

따라 하면서 배우는 IT

연결지향형 TCP 프로토콜

목차

INDEX

TCP 프로토콜

TCP가 하는 일
TCP 프로토콜의 구조

TCP 플래그

TCP 플래그의 종류
각 플래그의 기능

TCP를 이용한 통신과정

연결 수립 과정
3WayHandshake
데이터 송수신 과정

TCP 상태전이도

TCP 연결 상태의 변화
3Way Handshaking과
함께보기

따라 學IT

TCP 3Way Handshake 과정
계산해보기
TCP 프로토콜 분석하기

따라 하면서 배우는 IT

TCP 프로토콜

TCP 프로토콜

TCP가 하는 일

전송 제어 프로토콜(Transmission Control Protocol, TCP)은 인터넷에 연결된 컴퓨터에서 실행되는 프로그램 간에 통신을 **안정적으로, 순서대로, 에러없이** 교환할 수 있게 한다.

TCP의 안정성을 필요로 하지 않는 애플리케이션의 경우 일반적으로 TCP 대신 비접속형 사용자 데이터그램 프로토콜(User Datagram Protocol)을 사용한다.

TCP는 UDP보다 안전하지만 느리다.

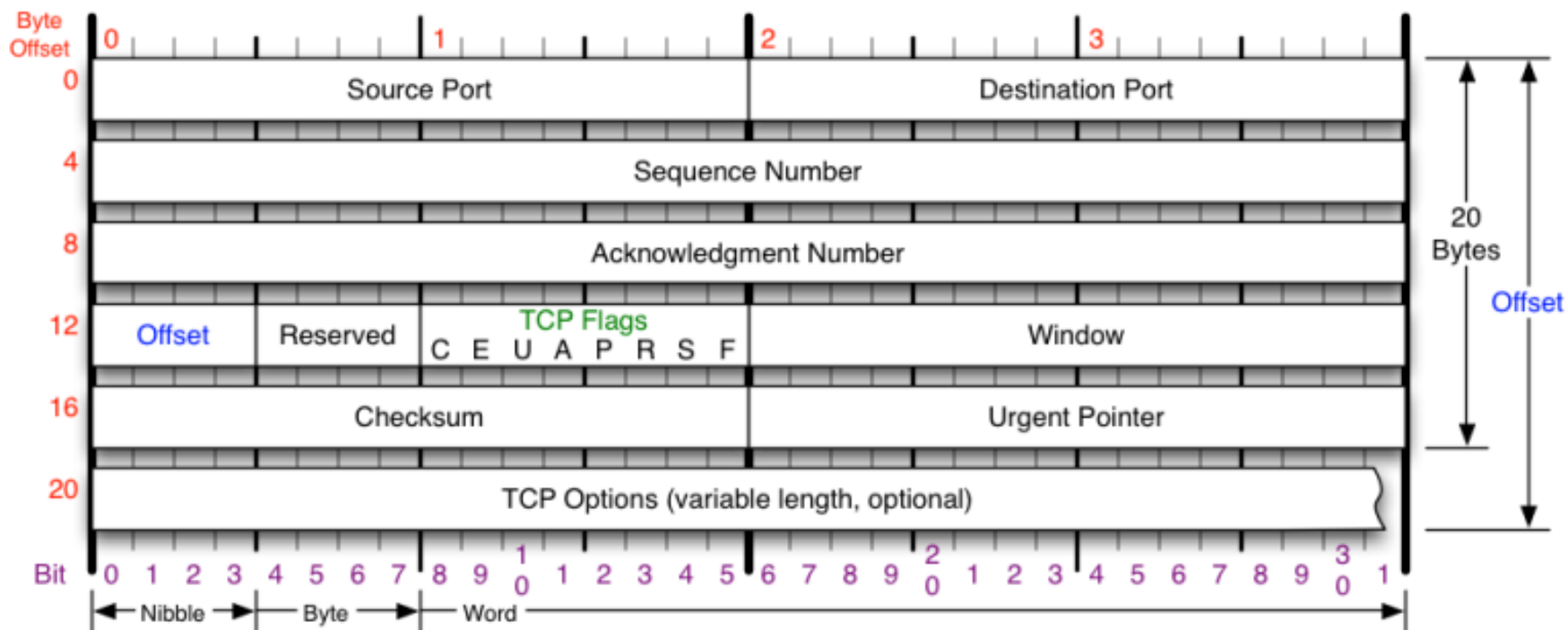
TCP 프로토콜

TCP 프로토콜의 구조

//

안전한 연결을 지향하는
TCP 프로토콜

//



따라 하면서 배우는 IT

TCP 플래그

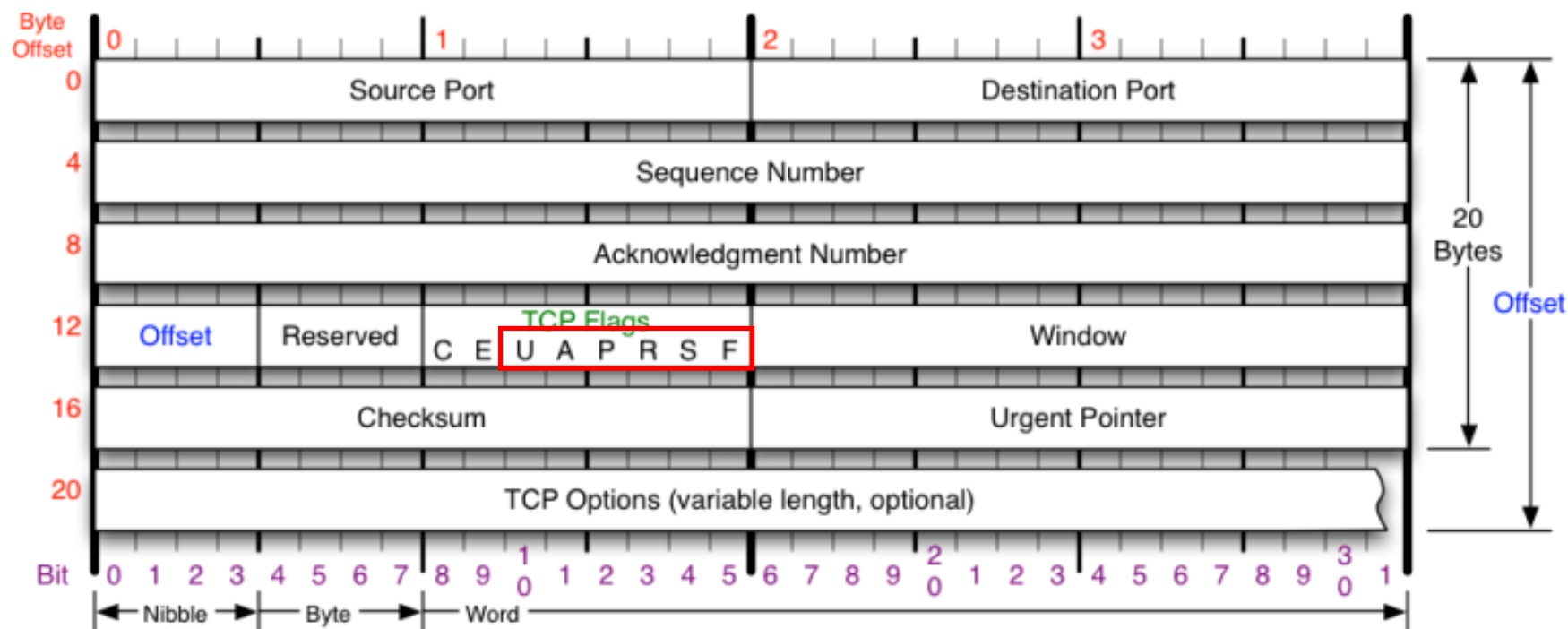
TCP 플래그

