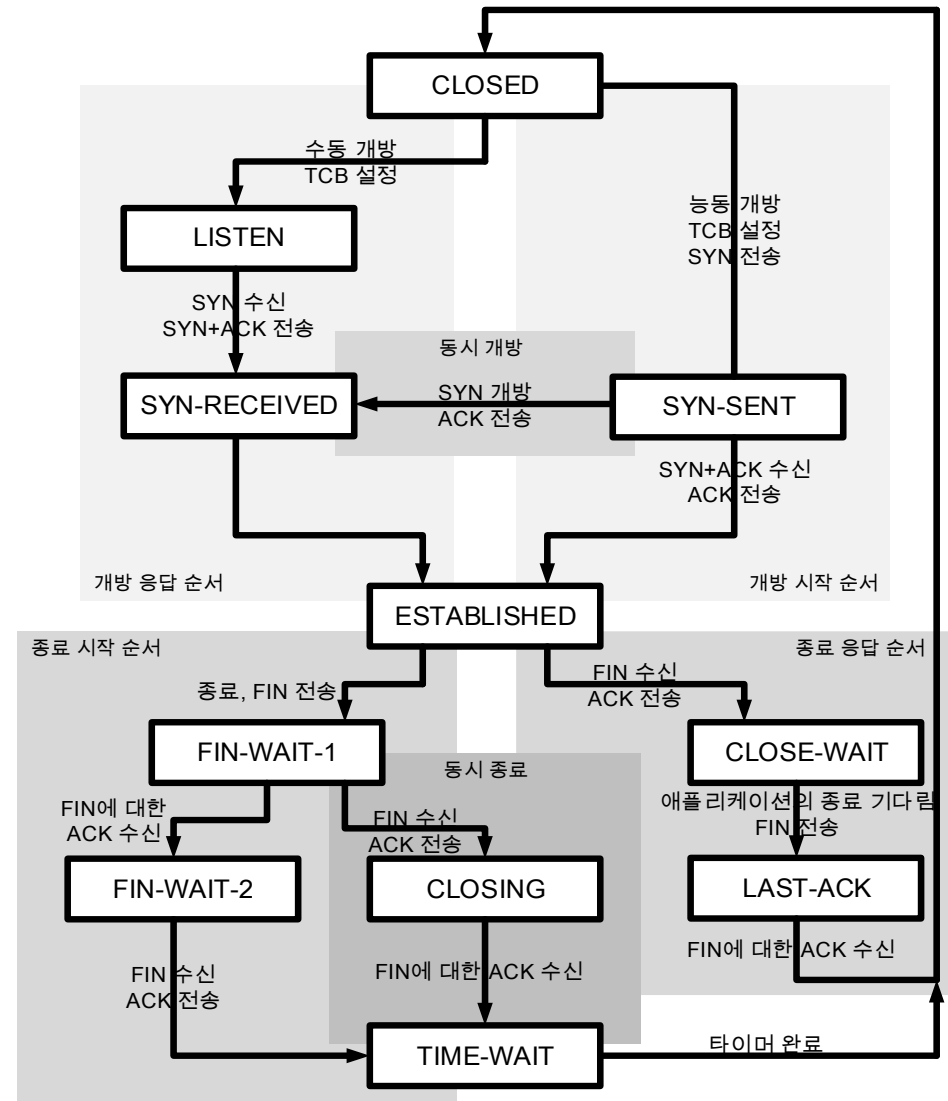
기본 FSM 개념	설명
상태	특정 시간에 프로토콜 소프트웨어가 처한 상황
전이	한 상태에서 다른 상태로 움직이는 행위
이벤트	상태 간 전이를 하게 만든 어떤 일
행동	장비가 이벤트에 대한 반응으로 다른 상태로 전이하기 전에 하는 일

TCP 기본 동작

- TCP 동작 방식: 유한 상태 머신(FSM, Finite State Machine)

- FSM 주요 메시지

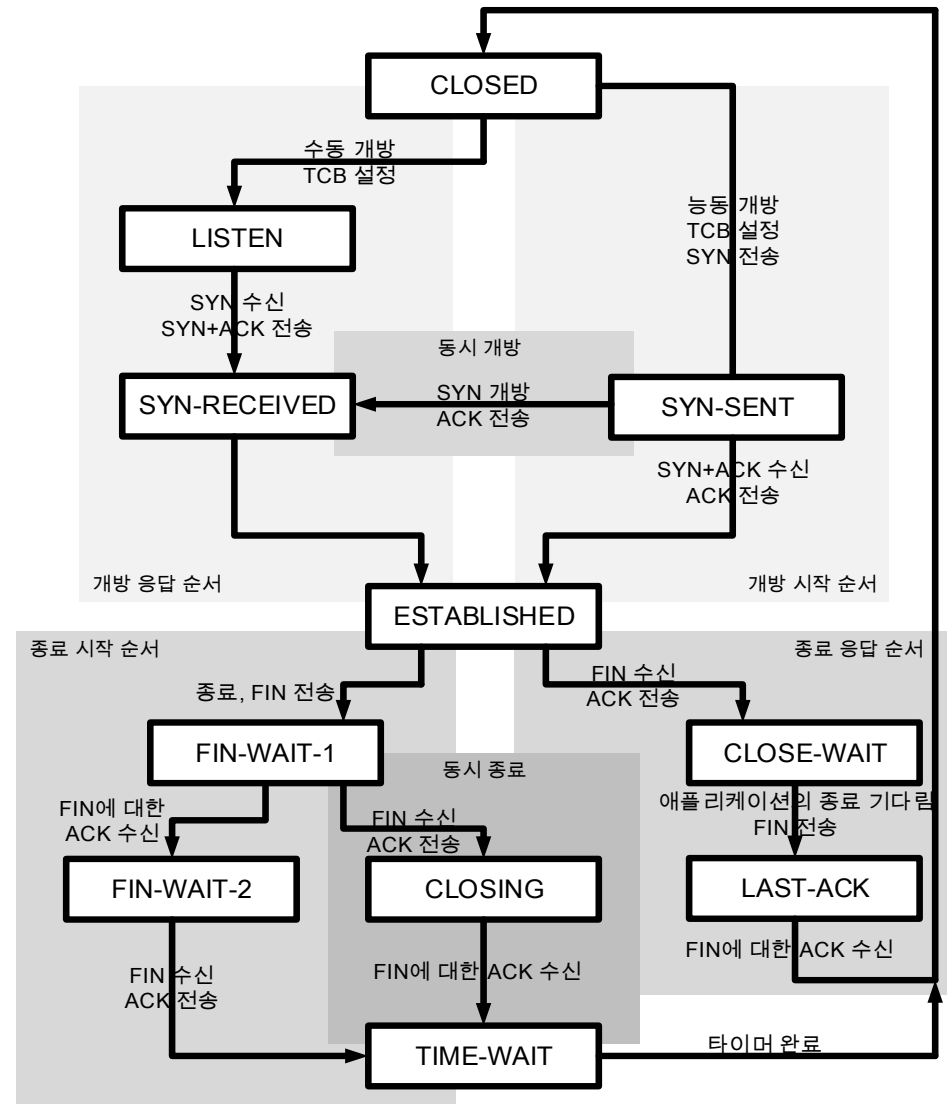
- SYN(Synchronize)
 - 동기화 메시지
 - 연결 초기화 및 수립
- FIN(Finish)
 - 종료 메시지
 - 연결 종료하고 싶은 상태임을 알림
- ACK(Acknowledgment)
 - 승인 메시지
 - SYN이나 FIN과 동일한 메시지 받음을 알림



TCP 기본 동작

- TCP 동작 방식: 유한 상태 머신(FSM, Finite State Machine)

