

6주차 2차시 TCP/IP 프로토콜

【학습목표】

1. TCP/IP의 개념 대해 설명할 수 있다.
2. TCP/IP 계층구조 및 IP헤더 및 주소 체계에 대해 설명할 수 있다.

학습내용1 : TCP/IP의 개념

서로 다른 네트워크에 연결되어 있는 여러 가지 다른 종류의 컴퓨터들이 서로 통신할 수 있도록 하는 프로토콜의 집합으로 데이터를 같은 크기의 패킷으로 나누어서 전송하며, 각 패킷은 연속적인 일련번호와 받는 사람의 주소가 첨가되어 있다.

1. TCP(Transmission Control Protocol)

데이터를 패킷으로 나누며, TCP는 데이터의 흐름을 관리하고 데이터가 정확한지를 검사한다.

2. IP(Internet Protocol)

나누어진 패킷을 네트워크나 원거리에 있는 호스트로 보내주며, 패킷을 한 장소에서 다른 곳으로 옮기는 역할을 한다.

3. TCP/IP와 OSI 모델의 비교

(1) TCP/IP가 성공하게 된 요인

- 어느 네트워크에도 쉽게 적용 가능한 유연성

(2) TCP/IP의 단점

- 다른 프로토콜 스택(stack)들과는 호환되지 않아서, TCP/IP를 사용하지 않는 네트워크에서 쓰기에는 적합하지 않음

(3) TCP/IP와 OSI 모델의 공통점

- 독립적인 프로토콜들로 이루어진 스택
- 대응하는 각 계층은 유사한 기능을 함

(4) TCP/IP와 OSI 모델의 차이점

- 시스템 유연성에 대한 차이

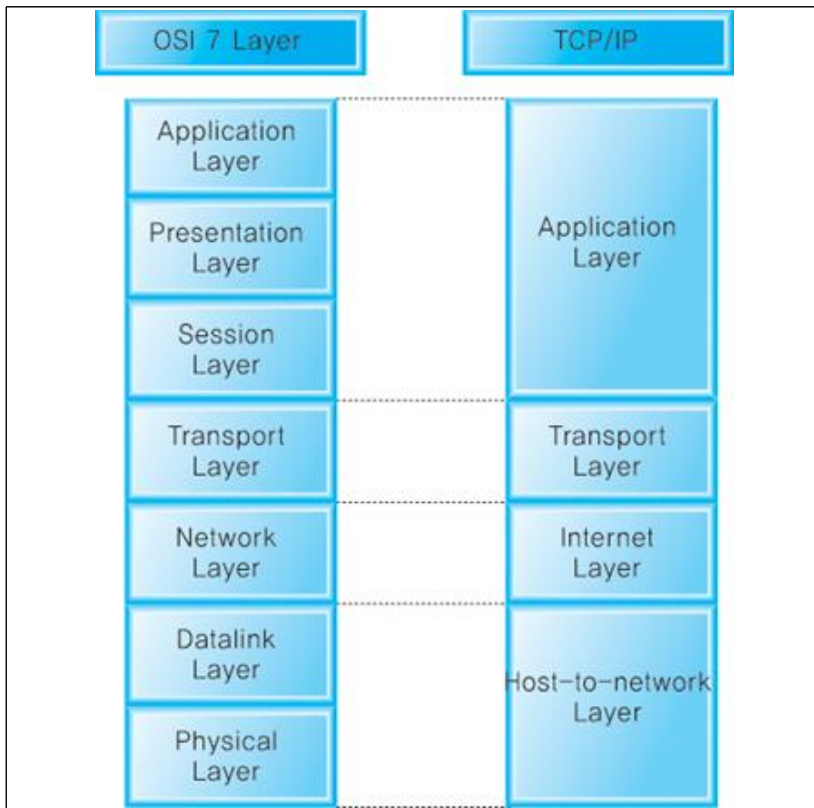
① OSI 계층

- 계층의 독립성과 인접 계층 간의 인터페이스 고려
- 하나의 가상적 네트워크를 대상으로 조직적으로 개발된 모형
- 비연결 지향형 서비스를 제공

② TCP/IP 계층

- 네트워크 환경에 따라 여러 개의 프로토콜을 허용
- 각 모형에 적합한 서비스 특성의 차이
- 다양한 네트워크를 연결하는 과정에서 많은 시도와 실패를 거치면서 점진적으로 진화
- 비연결 지향형 서비스를 제공
- 계층 수의 차이

[그림] OSI계층과 TCP/IP계층 모형



학습내용2 : TCP/IP 계층 구조

1. 응용 계층(Application Layer)

인터넷 사용자들이 실제로 접하게 되는 네트워크 응용 프로그램으로 클라이언트-서버 방식으로 지원된다.