TCP 플래그의 종류

//

우아~프로스펙스
TCP 플래그

//



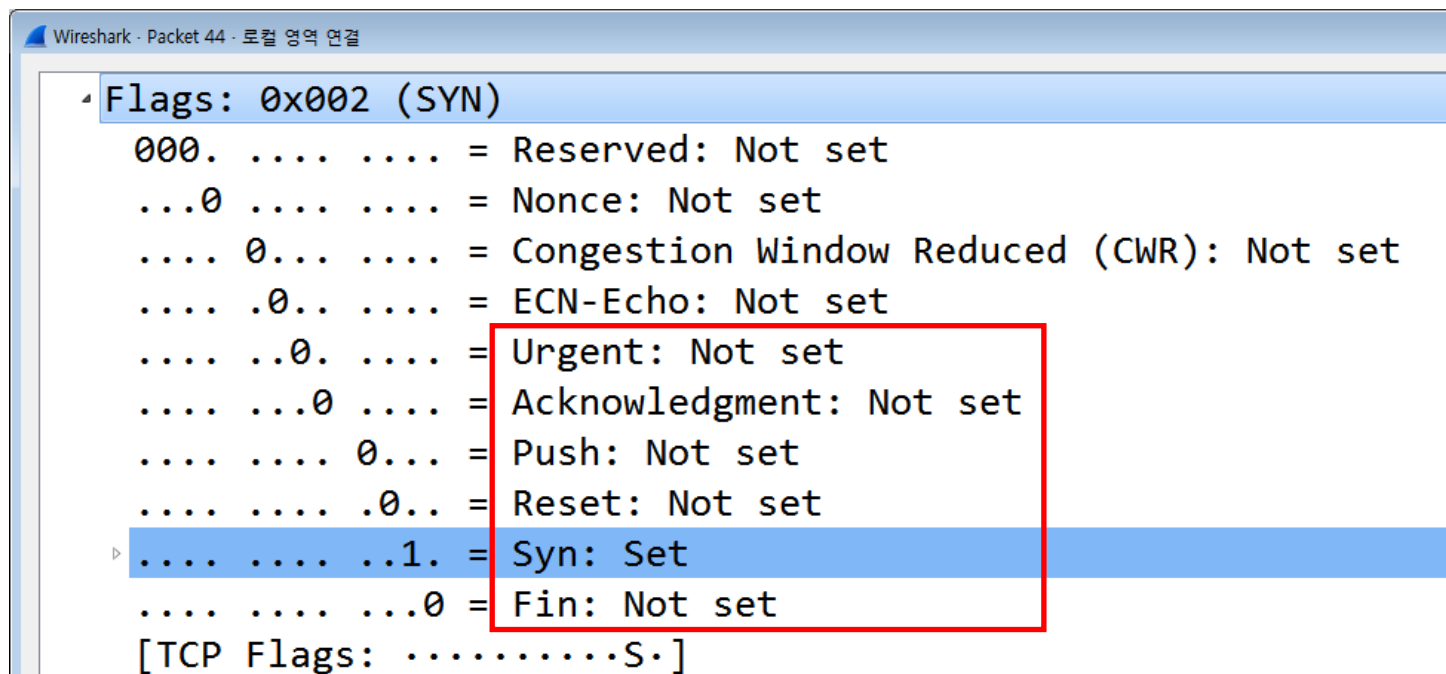
TCP 플래그

TCP 플래그의 종류

//

우아~프로스펙스
TCP 플래그

//



Wireshark - Packet 44 · 로컬 영역 연결

```
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
> .... .... ..1. = Syn: Set
.... .... ...0 = Fin: Not set
[TCP Flags: .....S.]
```


TCP 플래그

각 플래그의 기능

//

우아~프로스펙스
TCP 플래그

//

Urgent : 긴급 bit

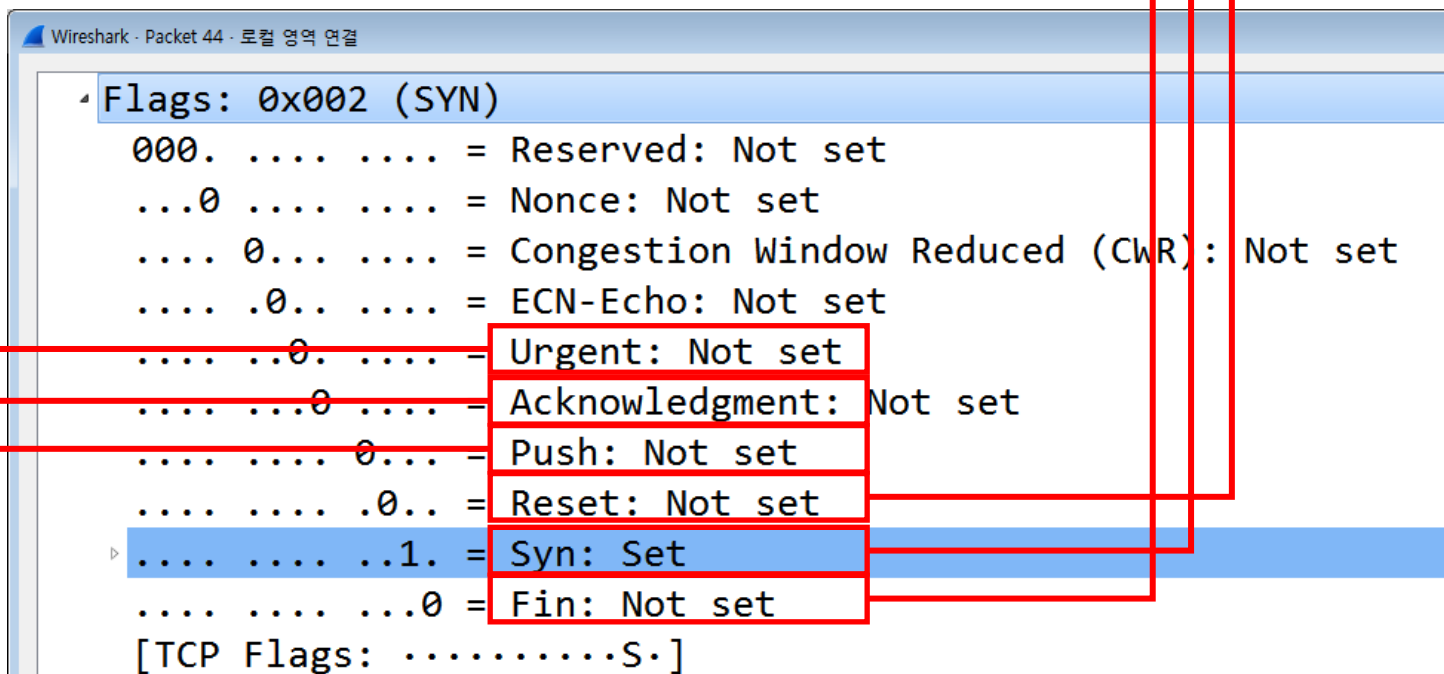
Acknowledgment : 승인 bit

Push : 밀어넣기 bit

Reset : 초기화 bit

Syn : 동기화 bit

Fin : 종료 bit



따라 하면서 배우는 IT

TCP를 이용한 통신과정

TCP를 이용한 통신과정

연결 수립 과정

TCP를 이용한 데이터 통신을 할 때 프로세스와 프로세스를 연결하기 위해
가장 먼저 수행되는 과정

1. 클라이언트가 서버에게 요청 패킷을 보내고
2. 서버가 클라이언트의 요청을 받아들이는 패킷을 보내고
3. 클라이언트는 이를 최종적으로 수락하는 패킷을 보낸다.