상태	설명
CLOSED	연결 없음 상태
LISTEN	SYN을 기다리는 상태
SYN-SENT	자신의 SYN 송신 및 상대의 응답 SYN을 기다리는 상태
SYN-RECEIVED	자신의 SYN 송신 후 ACK 대기 상태
ESTABLISHED	연결 수립 상태
CLOSE-WAIT	종료 요청(FIN) 받은 상태
LAST-ACK	종료 요청 승인 후, 자신의 FIN 송신
FIN-WAIT-1	자신의 종료 요청 승인을 기다리거나 상대의 연결 종료 요청을 기다리는 상태
FIN-WAIT-2	ACK를 수신하고, 상대 장비에서 FIN 오기를 기다림
CLOSING	상대의 FIN을 받아 ACK를 보냈지만, 자신의 FIN에 대한 ACK를 받지 못한 상태
TIME-WAIT	FIN을 받아 ACK 보냈고, 자신의 FIN에 대한 ACK도 받은 상태



TCP 기본 동작

- TCP 연결 준비
 - 전송 제어 블록(TCB, Transmission Control Block)
 - 연결을 식별하기 위한 데이터 구조
 - 연결 정보 저장
 - 연결 식별을 위한 두 소켓 번호
 - 송·수신 데이터를 가진 버퍼를 가리키는 포인터
 - 승인하거나 승인하지 않은 바이트 수, 현재 윈도우 크기 등을 추적하는 변수
- 클라이언트와 서버의 개방 동작
 - 능동 개방
 - 클라이언트는 서버에게 SYN 메시지를 보내 연결 시작
 - 수동 개방
 - 서버는 클라이언트의 연결 요청을 받아들일 준비 동작

TCP 기본 동작

- TCP 연결 수립

- 두 장비가 메시지를 교환하여 초기 접속 상태(CLOSED)에서 정상 동작 상태(ESTABLISHED)로 전이함

- 연결 수립 기능

- 접촉과 통신

- 클라이언트와 서버는 서로 접촉하여 메시지 전송 후 통신 시작
 - 접촉과 통신 과정을 위한 제어 메시지
 - 연결 초기화에 사용하는 세그먼트임을 알리는 SYN 메시지
 - 세그먼트 전송 장비에게 메시지를 잘 수신했다고 알리는 ACK 메시지

- 순서 번호 동기화 (1/2)

- 순서 번호는 전송하는 데이터의 순서
 - 승인 번호는 다음에 전송해야 하는 데이터의 시작 위치
 - 상대 장비가 보낸 순서 번호 + 1(수신한 데이터 바이트)

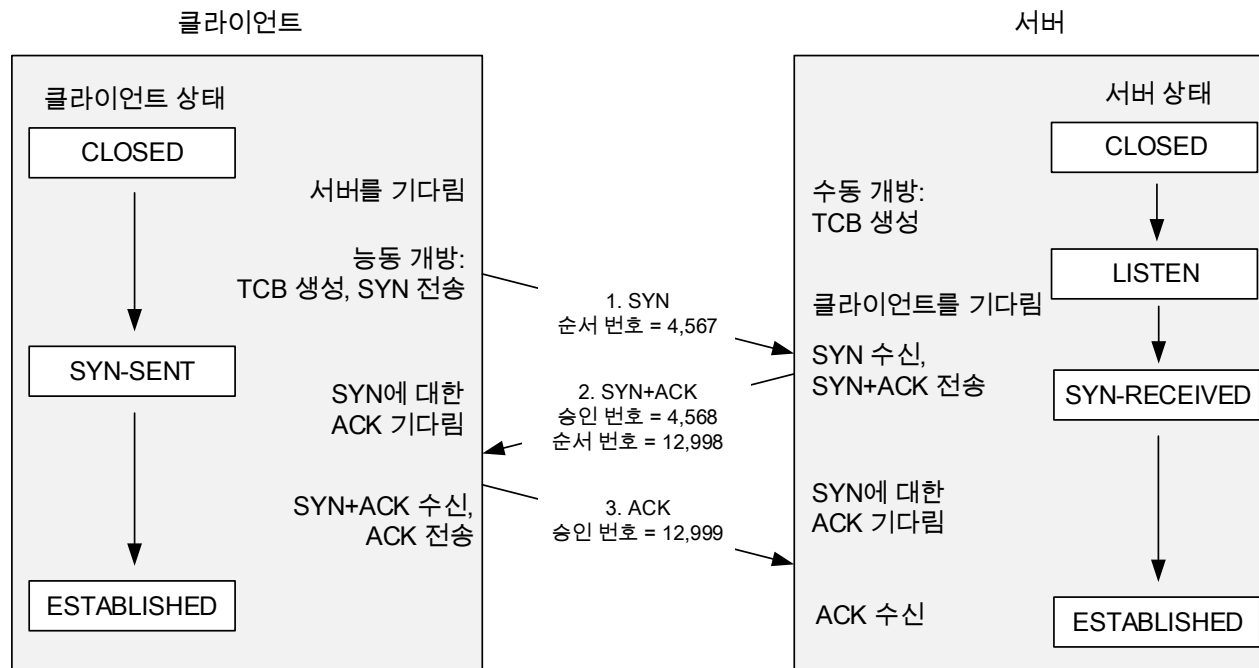
TCP 기본 동작

- TCP 연결 수립

- 연결 수립 기능

- 순서 번호 동기화 (2/2)

1. 클라이언트의 연결 요청
2. 서버의 승인과 연결 요청
3. 클라이언트의 승인



TCP 기본 동작

- TCP 연결 수립
 - 연결 수립 기능
 - 인자 교환
 - 윈도우 크기
 - 16비트인 TCP 윈도우 크기보다 더 큰 값 사용 가능
 - 선택적 승인 허용
 - 잃어버린 세그먼트만을 재전송할 수 있도록 사용 가능
 - 대체 체크섬 방식
 - 표준 TCP 체크섬이 아닌 체크섬 방법 사용 가능

TCP 기본 동작

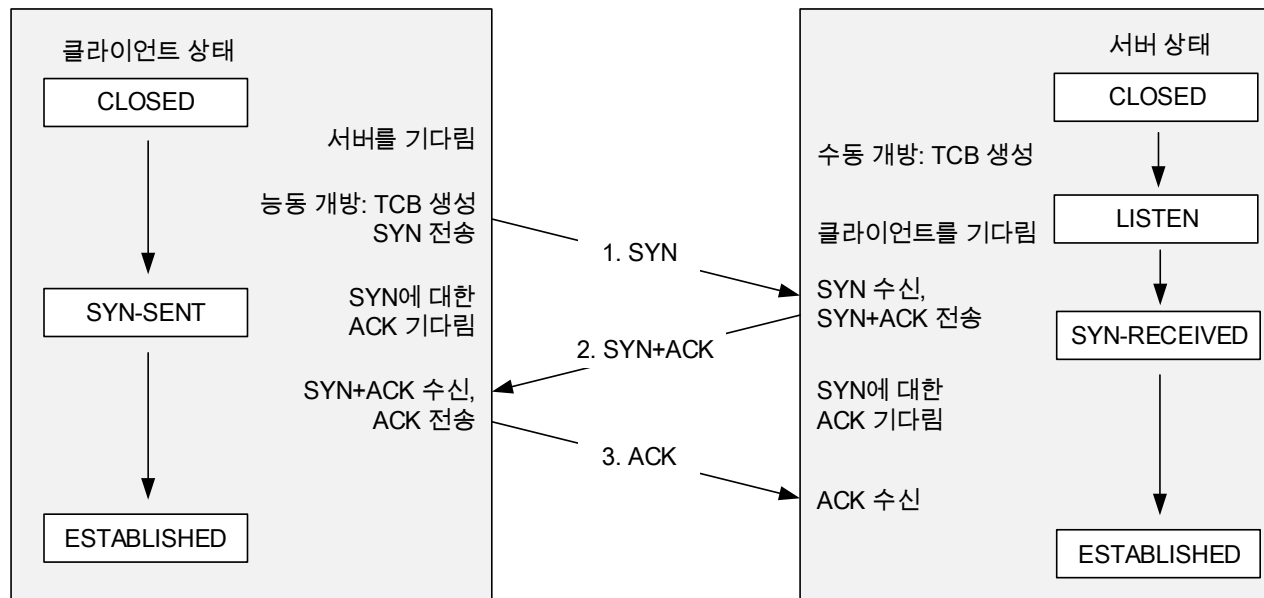
- TCP 연결 수립

- 연결 수립 방법

- 쓰리 웨이 핸드셰이크(Three-way Hand-shake)