① 지원되는 프로토콜

TELNET, FTP, TFTP, SMTP, MIME 등

MIME(Multipurpose Internet Mail Extensions)

IETF에서 제정

이메일 서비스를 이용할 때 아스키(ASCII) 데이터가 아닌 다른 미디어의 데이터를 전송하기 위해 고안된 프로토콜 SMTP 프로토콜을 변경하거나 대체시키지 않고, 임의의 미디어 데이터를 아스키 데이터 형식으로 인코딩 시킨 후에 표준 형식의 이메일 메시지로 전송

2. 전송 계층(Transport Layer)

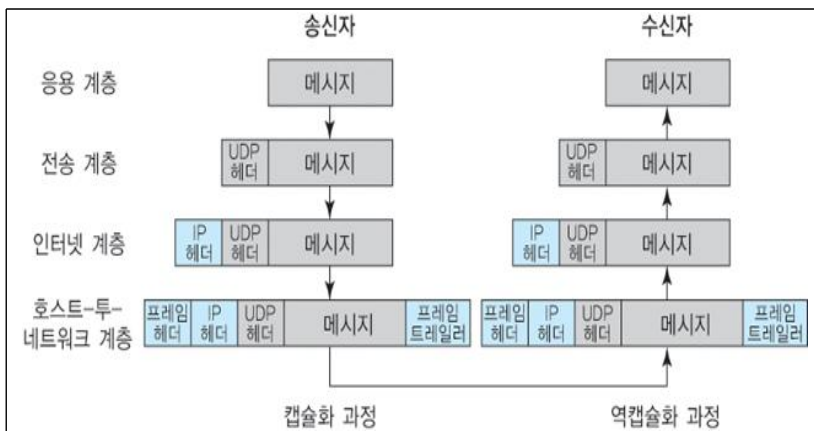
호스트-투-호스트 전송 계층(Host-to-host Transport Layer)이라고도 하며, 서로 다른 네트워크로 연결된 시스템의 호스트나 호스트 사이의 프로토콜에서 데이터를 전달하거나 수신할 수 있게 해준다. 또한 세션의 초기화, 오류 제어, 순서 검사를 포함하는 데이터 경로와 전달을 관리하고, TCP와 UDP(User Datagram Protocol)가 사용되며, 캡슐화와 역캡슐화(decapsulation)를 제공한다.

[세부설명]

TCP는 전달할 메시지를 세그먼트 단위로 분할하고 각 세그먼트마다 헤더를 추가하여 하위 계층으로 전달한다.

UDP는 메시지를 분할하지 않고 간단히 헤더만을 추가한 데이터 그램 상태로 하위 계층으로 전달하며, 역캡슐화 과정은 이 과정의 반대이다.

[그림] 캡슐화 과정과 역캡슐화 과정



(1) TCP

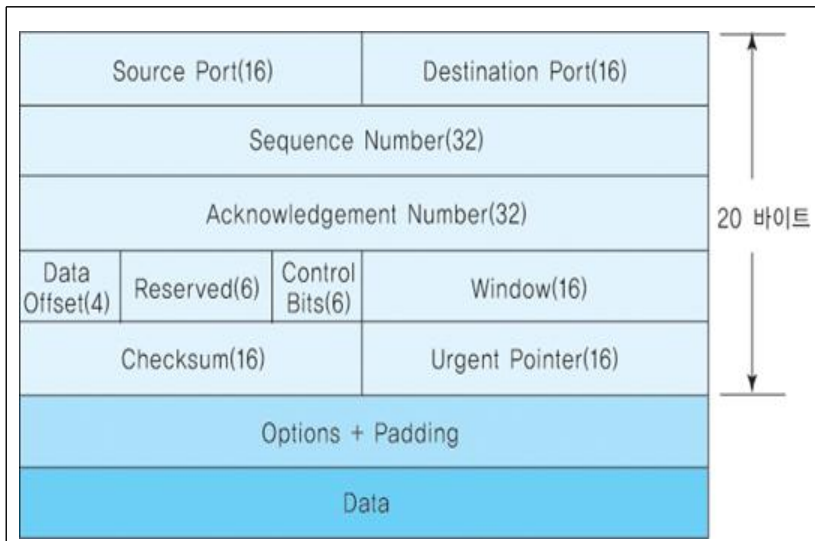
종단(End) 매체 시스템 사이의 오류를 감지하여 신뢰성 있는 데이터 전달을 제공해주는 프로토콜
데이터 스트림을 받아들이고 그 데이터 스트림을 세그먼트 단위로 나눈 후에, IP로 넘겨주는 역할
연결 지향형 서비스이면서 바이트 스트림 프로토콜

TCP의 신뢰성은 PAR(Positive Acknowledgement with Retransmission)의 재전송 방식을 사용하여 보장하는데, 만약 상대 시스템에 데이터가 올바르게 전송되었는가의 여부를 알지 못하면 PAR을 이용해서 데이터를 재전송

두 호스트 사이에 논리적인 종단 접속을 설정하거나 해제하는 역할

이 때, 3-way 핸드셰이킹(handshaking)을 사용

[그림] TCP 헤더



[세부 설명]

Source Port :송신지의 호스트 응용 프로그램에 의해 정의되는 TCP 포트 번호를 나타냄

[예] HTTP는 80번을 사용

Destination Port : 수신지의 포트 번호를 나타냄.