위의 3개의 과정을 3Way Handshake라고 부른다.

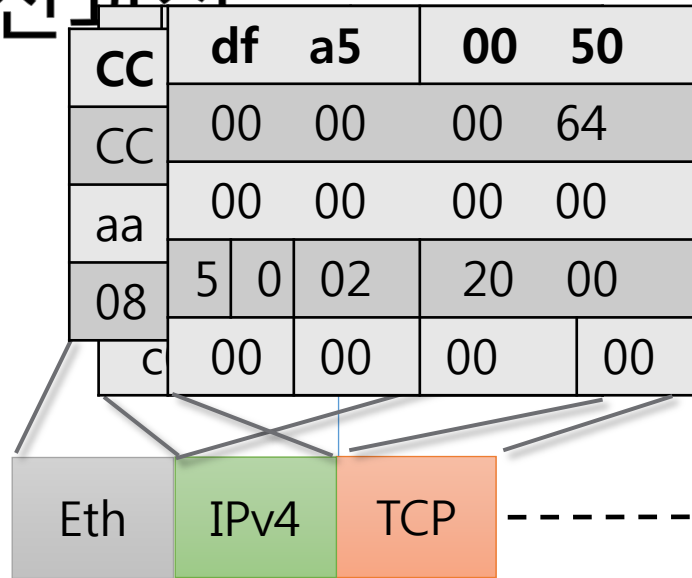
TCP를 이용한 통신과정

연결 수립 과정

//

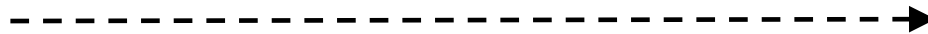
연결 수립을 하기 위한 통신
TCP 3Way Handshake

//



웹 서버

Flag : SYN
S:100 A:0



TCP를 이용한 통신과정

연결 수립 과정

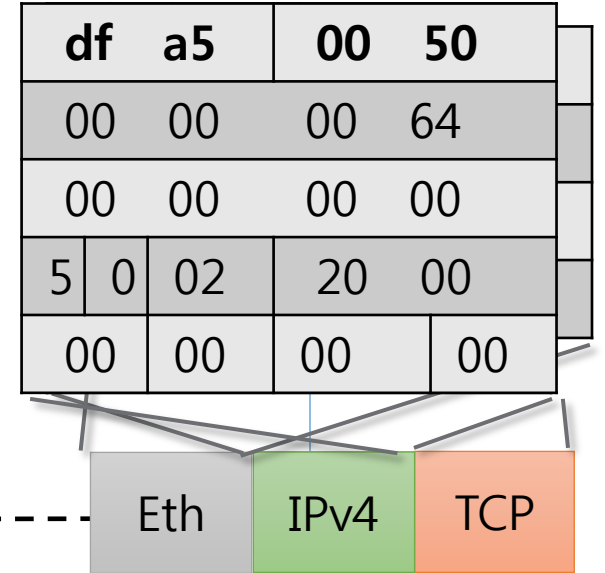


클라이언트

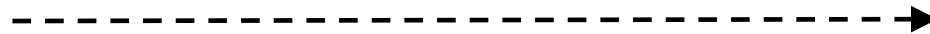
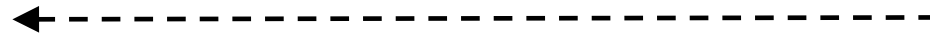
//