- 한 장비가 닫힌 상태에서 연결하는 메시지 교환 과정

1. 클라이언트가 SYN 전송
2. 서버는 1에 대한 ACK와 자신의 SYN를 합쳐서 전송
3. 클라이언트는 서버의 SYN에 대한 ACK 전송



TCP 기본 동작

- TCP 연결 수립

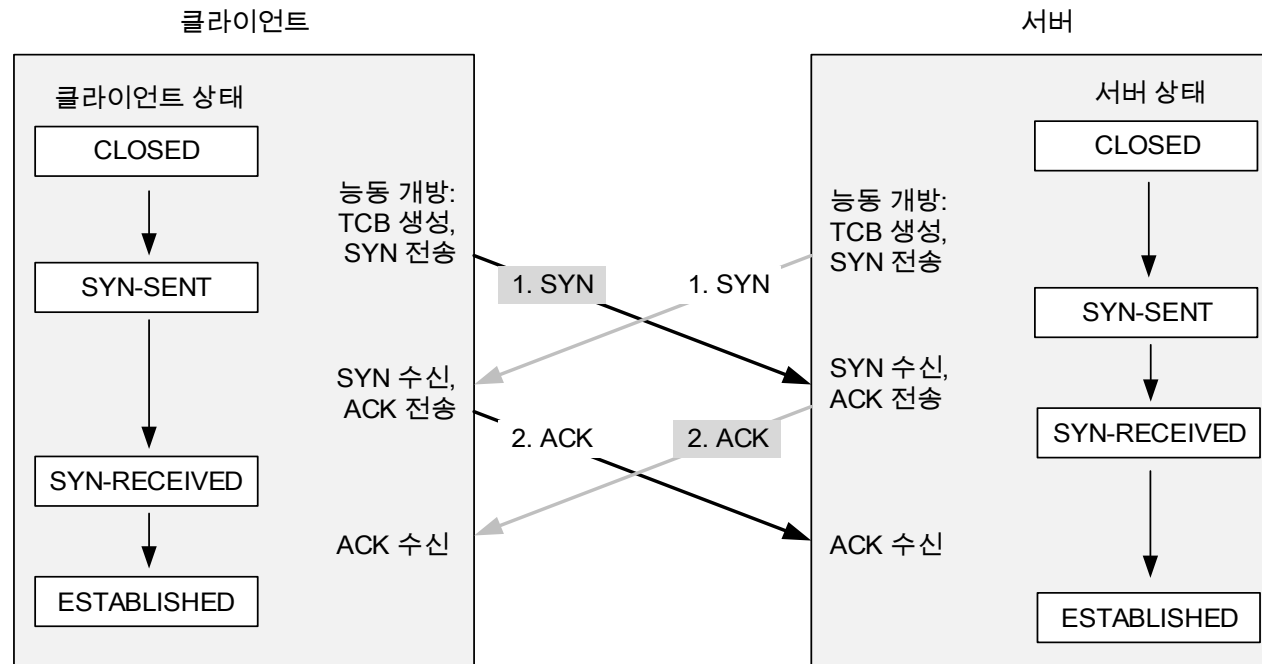
- 연결 수립 방법

- 동시 개방

- 두 장비가 상대 장비로 동시에 연결하는 메시지 교환 과정

- 쓰리 웨이 핸드셰이크 방식과의 차이

- 동시 개방은 SYN을 받고 ACK를 보내고, 쓰리웨이는 SYN와 ACK를 함께 보냄



TCP 기본 동작

- TCP 연결 관리 문제
 - TCP 연결 중 발생 가능한 문제
 - 반 개방 연결(Half-open Connection)
 - 한 장비는 ESTABLISHED 상태, 다른 장비는 CLOSED 상태
 - 상대 장비에게 알리지 않은 채 연결을 닫거나 중지하는 경우
- TCP 초기화
 - 세그먼트 헤더의 RST 플래그를 1로 설정하여 전달
 - 연결을 초기화하는 상황
 - 세그먼트를 보낸 장비와 연결을 맺고 있지 않는 경우
 - 부정확한 순서/승인 번호를 가지는 메시지를 수신한 경우
 - 연결을 기다리는 프로세스가 없는 포트로 SYN 메시지를 수신한 경우

TCP 기본 동작

- TCP 연결 관리 문제
 - TCP 초기화 세그먼트 처리
 - SYN 메시지가 유효한지 검사하는 것
 - e.g., 순서 번호 필드
- TCP 초기화 세그먼트 처리 방식
 - 장비가 LISTEN 상태인 경우
 - 초기화 메시지를 무시하고 그 상태에 남아있음
 - 장비가 SYN-RECEIVED 상태 이전에 LISTEN 상태에 있던 경우
 - LISTEN 상태로 돌아감
 - 이외의 경우
 - 장비는 연결을 종료하고 CLOSED 상태로 돌아감
 - 연결이 끊겼음을 의미

TCP 기본 동작

- TCP 연결 관리 문제
 - 킵알라이브(Keep-alive) 메시지
 - 유틸(Idly) 연결을 처리하는 메시지
 - 연결이 오랜 기간 동안 정지 상태에 있는 것
 - 다른 장비에게 연결이 수립된 상태임을 알려줌
 - 연결이 유효한 경우, 상대 장비는 승인을 포함하는 세그먼트 전송
 - 연결이 유효하지 않은 경우, 상대 장비는 초기화 세그먼트 전송

