1. LAN어댑터에서 수신 신호를 디지털 데이터로 변환

여기에서는 클라이언트가 보낸 패킷이 서버에 도착한 부분부터 시작한다.

서버에 도착한 패킷의 실체는 전기나 빛의 신호이다.

- **수신 동작**

  ➔ 패킷의 신호를 LAN어댑터에서 수신하고 디지털 데이터로 바꾸는 부분에서 시작한다.

  ➔ LAN을 흐르는 패킷의 신호는 1과 0으로 이루어진 디지털 데이터의 신호와 타이밍을 나타내는 클록 신호를 합성한 것이다.

  ➔ 여기에서 클록 신호를 추출하고, 클록 신호에서 타이밍을 계산하면서 신호를 읽어오면 1과 0의 디지털 데이터로 바꿀 수 있다.

  ➔ 이후 FCS를 이용하여 오류 유무를 검사한다.

  ➔ 오류가 없으면 맨 앞의 MAC 헤더에 있는 수신처 MAC주소를 조사하여 패킷이 자신을 수신처로 하는지 판단한다.

  ➔ 이후 데이터를 LAN어댑터 내부의 버퍼 메모리에 저장한다.

    ■ 여기까지는 LAN어댑터의 MAC부분이 실행한다.

  ➔ 이때까지 CPU는 패킷의 도착을 모르기 때문에 인터럽트 방법을 사용하여 LAN어댑터에서 CPU로 패킷의 도착을 알린다.

  ➔ 이 시점에서 CPU는 LAN드라이버로 실행을 전환하고 버퍼 메모리에서 수신한 패킷을 추출한다.

  ➔ 이후 MAC헤더로부터 프로토콜을 판단하여 프로토콜 스택에 패킷을 건네 준다.

2. IP담당 부분의 수신 동작

- **수신 동작 흐름**

  ➔ 프로토콜 스택의 IP담당 부분은 IP헤더를 점검하고 자신을 대상으로 하는 것인지 판단한다.

  ➔ 조각 나누기에 의한 패킷의 분할이 있는지 조사한다.

    ■ IP헤더를 조사하면 분할 되었는지 알 수 있으므로 분할되어 있는 경우 패킷을

일시적으로 메모리에 저장한다.

- 이후 분할된 패킷 조각이 전부 도착한 시점에서 조각을 전부 조립하여 원래 패킷으로 복원한다.

➔ TCP담당 부분 또는 UDP담당 부분에 패킷을 건네 준다.

3. TCP담당 부분의 수신 동작

- **접속 패킷 수신 동작 흐름**

➔ 패킷이 접속 동작의 패킷인 경우 TCP 담당 부분은 TCP 헤더의 SYN의 컨트롤 비트를 확인한다.

- SYN컨트롤 비트가 1로 되어 있으면 접속 동작의 패킷이다.

➔ 수신처 포트 번호를 조사한다.

- 같은 번호로 할당한 접속 대기 상태의 소켓이 없을 경우 무언가 잘못된 것이므로 오류 통지 패킷을 클라이언트에 반송한다.

➔ 해당하는 접속 대기 소켓을 복사하여 새 소켓을 작성한다.

➔ 새 소켓에 송신처의 IP 주소나 포트 번호 등을 기록한다.

- **데이터 패킷 수신 동작 흐름**

➔ 데이터의 패킷을 수신한 경우 TCP 담당 부분은 도착한 패킷의 송신처 IP 주소, 송신처 포트 번호, 수신처 IP주소, 수신처 포트 번호로부터 해당하는 소켓을 판단한다.

- 접속이 끝난 소켓의 경우 서버측의 포트 번호로서 같은 값을 할당한 여러 개의 소켓이 존재할지도 모르므로 수신처 포트번호만으로는 소켓을 지정할 수 없다.

➔ 데이터의 조각을 연결하여 수신 버퍼에 보관한다.

- 소켓에 기록된 지난 번 시퀀스 번호나 데이터 조각의 길이로부터 다음 시퀀스 번호의 값을 계산하고, 도착한 패킷의 TCP헤더에 기록된 시퀀스 번호와 합치되는지 조사한다.

- 합치되면 제대로 서버까지 도착한 것이므로 데이터 조각을 추출하여 수신 버퍼에 저장한다.

➔ 클라이언트에게 ACK를 되돌려준다.

- 수신 확인 응답용 TCP헤더를 만들고, 여기에 수신 패킷의 시퀀스 번호와 데이터 조각의 길이로부터 계산한 ACK번호를 기록하고, IP담당 부분에 의뢰하여 클라이언트에게 반송한다.

4. TCP 담당 부분의 연결 끊기 동작

TCP 프로토콜의 규칙에 따르면 연결 끊기 동작은 클라이언트와 서버 중 어느 쪽이 먼저 실행해도 상관없다.

어느 경우 든지 연결 끊기 동작이 끝나면 잠시 기다렸다가 소켓을 말소한다.