연결 수립을 하기 위한 통신
TCP 3Way Handshake

//



Flag : SYN
S:100 A:0



TCP를 이용한 통신과정

연결 수립 과정

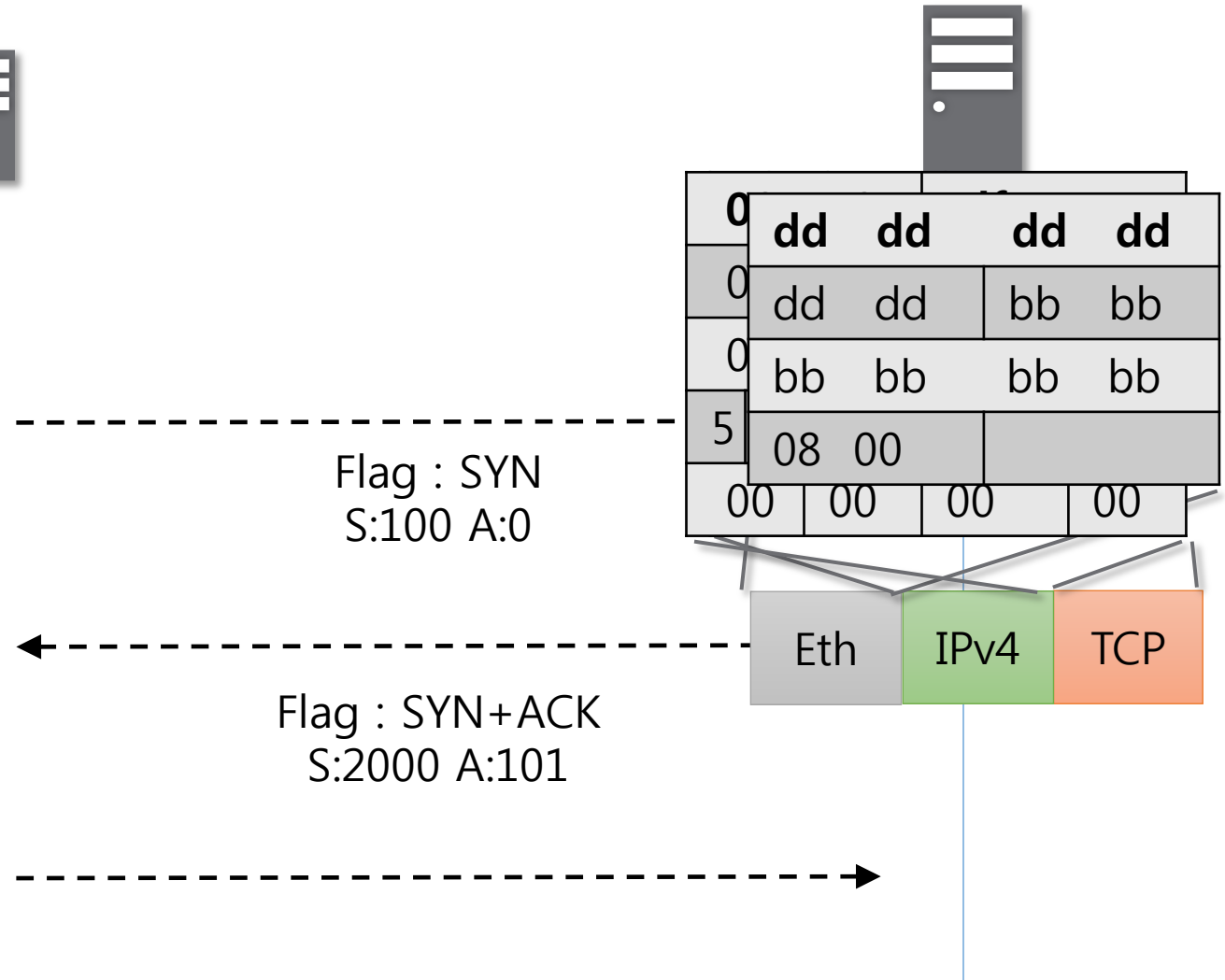


클라이언트

//

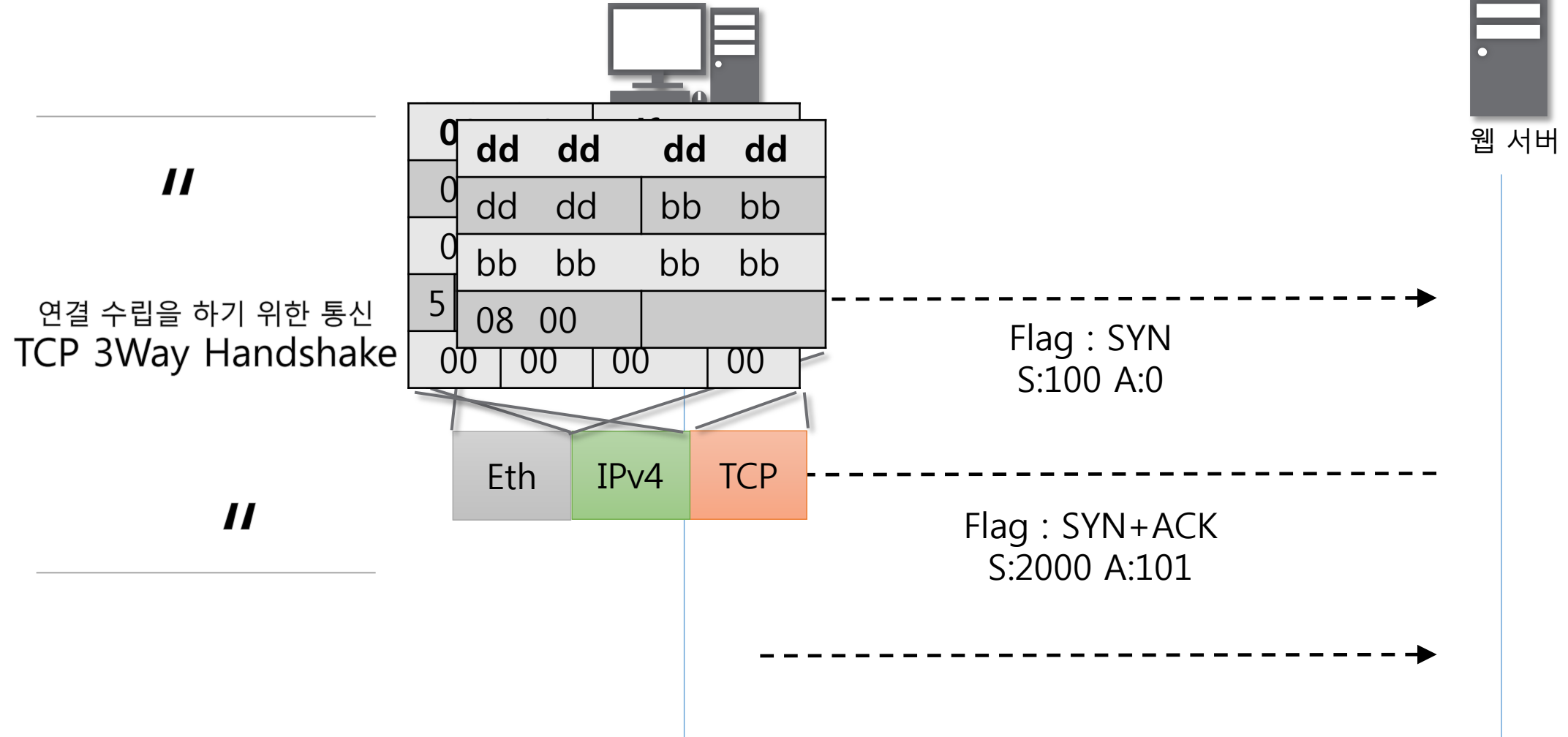
연결 수립을 하기 위한 통신
TCP 3Way Handshake

//



TCP를 이용한 통신과정

연결 수립 과정



TCP를 이용한 통신과정

연결 수립 과정



클라이언트

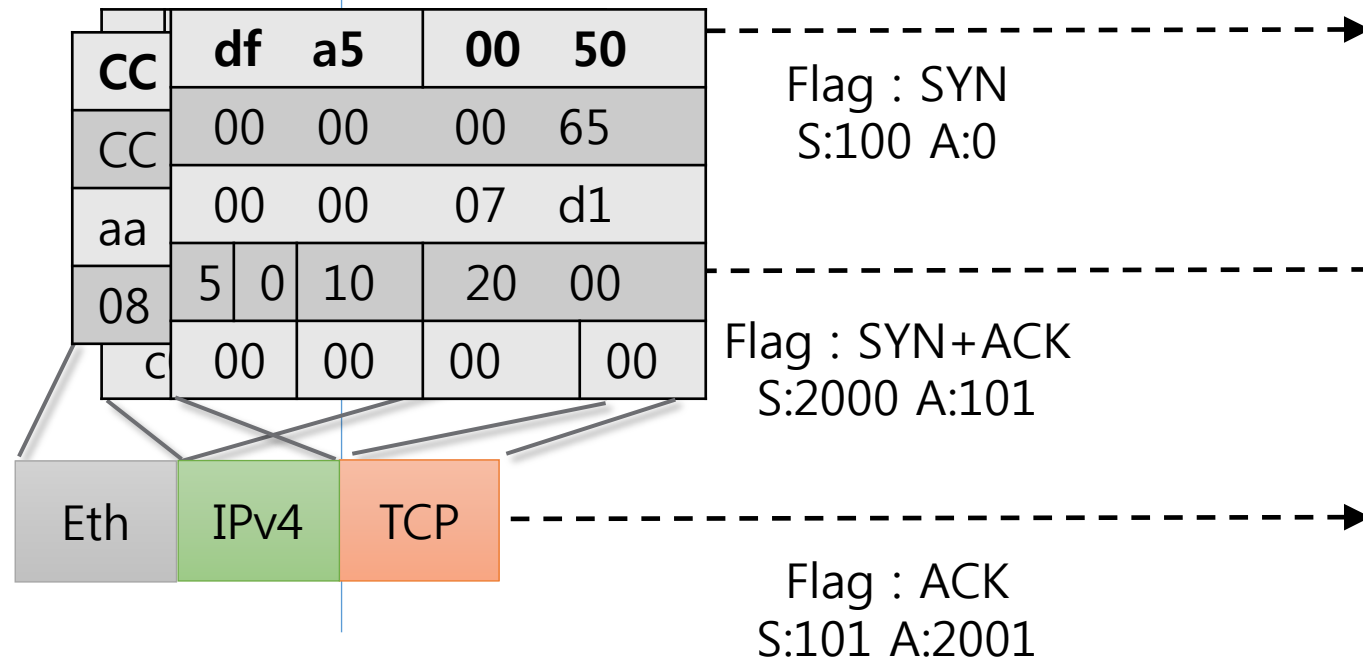


웹 서버

//

연결 수립을 하기 위한 통신
TCP 3Way Handshake

//



TCP를 이용한 통신과정

데이터 송수신 과정

TCP를 이용한 데이터 통신을 할 때 단순히 TCP 패킷만을 캡슐화해서 통신하는 것이 아닌 페이로드를 포함한 패킷을 주고 받을 때의 일정한 규칙

1. 보낸 쪽에서 또 보낼 때는 SEQ번호와 ACK번호가 그대로다.
2. 받는 쪽에서 SEQ번호는 받은 ACK번호가 된다.
3. 받는 쪽에서 ACK번호는 받은 SEQ번호 + 데이터의 크기