TCP 기본 동작

- TCP 연결 종료

- 두 장비 모두 데이터를 보내지 않는다는 의미

- TIME-WAIT 상태 필요한 이유

- 상대 장비가 ACK을 받았다는 것을 확신하기 위함

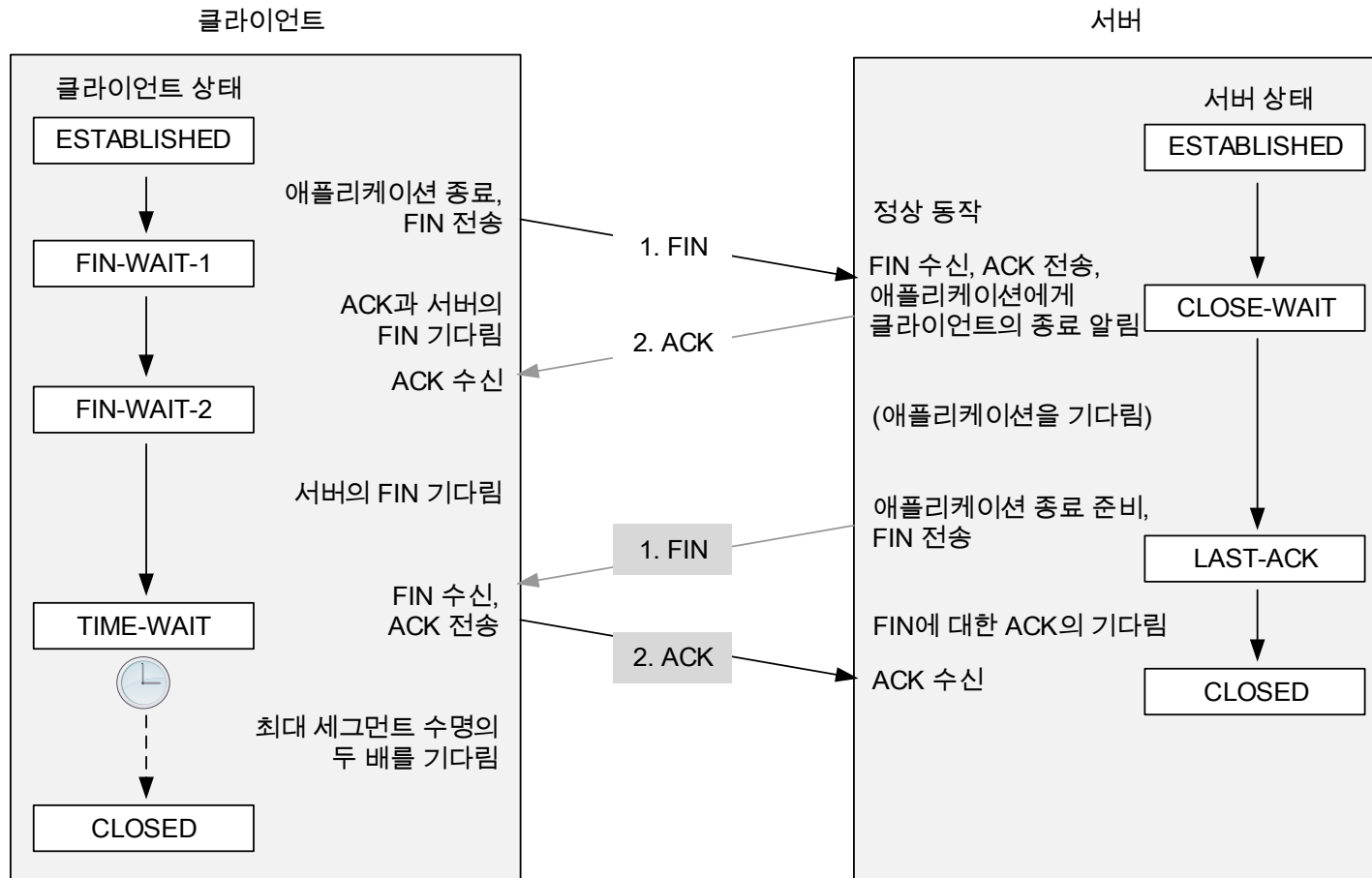
- 일반적인 동작 과정에서 ACK가 사라진 경우, ACK 재전송

- 한 연결과 다른 연결 사이에 일정 시간이 필요함

- 동시 연결 종료 과정에서 다른 연결에서 온 세그먼트와 섞여 혼란을 일으킬 수 있음

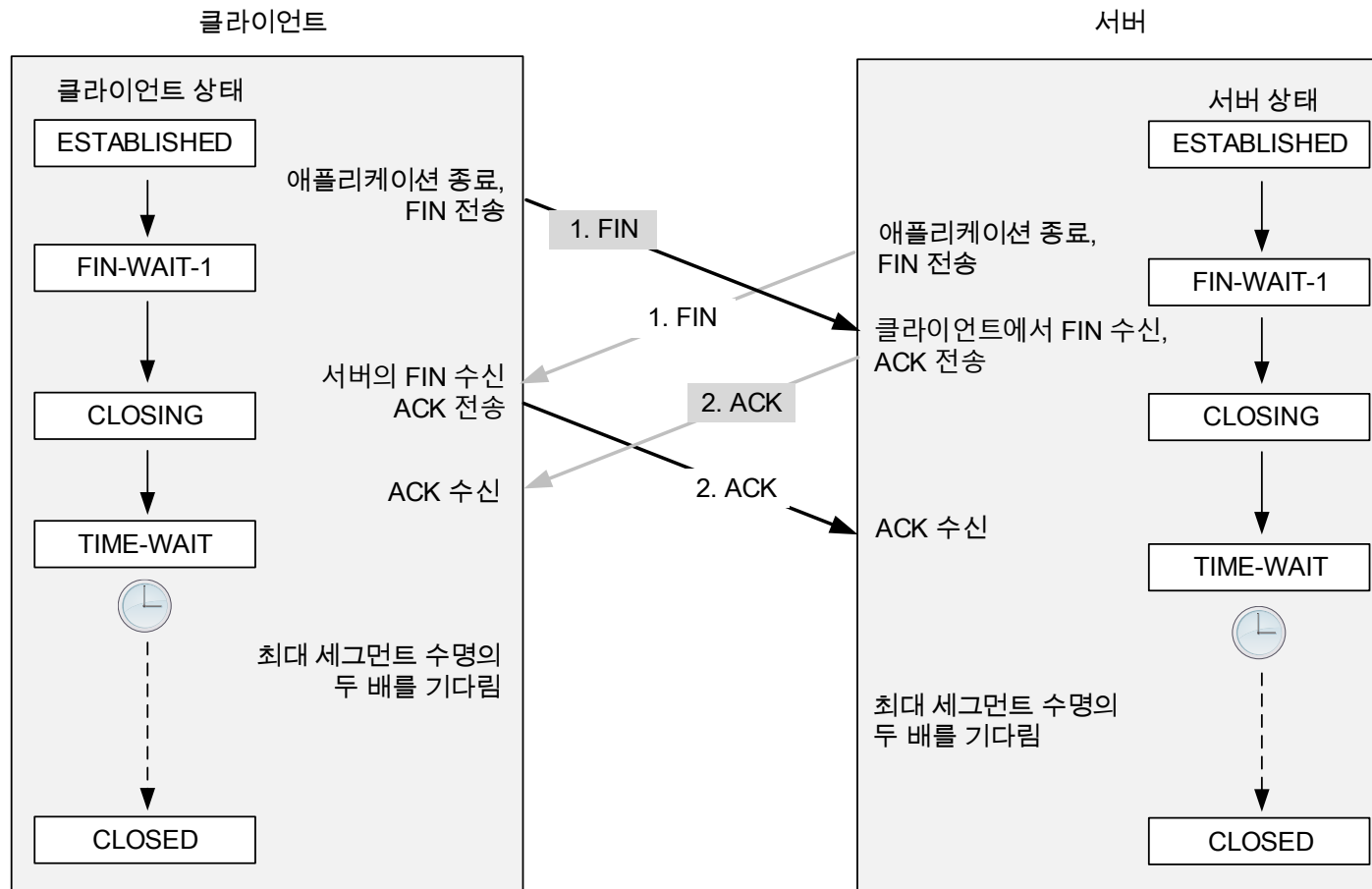
TCP 기본 동작

- TCP 연결 종료
 - 연결 종료 방법
 - 일반적인 과정



TCP 기본 동작

- TCP 연결 종료
 - 연결 종료 방법
 - 동시 종료 과정



목 차

- 보충
 - ICMPv4 오류 메시지 유형
 - ICMPv4 정보 제공 메시지 유형
- TCP/IP 전송 계층 프로토콜
 - TCP 개요
 - TCP 원리와 일반 동작
 - TCP 기본 동작: 연결 수립, 관리와 종료
 - TCP 세그먼트 포맷과 데이터 송신
 - TCP 신뢰성과 흐름 제어 기능