Sequence Number : 나누어진 세그먼트(segment)에 대해, 그 순서에 따라 붙인 일련번호를 나타냄

Acknowledgement Number : 수신한 마지막 바이트의 sequence number + 1

제어 비트 필드의 ACK 플래그가 설정된 경우에만 의미가 있음

Data Offset (또는 Header Length) : 헤더 내에 몇 개의 32비트 워드가 있는지 나타냄

헤더의 크기를 나타내며, 데이터의 시작 부분의 위치를 알 수 있음

Reserved : 차후에 사용하기 위해 남겨 둔 필드로 현재는 0의 값을 가짐

Control Bits : 세그먼트의 용도와 내용을 결정하기 위해 쓰이며, 1로 설정되어 있으면 그에 해당하는 것을 가리킴(URG, ACK, PSH, RST, SYN, FIN)

Window : 흐름 제어에 사용

Checksum : 오류 제어를 위해 체크섬 기능 제공

Urgent Pointer : 긴급 데이터에 이어지는 바이트(보통 비긴급 데이터)의 sequence number를 가리킴

TCP 세그먼트 내의 긴급 데이터의 위치 식별 가능

제어 비트 필드의 URG 플래그가 설정되었을 때에만 동작

Options : 옵션들이 정의되는 필드로, 그 크기는 가변적

Padding : TCP 헤더를 32비트 경계선에서 끝나도록 하기 위해, 필요한 경우 0으로 채움

(2) UDP

전송량이 적은 경우에 사용되며, 비연결형 데이터 그램 전달 서비스를 제공하는 프로토콜을 말함

메시지를 세그먼트로 나누지 않고 블록의 형태로 전송하며, 재전송이나 흐름 제어와 같은 기능이 없어서 메시지의 신뢰성 있는 전송을 보장할 수 없음

TCP에 비해 헤더 구조가 간단하며, 지원해 주는 기능도 단순

① UDP 헤더

Source Port : 송신자의 포트 번호

Destination Port : 수신자의 포트 번호

Length : 메시지 길이

Checksum : 오류 제어를 위해 헤더와 데이터 모두에 수행되는 체크섬

[표] TCP와 UDP의 비교

구분	프로토콜	TCP	UDP
서비스		연결형 서비스	비연결형 서비스
수시하는 순서		송신 순서와 같음	송신 순서와 다를 수 있음
오류제어/흐름제어		있음	거의 없음

3. 인터넷 계층 (Internet Layer)

TCP/IP 프로토콜에서 사용하는 전송 메커니즘으로 비연결 지향형 데이터그램 프로토콜이며, 비신뢰성 프로토콜이다. 오류 검사나 추적을 제공하지 않고 best-effort 방법으로 전송 하며, 데이터의 주소, 전송, 패킷의 분할과 복구의 기능 제공한다. IP 프로토콜을 지원하기 위한 프로토콜로는 주소 변환 프로토콜(ARP : Address Resolution Protocol) , 역주소 변환 프로토콜(RARP : Reverse Address Resolution Protocol), 인터넷 제어 메시지 프로토콜(ICMP : Internet Control Message Protocol), 인터넷 그룹 메시지 프로토콜(IGMP : Internet Group Message Protocol) 이 있다.

4. 호스트-투-네트워크 계층(Host-to-Network Layer)

단위 네트워크 내에서 패킷 전송을 담당하며, 전송 매체의 접근 방법, 네트워크 사이의 데이터 전송의 순서를 기술한다. 이 계층은 특정 프로토콜을 규정하는 것이 아니라, 모든 표준과 관련된 기술적인 프로토콜을 지원한다.