TCP를 이용한 통신과정

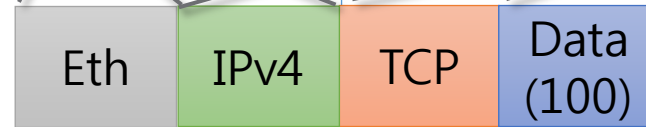
데이터 송수신 과정

//

HTTP나 FTP와 같은 각종
데이터를 포함한 통신

//

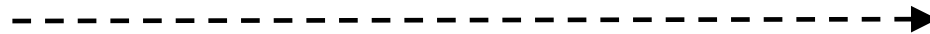
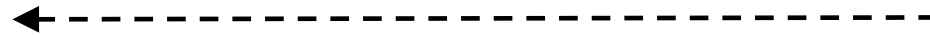
4	df	a5	00	50
1	00	00	00	65
80	00	00	07	d1
c	5	0	18	20 00
c	00	00	00	00



Flag : PSH+ACK
S:101 A:2001



웹 서버



TCP를 이용한 통신과정

데이터 송수신 과정

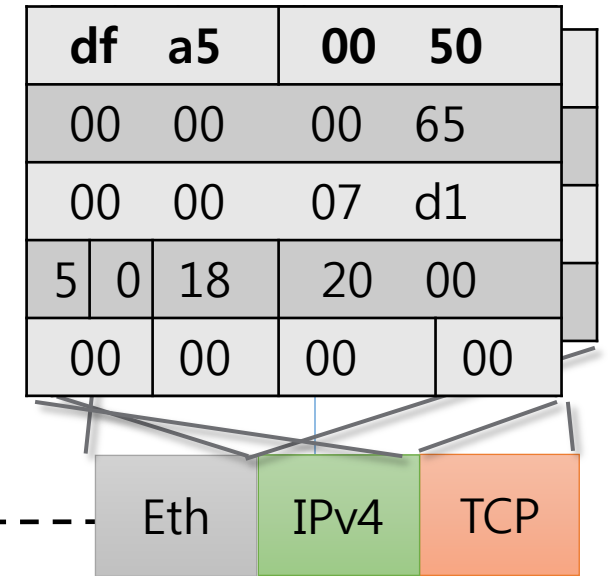


클라이언트

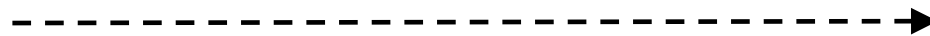
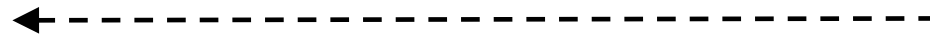
//