TCP 세그먼트 포맷과 데이터 송신

- TCP 세그먼트 포맷

- 목적

- 프로세스 주소 지정

- 출발지와 목적지 장비에 있는 프로세스를 포트 번호로 식별

- 슬라이딩 윈도우 시스템 구현

- 순서/승인 번호, 윈도우 크기 필드로 구현

- 제어 비트와 필드 설정

- 제어 기능 구현을 위한 비트와, 포인터나 데이터를 저장하는 필드

- 데이터 송신

- 데이터 필드에 실제로 송신되는 바이트 단위의 데이터 포함

- 다양한 기능 구현

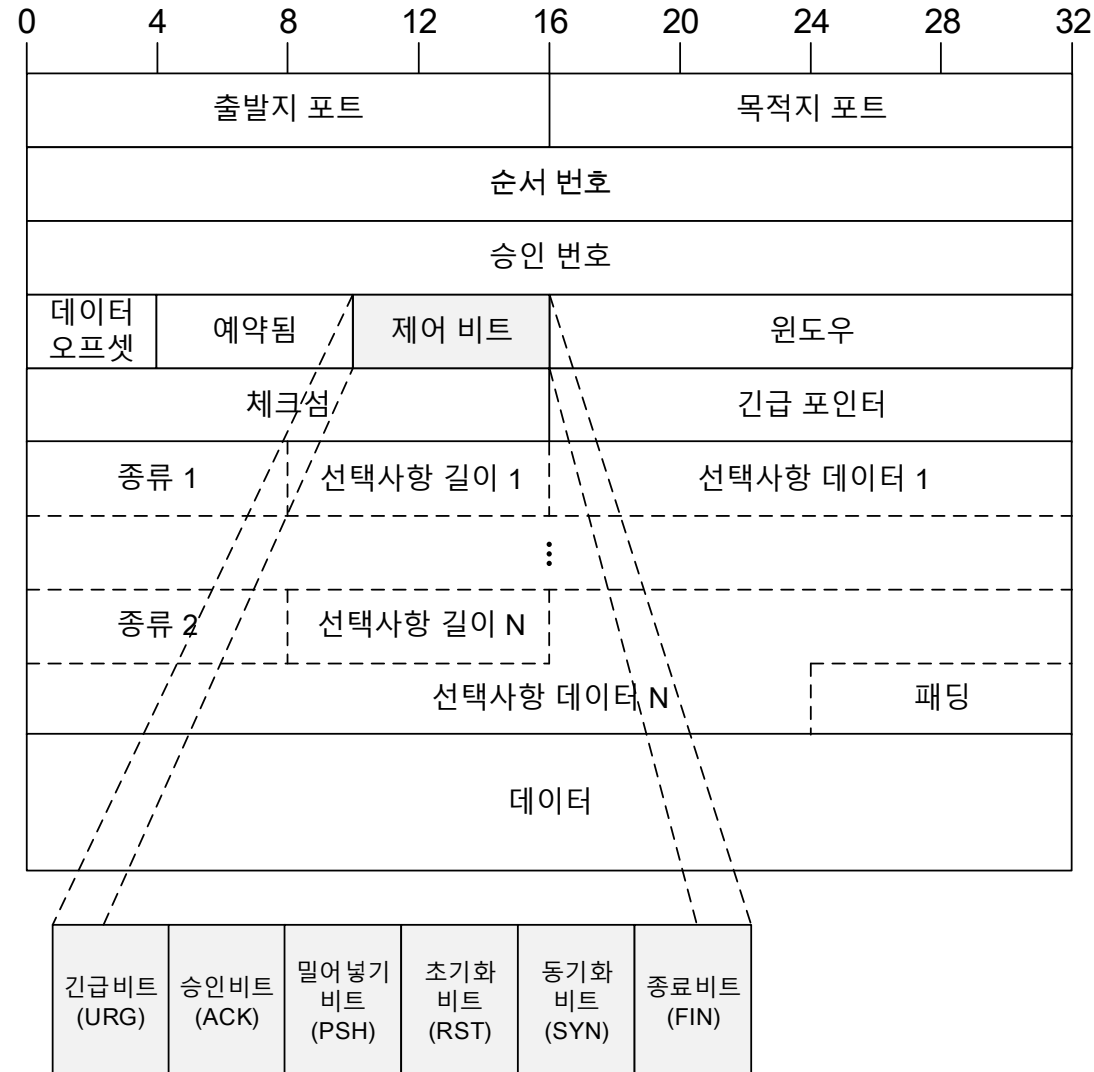
- 데이터 보호를 위한 체크섬과 연결 수립을 위한 선택 사항

TCP 세그먼트 포맷과 데이터 송신

• TCP 세그먼트 포맷

필드명	설명
윈도우	한 번에 수신 가능한 바이트 수
체크섬	데이터 무결성 보호
긴급 포인터	긴급 데이터의 마지막 바이트 순서 번호
선택사항	최대 세그먼트 크기 값, 윈도우 크기, 대체 체크섬
패딩	선택사항 필드가 32비트의 배수가 되도록 0으로 채움

제어 비트명	설명
URG	우선 순위 높은 데이터 위치 알림
ACK	승인 번호(다음 순서 번호) 포함
PSH	송신 장비의 밀어넣기 기능
RST	연결 초기화해야 함
SYN	순서 번호 동기화 및 연결 수립 요청
FIN	송신 장비의 연결 종료 요청



TCP 세그먼트 포맷과 데이터 송신

- TCP 세그먼트 포맷

- TCP 가상 헤더(Pseudo Header)

- 체크섬 계산을 위해 생성되는 필드

- 송신 중 오류 발생에 대처하기 위한 보호 방식

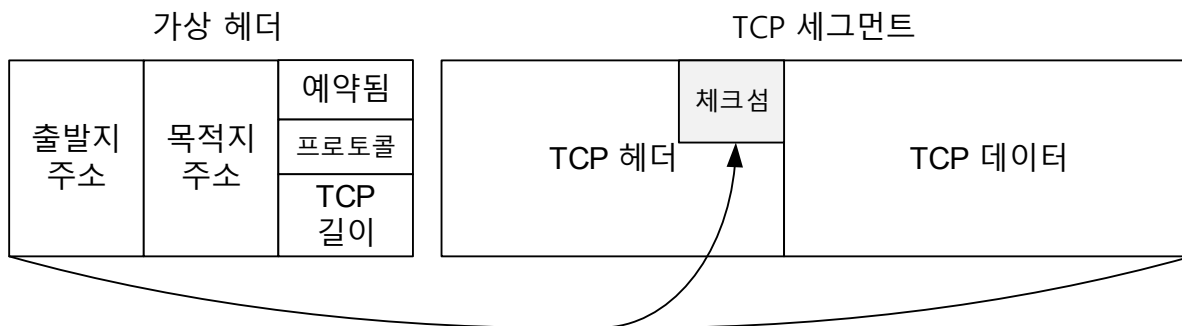
- 송신자는 데이터 바이트의 합을 데이터 스트림과 함께 송신

- 수신자는 데이터 바이트의 합을 검사하여 오류 발생 여부 확인

- 포맷



- 체크섬 계산 과정



TCP 세그먼트 포맷과 데이터 송신

- TCP 세그먼트 포맷
 - TCP 가상 헤더(Pseudo Header)
 - 가상 헤더 사용 장점
 - 잘못된 세그먼트 송신 문제 방지
 - 명시한 주소와 실제로 송수신한 주소가 다른 경우, 체크섬 불일치
 - 잘못된 프로토콜 문제 방지
 - 명시된 프로토콜이 아닌 프로토콜로 송신된 경우, 체크섬 불일치
 - 잘못된 세그먼트 길이 문제 방지
 - 세그먼트 일부가 유실된 경우, 출발지와 목적지가 사용하는 길이 값 불일치

TCP 세그먼트 포맷과 데이터 송신

- TCP 세그먼트 포맷
 - TCP 최대 세그먼트 크기(MSS, Maximum Segment Size)
 - 정의
 - 세그먼트의 데이터 필드에서 사용 가능한 최대 바이트 수
 - MSS 선택 시 고려 사항
 - 과부하 관리
 - TCP 헤더는 20바이트, IP 헤더는 20바이트 이상 사용
 - MSS가 너무 작은 경우, 대역폭을 비효율적으로 사용하게 됨
 - e.g., MSS가 40바이트인 경우
 - IP 데이터그램 단편화
 - 최대 송신 단위(MTU, Maximum Transmission Unit) 이상 송신 불가능

TCP 세그먼트 포맷과 데이터 송신

- TCP 세그먼트 포맷
 - TCP 최대 세그먼트 크기(MSS)
 - 기본 MSS
 - 보통 세그먼트에서 단편화 없이 송신될 수 있는 최대 크기로 결정
 - TCP에서 사용하는 표준 MSS는 536바이트
 - IP 네트워크의 최소 MTU는 576바이트에서 시작
 - TCP와 IP 헤더로 40바이트를 사용
 - MSS 값 명시
 - 표준 MSS보다 크거나 작은 MSS를 사용하는 경우에 MSS 값 명시
 - SYN 메시지의 최대 세그먼트 크기 필드 이용
 - e.g., IPsec을 사용하는 경우, AH 헤더나 ESP 헤더 추가로 인해 헤더 크기가 커지기 때문에 더 작은 MSS 사용

TCP 세그먼트 포맷과 데이터 송신

- TCP 데이터 송신 방식: 슬라이딩 윈도우

- 전송 카테고리

카테고리	설명
전송 카테고리 1	전송했고 승인 받음
전송 카테고리 2	전송했지만 아직 승인 받지 못함
전송 카테고리 3	수신자는 준비됐지만 아직 전송하지 못함
전송 카테고리 4	수신자가 준비되지 않았고 전송하지도 못함

- 수신 카테고리

- 송신자는 승인을 기다려야 하지만 수신자는 받은 것에 대한 승인을 할 필요가 없음

카테고리	설명
수신 카테고리 1+2	수신했고 승인 받음
수신 카테고리 3	수신자는 준비됐지만 아직 수신하지 못함
수신 카테고리 4	수신자가 준비되지 않았고 수신하지도 못함