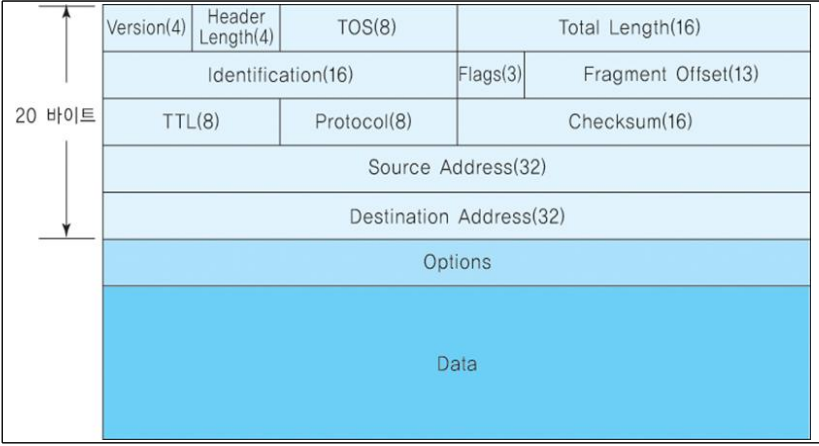
[표] TCP/IP 프로토콜의 각 계층 기능

계층	기능
응용 계층	응용 프로세스간의 정보 교환
전송 계층	호스트 간의 데이터 경로와 전달 관리
인터넷 계층	통신전담 프로세서간의 네트워크를 통한 패킷 교환
호스트-투-네트워크 계층	단위 네트워크 내에서의 패킷과 신호 전송

학습내용3 : IP 헤더 및 주소 체계

1. IPv4 헤더

[그림] IPv4 헤더 모형



[세부설명]

Version : 4

Header Length : 헤더의 전체 길이를 4바이트 단위로 표시

TOS(Type Of Service) : 데이터그램이 라우터에서 어떻게 처리되어야 하는지를 정의

우선 순위를 주어 혼잡도가 높을 때 폐기하는 순서를 지정할 수 있음

Total Length : 데이터 그램 전체 길이를 바이트 단위로 나타냄

Identification : 데이터 그램이 발신지에서 생성될 때 지정 받은 값

데이터 그램이 잘게 쪼개어져도 이 식별자 값은 유지되며 최종 목적지에서 다시 재조립될 때 이용됨

Flags

- 첫 번째 비트 : 사용되지 않음
- 두 번째 비트 : DF(Don't Fragment)로 더 이상 분할할 수 없음을 나타냄
- 세 번째 비트 : MF(More Fragment)로 마지막 조각인지를 알려줌. 만약 MF가 1이면

마지막 조각이 아니고, 0이면 마지막 조각이거나 분할되지 않았음을 의미

Fragment Offset : 쪼개진 데이터그램이 원래 데이터그램의 어느 부분에 위치하는지를 나타내는 필드

TTL(Time To Live) : 인터넷에 체류할 수 있는 시간을 홉(hop) 수로 나타낸 필드

라우터를 지날 때마다 1씩 감소되고 0이면 데이터 그램이 폐기됨

Protocol : IP 상위 계층의 프로토콜을 가리키는 식별자

Checksum : 오류 확인을 위한 필드

Source Address

Destination Address

Options

1 바이트 옵션과 다중 바이트 옵션이 있음

2. IP 주소 형식

[그림] IP 주소 형식



IP 주소 이용 시 네트워크 상의 유일한 호스트를 식별할 수 있을 뿐만 아니라 호스트가 있는 네트워크도 식별 가능하며, IP 주소는 클래스로 나뉘며, 하나의 네트워크에 속한 모든 호스트들은 동일한 prefix를 공유한다. 클래스(Class) A의 경우 한 네트워크 내에 많은 호스트에 주소를 할당, 클래스 C의 경우 이보다 적은 호스트에 주소 할당 가능, 클래스 D는 일대다 통신인 멀티캐스트 형태의 통신을 지원하기 위한 주소 형식이다. 멀티캐스트 그룹을 식별하는 멀티캐스트 주소를 이용하여 그 그룹에 속한 모든 호스트가 통신에 개입하는 방식이다.

【학습정리】

1. TCP/IP 계층 구조의 응용 계층(Application Layer)프로토콜에는 TELNET, FTP, TFTP, SMTP, MIME 등이 포함된다.
2. 전송 계층(Transport Layer)에는 TCP와 UDP(User Datagram Protocol)가 포함된다.
3. 인터넷 계층(Internet Layer) 프로토콜로는 주소 변환 프로토콜(ARP : Address Resolution Protocol), 역주소 변환 프로토콜(RARP : Reverse Address Resolution Protocol), 인터넷 제어 메시지 프로토콜(ICMP : Internet Control Message Protocol), 인터넷 그룹 메시지 프로토콜(IGMP : Internet Group Message Protocol) 등이 속한다.
4. 호스트-투-네트워크 계층(Host-to-Network Layer)에는 네트워크 사이의 데이터 전송의 순서를 기술을 하며, 호스트-투-네트워크 계층은 특정 프로토콜을 규정하는 것이 아니라, 모든 표준과 관련된 기술적인 프로토콜을 지원한다.