HTTP나 FTP와 같은 각종
데이터를 포함한 통신

//



Flag : PSH+ACK
S:101 A:2001



TCP를 이용한 통신과정

데이터 송수신 과정

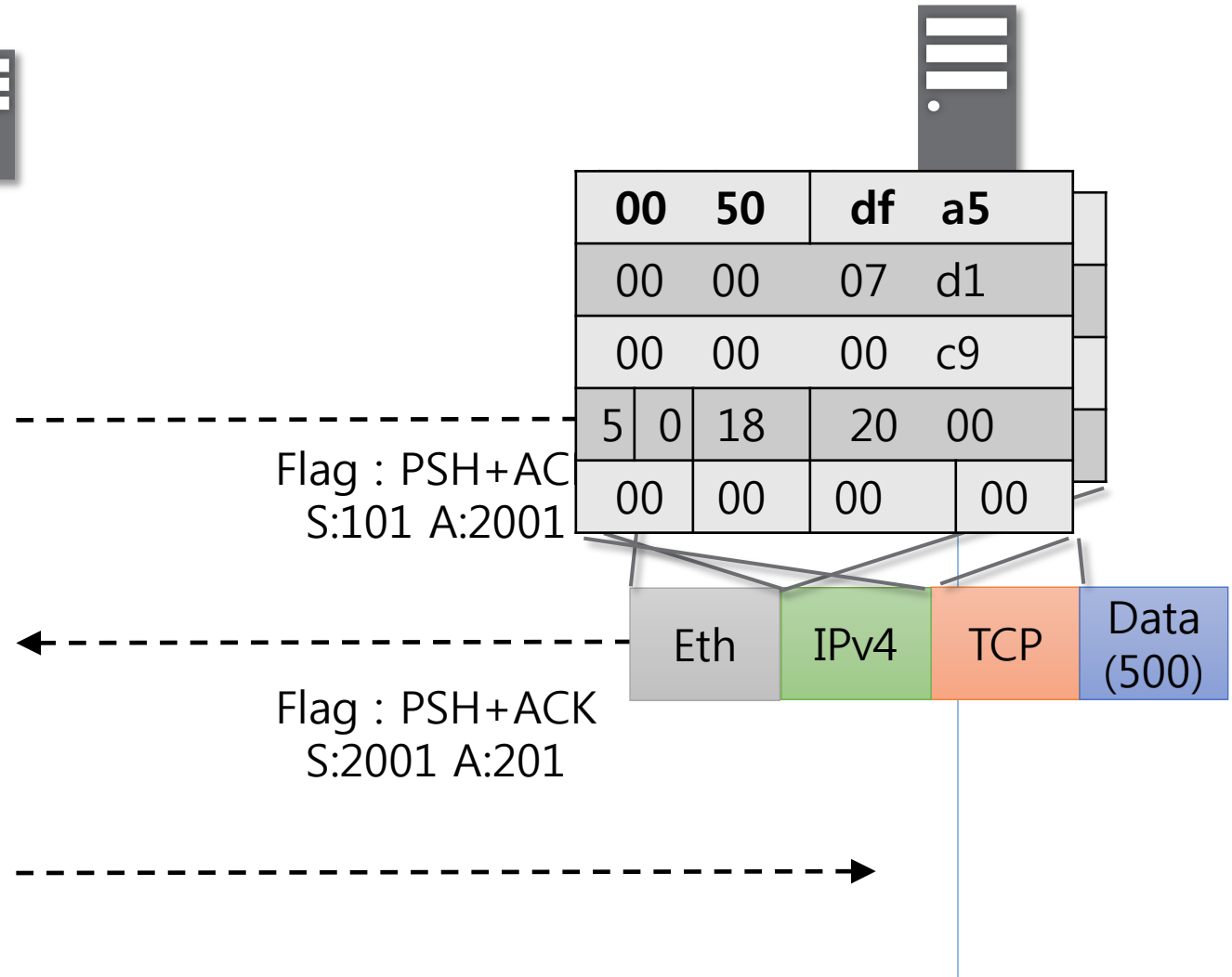


클라이언트

//

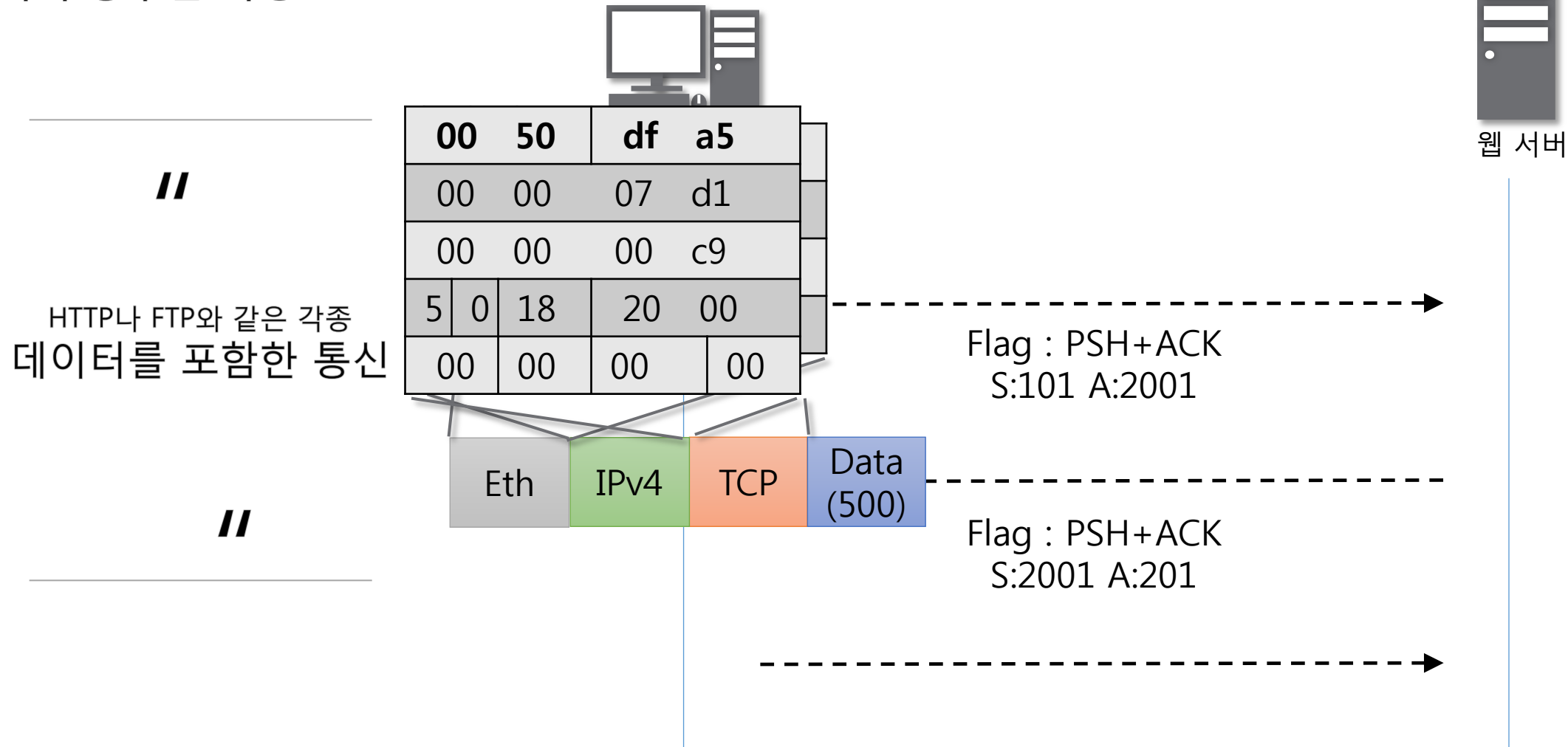
HTTP나 FTP와 같은 각종
데이터를 포함한 통신

//



TCP를 이용한 통신과정

데이터 송수신 과정



TCP를 이용한 통신과정

데이터 송수신 과정



클라이언트

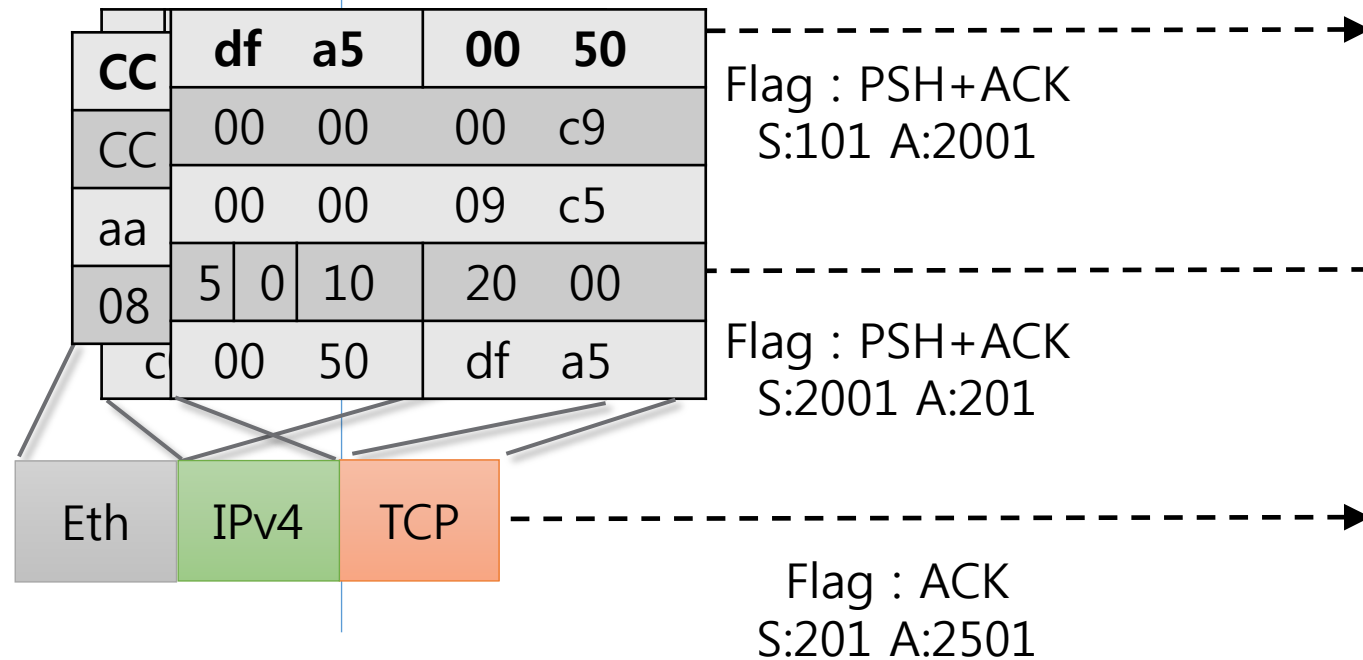


웹 서버

//

HTTP나 FTP와 같은 각종
데이터를 포함한 통신

//



따라 하면서 배우는 IT

TCP 상태전이도

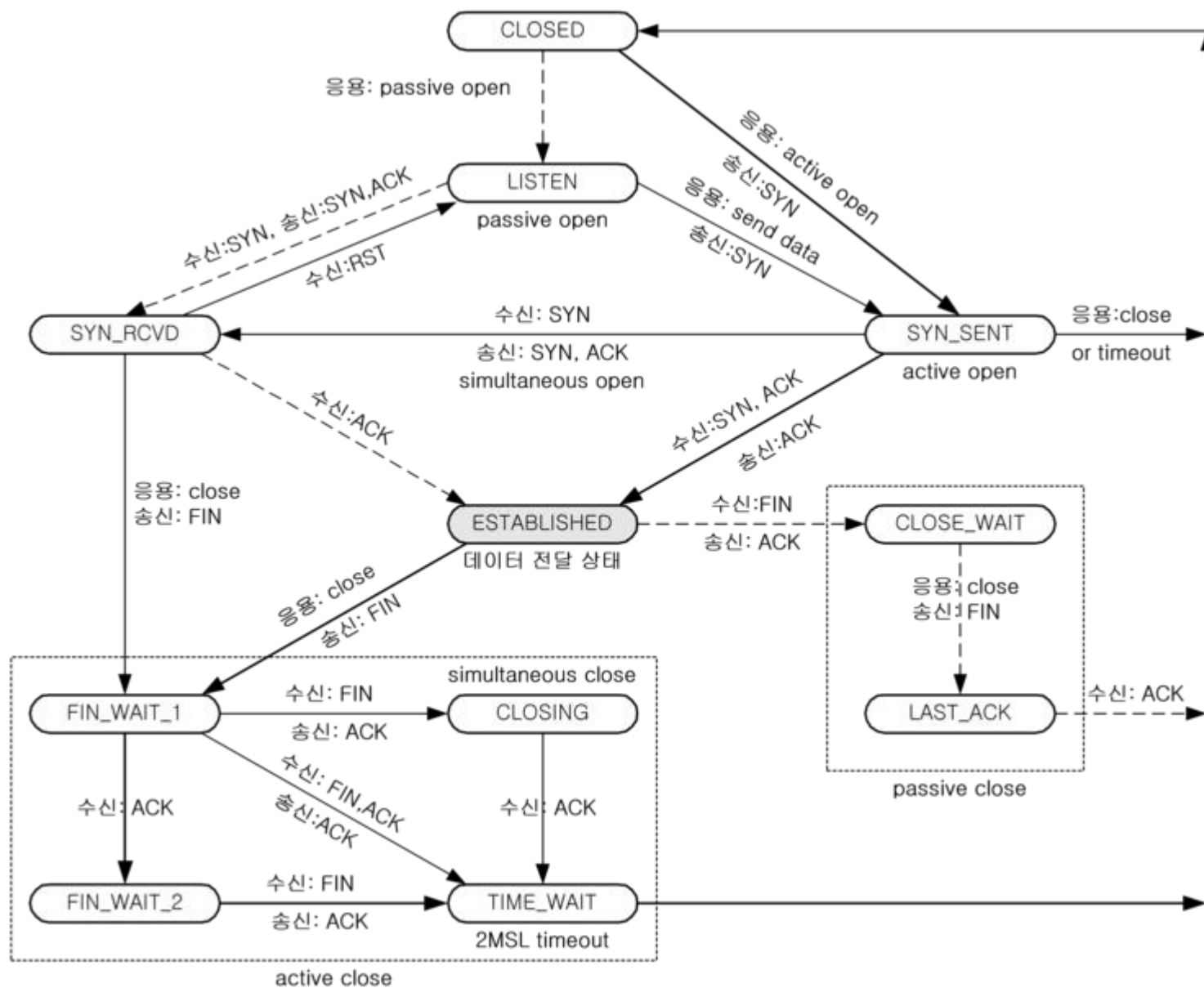
TCP 상태전이도

TCP 연결 상태의 변화

//

TCP의 여러가지
상태 변화

//



TCP 상태전이도

3Way-Handshake와 함께보기

//

연결을 수립하는
3Way-Handshake 과정
에서의 상태 변화

//