TCP 세그먼트 포맷과 데이터 송신

- TCP 데이터 송신 방식: 슬라이딩 윈도우
 - 송신(SND) 포인터
 - 송신 비확인(SND.UNA)
 - 송신했지만 아직 승인되지 않은 첫 번째 데이터 순서 번호
 - 전송 카테고리 2의 첫 번째 바이트를 가리킴
 - 이전 순서 번호는 모두 전송 카테고리 1
 - 송신 다음(SND.NXT)
 - 상대 장비에게 송신할 다음 바이트의 순서 번호
 - 전송 카테고리 3의 첫 번째 바이트를 가리킴
 - 송신 윈도우(SND.WND)
 - 송신 윈도우의 크기이자 승인 없이 보낼 수 있는 총 바이트 수
 - 송신 비확인(SND.UNA)와 더하면, 전송 카테고리 4의 첫 번째 바이트 표시 가능

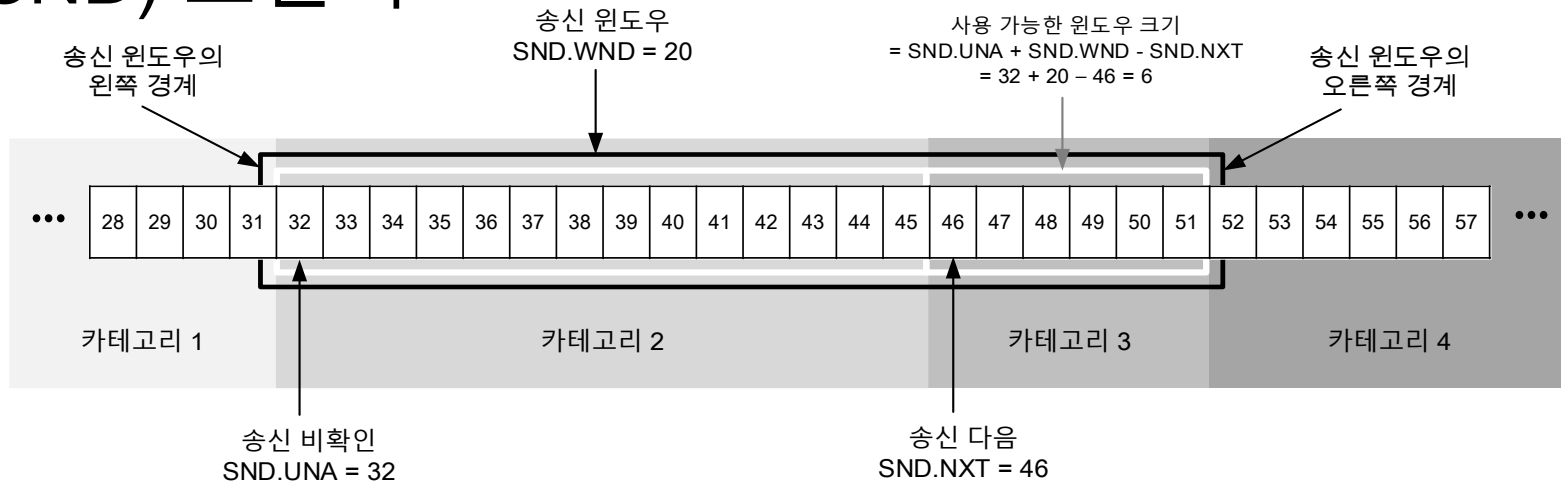
TCP 세그먼트 포맷과 데이터 송신

- TCP 데이터 송신 방식: 슬라이딩 윈도우
 - 수신(RCV) 포인터
 - 수신 다음(RCV.NXT)
 - 상대 장비에서 수신하려는 데이터의 다음 바이트 순서 번호
 - 수신 카테고리 3의 첫 번째 바이트를 가리킴
 - 수신 카테고리 1+2는 이미 수신과 승인이 된 상태임
 - 수신 윈도우(RCV.WND)
 - 수신 윈도우의 크기이자 장비가 한 번에 받길 원하는 바이트 수
 - RCV.NXT와 더하면, 수신 카테고리 4의 첫 번째 바이트 표시 가능