CC	df	a5	00	50	
CC	00	00	00	64	
aa	00	00	00	00	
08	5	0	02	20	00
c	00	00	00		00

Eth

IPv4

TCP

SYN_SENT

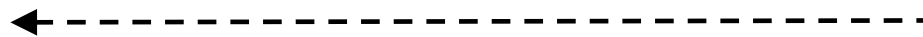
Flag : SYN
S:100 A:0



웹 서버

LISTENING

SYN_RECEIVED



TCP 상태전이도

3Way-Handshake와 함께보기



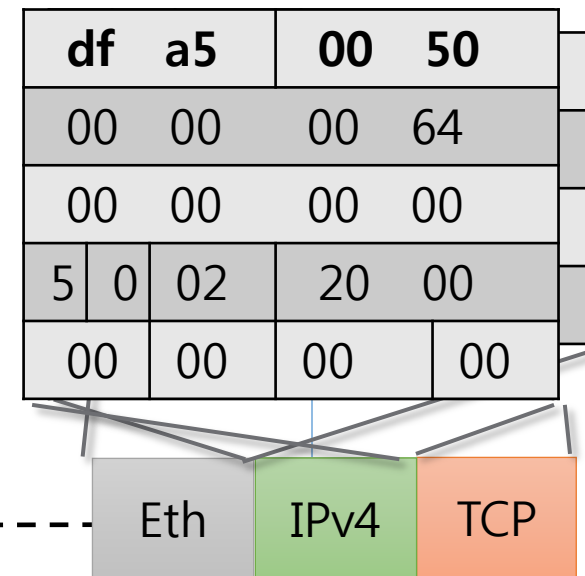
클라이언트

//

연결을 수립하는
3Way-Handshake 과정
에서의 상태 변화

SYN_SENT

//



Flag : SYN
S:100 A:0

SYN_RECEIVED



TCP 상태전이도

3Way-Handshake와 함께보기



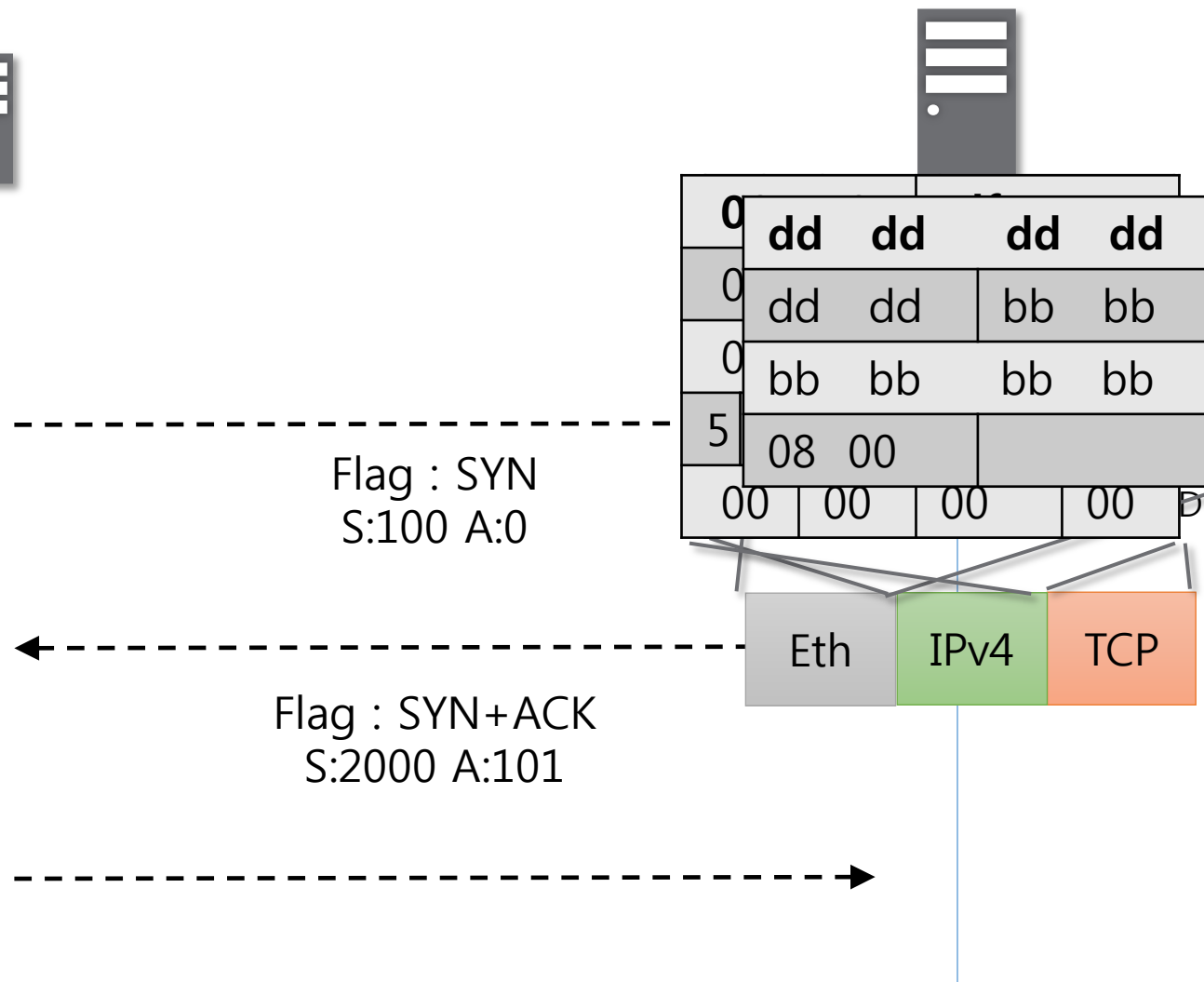
클라이언트

//

연결을 수립하는
3Way-Handshake 과정
에서의 상태 변화

SYN_SENT

//



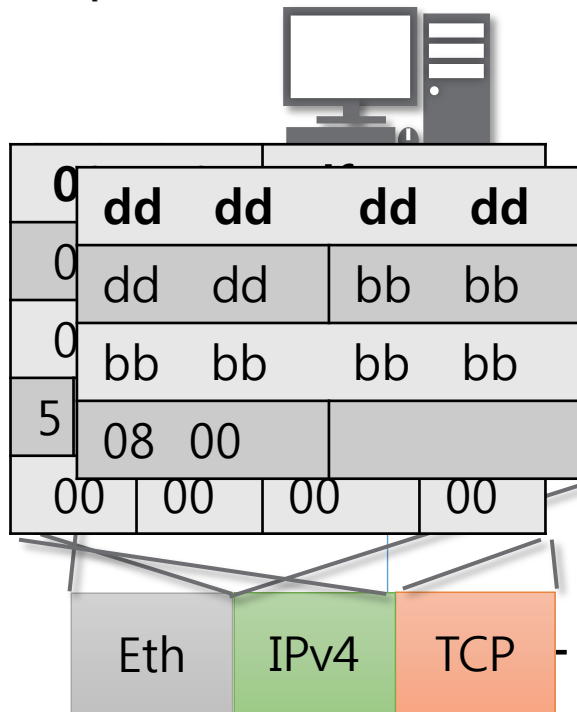
TCP 상태전이도

3Way-Handshake와 함께보기

//

연결을 수립하는
3Way-Handshake 과정
에서의 상태 변화

//



Flag : SYN
S:100 A:0

Flag : SYN+ACK
S:2000 A:101



웹 서버

LISTENING

SYN_RECEIVED

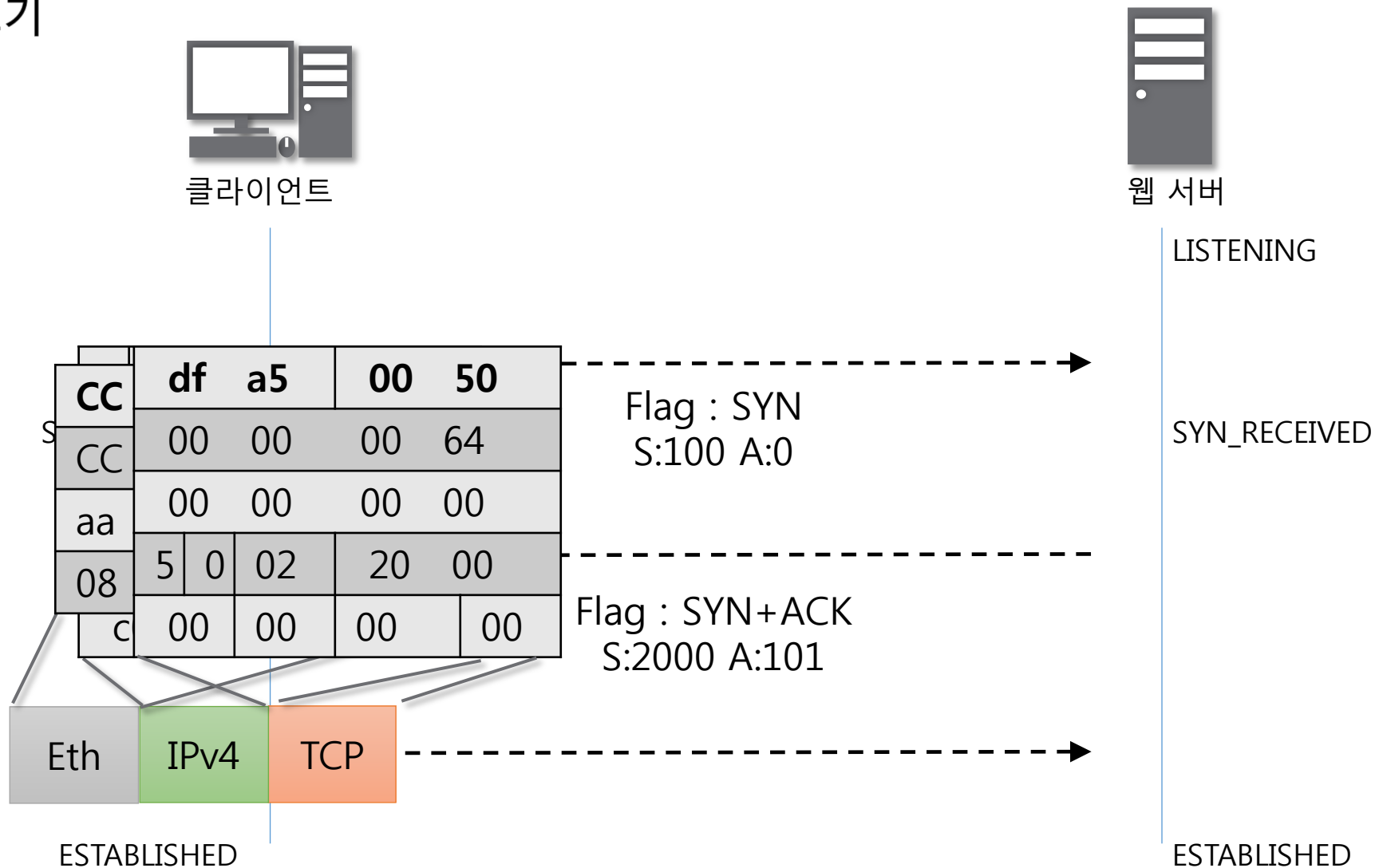
TCP 상태전이도

3Way-Handshake와 함께보기

//

연결을 수립하는
3Way-Handshake 과정
에서의 상태 변화

//



따라 하면서 배우는 IT

실습

1. TCP 3Way Handshake 과정 계산해보기

TCP 3Way Handshake 과정에서
플래그와 Seq번호, Ack번호를 확인해가며 직접 계산해보기

2. TCP 프로토콜 분석하기

TCP를 이용한 통신 과정을 Wireshark로 캡처하여 해당 패킷을 분석해보기

3. 데이터 송수신 과정 계산해보기

TCP를 이용한 통신을 할 때 데이터를 주고 받는 과정에서
플래그와 Seq번호, Ack번호를 확인해가며 직접 계산해보기

4. TCP 프로토콜 분석하기

TCP를 이용한 통신 과정을 Wireshark로 캡처하여 해당 패킷을 분석해보기