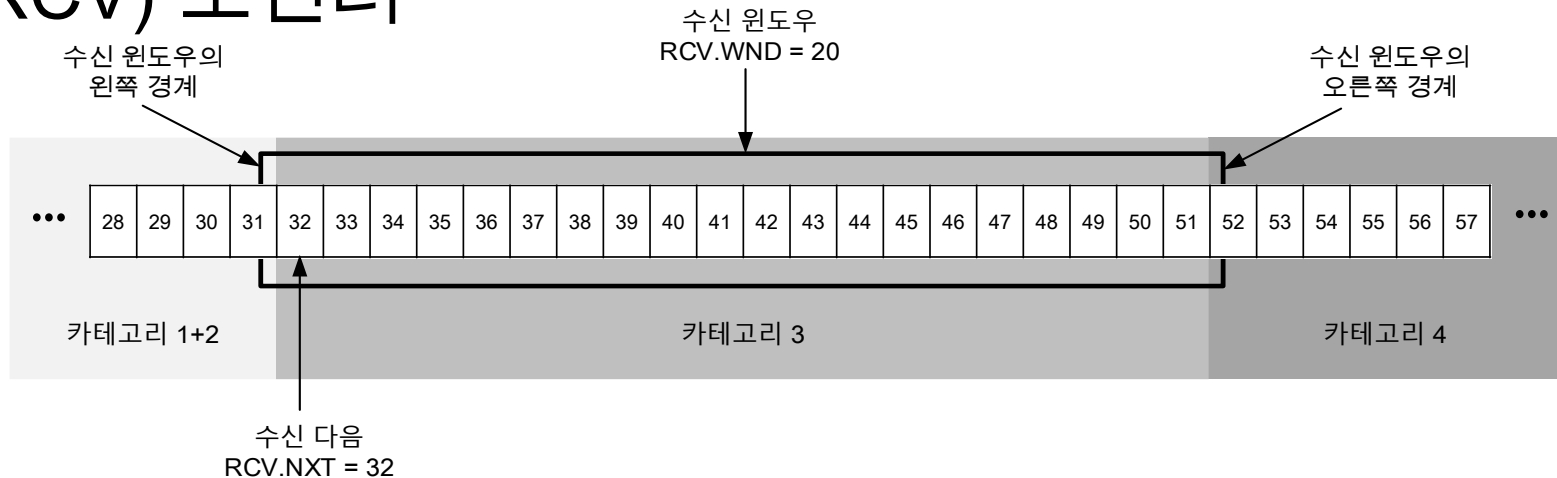
TCP 세그먼트 포맷과 데이터 송신

- TCP 데이터 송신 방식: 슬라이딩 윈도우

- 송신(SND) 포인터

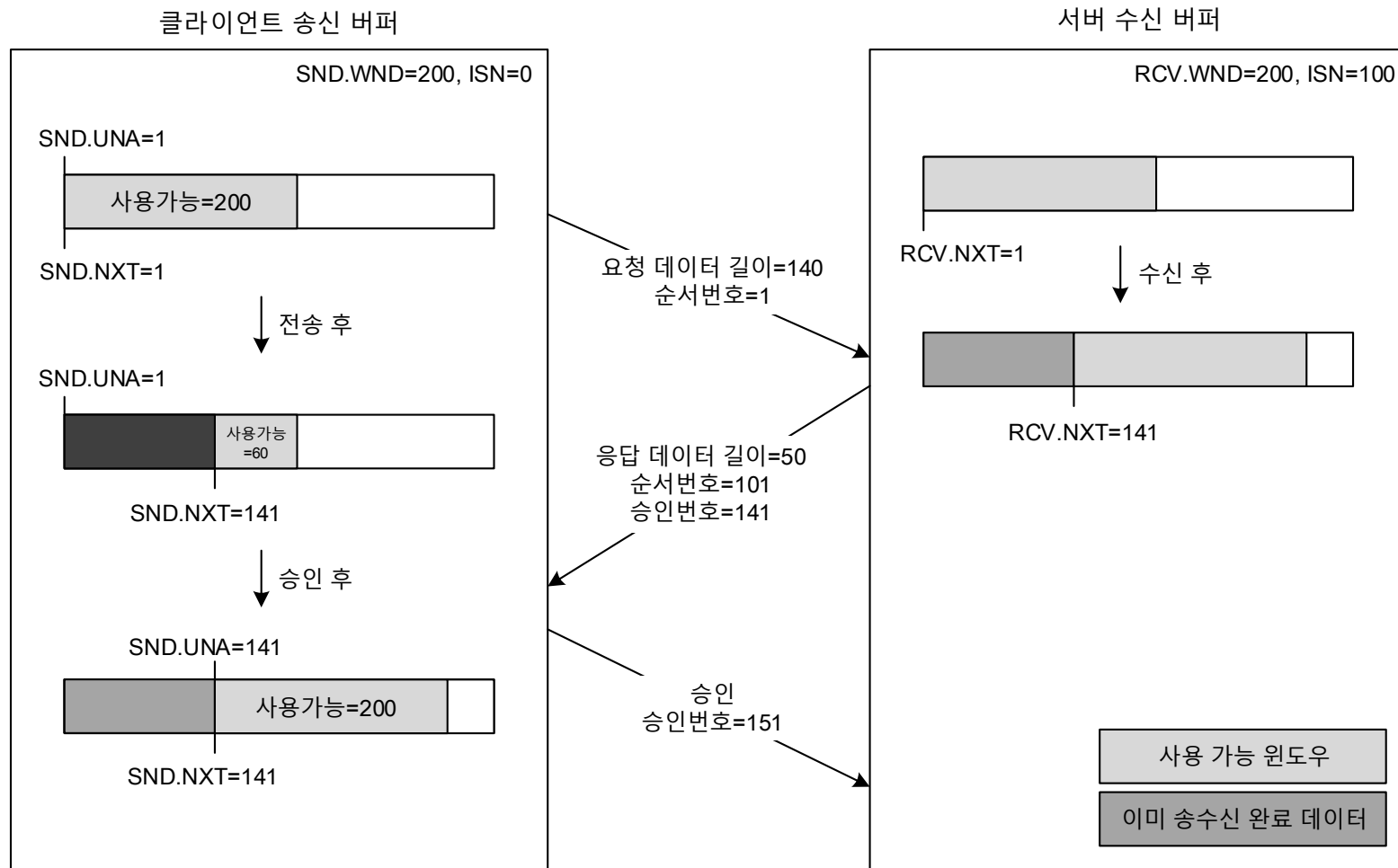


- 수신(RCV) 포인터



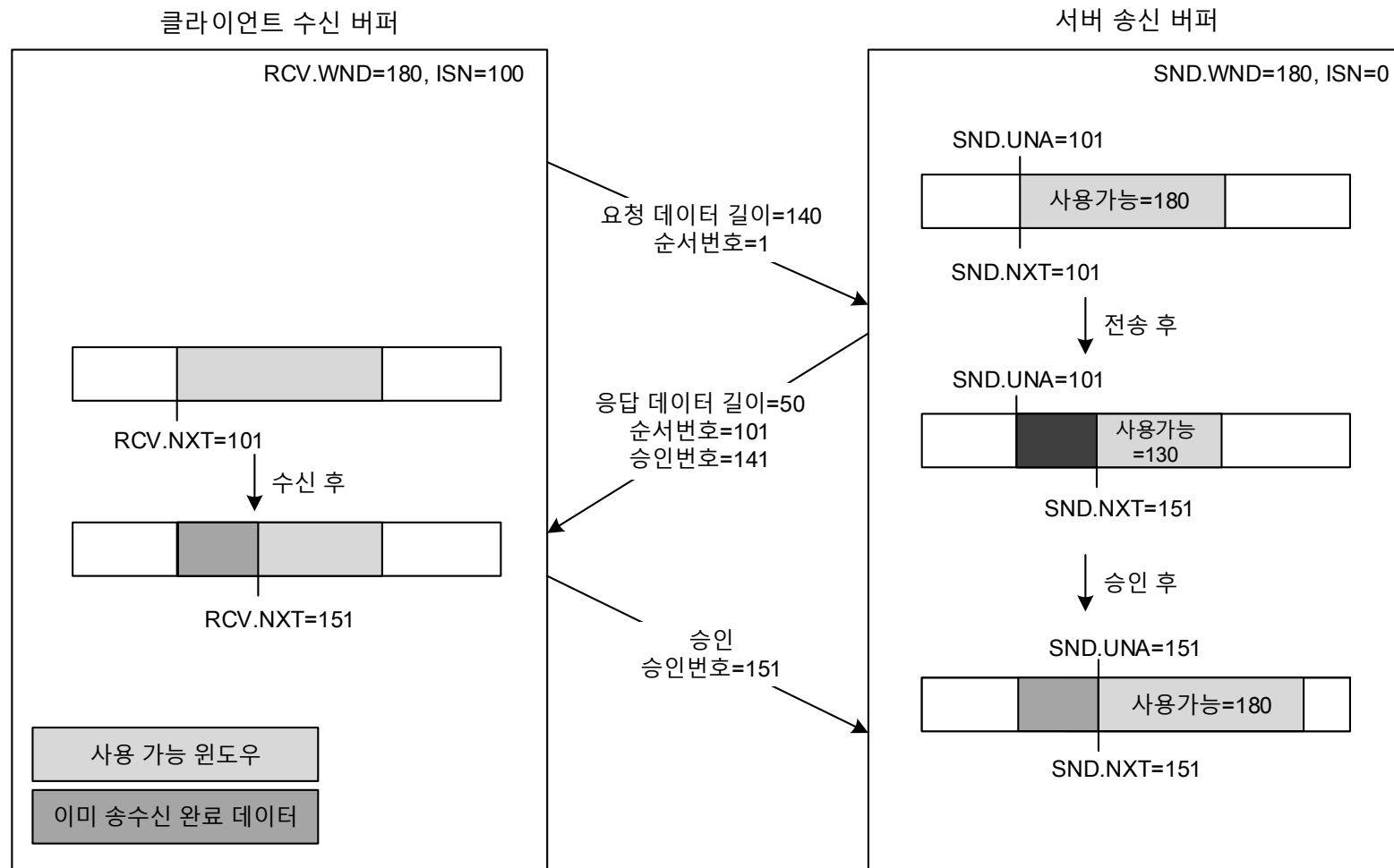
TCP 세그먼트 포맷과 데이터 송신

- TCP 데이터 송신 방식: 슬라이딩 윈도우
- 클라이언트 입장에서의 윈도우 방식



TCP 세그먼트 포맷과 데이터 송신

- TCP 데이터 송신 방식: 슬라이딩 윈도우
- 서버 입장에서의 윈도우 방식



TCP 세그먼트 포맷과 데이터 송신

- TCP 데이터 송신 방식: 슬라이딩 윈도우
 - 실제 복잡도

복잡한 이유	추가 설명
중복 송신	새로운 요청을 보냄과 동시에 수신한 세그먼트에 대한 승인
다중 세그먼트 승인	두 세그먼트를 수신한 후에 ACK 전송 가능
흐름 제어를 위한 윈도우 크기 조절	서버 공간이 부족한 경우, 송신한 데이터만큼 수신 윈도우 감소
송신 실패	송신 세그먼트가 사라지는 경우, 재전송 처리
작은 윈도우 문제 회피	바보 윈도우 증후군 현상 처리를 위한 슬라이딩 윈도우 수정
혼잡 처리와 회피	기본 슬라이딩 윈도우 방식을 수정하여 인터넷워크 혼잡 처리 및 회피

TCP 세그먼트 포맷과 데이터 송신

- TCP 데이터 송신 방식: 밀어넣기(Push)
 - 정의
 - 데이터를 즉각 전송하는 방식
 - 동작 방식
 - PSH 제어 비트 1로 설정하여 송신
 - 수신 장비는 애플리케이션으로 데이터 송신
- TCP 데이터 송신 방식: 긴급(Urgent)
 - 정의
 - 데이터를 우선 순위에 맞게 전송하는 방식
 - 동작 방식
 - URG 제어 비트 1로 설정하여 송신
 - 긴급 포인터 필드로 데이터의 마지막 바이트 가리킴
 - 수신 장비는 긴급 포인터로 긴급한 부분 결정

목 차

- 보충
 - ICMPv4 오류 메시지 유형
 - ICMPv4 정보 제공 메시지 유형
- TCP/IP 전송 계층 프로토콜
 - TCP 개요
 - TCP 원리와 일반 동작
 - TCP 기본 동작: 연결 수립, 관리와 종료
 - TCP 세그먼트 포맷과 데이터 송신
 - TCP 신뢰성과 흐름 제어 기능

TCP 신뢰성과 흐름 제어 기능

- TCP 세그먼트 재전송

- 재전송 과정

1. 재전송 큐에 배치, 타이머 시작

- 세그먼트 전송 시, 복사본을 재전송 큐라는 데이터 구조에 삽입
- 큐에 삽입 시 재전송 타이머 시작

2. 승인 처리

- 타이머 만료 전에 승인이 오는 경우, 큐에서 세그먼트 제거
 - 세그먼트가 지연되거나 버려지는 경우에 재전송 타이머가 만료되었다고 함

3. 재전송 시간 만료

- 타이머 만료 전에 승인이 오지 않는 경우, 재전송 시간 만료로 인해 세그먼트 자동 재전송

TCP 신뢰성과 흐름 제어 기능

- TCP 세그먼트 재전송
 - 세그먼트 승인 시간
 - 누적 순서 번호 사용
 - 세그먼트의 승인 번호 필드가 세그먼트의 마지막 바이트보다 더 큰 값을 가지는 경우, 세그먼트 승인 완료
 - e.g., 서버가 연속해서 네 개의 세그먼트를 보냈다고 가정

세그먼트	순서 번호 필드 (첫 번째 바이트 번호)	세그먼트 길이	세그먼트 마지막 순서 번호
1	1	80	80
2	81	120	200
3	201	160	360
4	361	140	500

TCP 신뢰성과 흐름 제어 기능

- TCP 재전송 처리 방식
 - 비연속적 승인 처리
 - 시간 만료된 세그먼트만 재전송
 - 여러 개의 세그먼트가 사라진 경우, 대기 시간 증가
 - 승인 받지 못한 모든 세그먼트 재전송
 - 시간 만료된 세그먼트와 승인 받지 못한 세그먼트 재전송
 - 필요하지 않은 경우에도 재전송하는 문제 존재
 - 첫 번째 세그먼트만 사라진 경우, 나머지 세그먼트는 필요치 않게 재전송됨

TCP 신뢰성과 흐름 제어 기능

- TCP 재전송 처리 방식
 - 선택적 승인(SACK, Selective Acknowledgment)
 - 비연속적 승인 처리의 해결책
 - 연결 수립 시 선택적 승인 허용 선택 사항을 사용하여 협상
 - 수신했으나 아직 승인하지 않은 세그먼트 범위에 대한 목록
 - 동작 과정
 1. 각 장비는 재전송 큐를 수정하여 세그먼트가 선택적으로 승인된 경우, SACK 비트를 1로 설정
 2. 특정 세그먼트 재전송 시, 세그먼트 중 SACK 비트가 1이 아닌 모든 세그먼트 재전송

TCP 신뢰성과 흐름 제어 기능

- TCP 재전송 처리 방식
 - RTT(Round-Trip Time) 계산에 기반한 적응형 재전송
 - 왕복 시간(RTT)
 - 송신된 세그먼트가 도착하여 승인을 되돌려 보내는데 걸리는 시간
 - RTT 계산
 - 새 RTT = $a * \text{예전 RTT} + ((1 - a) * \text{가장 최근 측정한 RTT})$
 - a 는 0에서 1까지의 값을 가짐
 - 모호한 승인(Acknowledgment Ambiguity)
 - 원래 세그먼트에 대한 승인인지 재전송 세그먼트에 대한 승인인지 알 수 없는 현상

TCP 신뢰성과 흐름 제어 기능

- TCP 재전송 처리 방식
 - 칸의 알고리즘
 - 재전송된 세그먼트에 적용되는 타이머 시간 계산과 평균 RTT 계산을 분리하는 알고리즘
 - 모호한 승인 문제 해결
 - 타이머 백오프(Backoff) 방식 도입
 - 평균 RTT에 기반하는 새로운 세그먼트의 재전송 타이머 설정
 - 세그먼트 재전송 시 타이머를 백오프로 몇 배 증가시켜 재전송 시간을 여유롭게 설정
 - 타이머 값은 재전송 성공할 때까지 증가하지만 일정 한도 존재
 - 세그먼트가 빠르게 재전송되는 상황을 방지할 수 있음

TCP 신뢰성과 흐름 제어 기능

- TCP 흐름 제어
 - TCP 윈도우 크기 조절
 - 윈도우 크기
 - 송신 전, 상대 장비로부터 받은 데이터를 저장할 수 있는 바이트 수
 - e.g., 서버 윈도우 크기가 360인 경우, 서버는 360바이트 이상 받지 않음
 - 상대 장비에서 들어오는 데이터 흐름을 조절하는 방법
 - 윈도우 크기 감소
 - 송신 측 데이터가 전달될 수 있는 양을 감소시킴
 - 송신 윈도우의 오른쪽 끝을 왼쪽으로 이동

TCP 신뢰성과 흐름 제어 기능

- TCP 바보 윈도우 증후군(SWS, Silly Window Syndrome)
 - 정의
 - 세그먼트 크기가 헤더 크기보다 작은 경우, 전송 시 최소 40바이트의 헤더를 붙여주어야 하는 비효율적인 현상
 - 회피 알고리즘
 - 수신자 SWS 회피
 - 수신 버퍼에 충분한 공간이 생길 때까지 대기
 - 수신자는 윈도우의 오른쪽 끝을 최소 단위만큼 움직여야 함
 - 최소 단위는 MSS나 버퍼의 절반 중 작은 것으로 결정
 - 송신자 SWS 회피와 네이글(Nagle)의 알고리즘
 - 승인 받지 못한 데이터가 없는 경우, 데이터 즉각 전송
 - 승인 받지 못한 데이터가 있는 경우, 모두 승인되거나 충분한 크기(MSS)의 세그먼트를 만들 만큼 데이터가 모이지 않은 한 후속 데이터 보내지 않음

TCP 신뢰성과 흐름 제어 기능

- TCP 혼잡과 회피 알고리즘

- 혼잡

- 세그먼트 송신 속도가 느려지거나 버려지는 경우를 의미
- 계속적인 재전송에 의해 혼잡 붕괴(Congestion Collapse) 현상 발생 가능
- 세그먼트 송신 후 승인 받지 못한 비율로 혼잡 정도를 알 수 있음

TCP 신뢰성과 흐름 제어 기능

- TCP 혼잡과 회피 알고리즘

- 혼잡 회피 알고리즘

- 느린 시작

- 초기에 세그먼트의 속도를 제한하는 알고리즘
 - 장비는 충분한 크기(MSS)의 세그먼트 하나를 송신 시 느리게 시작
 - 송신 윈도우 크기만큼 송신하거나 혼잡 상황을 알게 될 때까지 점점 더 많이 송신

- 혼잡 회피

- 혼잡 발생 시 세그먼트 속도를 억제하는 알고리즘
 - 느린 시작 알고리즘을 사용하여 혼잡이 다시 일어나지 않도록 다시 송신 속도를 증가시킴

TCP 신뢰성과 흐름 제어 기능

- TCP 혼잡과 회피 알고리즘

- 혼잡 회피 수정 알고리즘

- 빠른 재송신

- 승인을 세 번 이상 받는 경우 장비는 세그먼트가 손실되었다고 간주
 - 장비는 재송신 큐 과정 생략 후 사라진 세그먼트 재송신
 - 추가 지연 시간이 줄어들게 되므로 TCP 성능 높일 수 있음
 - 시간 만료를 기다리지 않기 때문

- 빠른 회복

- 빠른 재송신이 이루어지는 경우, 장비가 혼잡 회피 알고리즘을 이용하여 송신 속도를 증가시키는 알고리즘

Thanks!

김 지 혜 (jihye@pel.sejong.ac.kr)