[기말고사 키워드] 컴퓨터네트워크

1. 프로토콜 [6-7주차]

프로토콜은 서로 다른 시스템에 있는 개체 간에 성공적으로 데이터를 전송하는 통 신 규약을 말한다. 개체에는 데이터베이스 관리 시스템, 전자우편 시스템, 사용자 프로그램 등이 포함되며, 시스템은 하나 이상의 개체를 보유한 컴퓨터를 의미한다. 프로토콜은 계층적 구조로 정의되고 각 계층의 역할을 구분한다. 이는 편지 배달 과정을 편지를 써서 우체통에 넣는 단계, 편지를 수거하는 단계, 편지를 지역별로 구분하는 단계, 지역별로 차량에 싣는 단계 등으로 세분하는 것에 비유할 수 있다.

프로토콜은 시스템 간의 통신과 관련된 복잡한 상호 작용을 세분하여 계층화한 것 이기 때문에 이해하기 쉽고, 각 계층 간 표준 인터페이스가 정의되어 있어 이 표준 만 따르면 다른 업체의 시스템과도 호환이 가능하다.

프로토콜은 두 나라 간의 의정서 또는 의례에서 유래된 용어로, 네트워크에서 통신하려는 두 시스템 간에 무엇을, 언제, 어떻게 통신할 것인지 미리 정해놓은 약속이다.

2. TCP/IP 4 Layer 구조 [6-7주차]

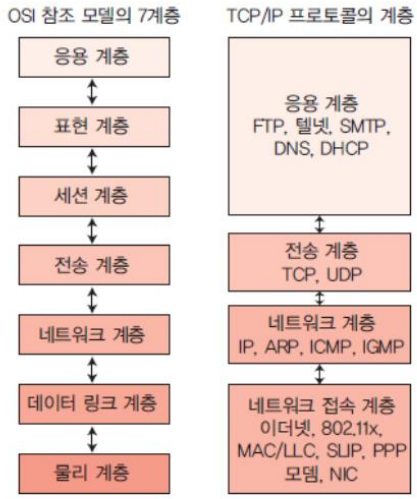

그림 5-2 OSI 참조 모델의 7계층과 TCP/IP 프로토콜의 계층

TCP/IP 프로토콜은 네트워크 접속 계층, 네트워크 계층, 전송 계층, 응용 계층으로 구성

네트워크 접속 계층

– TCP/IP의 경우 하위 계층인 물리 계층과 데이터 링크 계층을 특별히 정의하지 않았으며, 단지 모든 표준 및 임의 네트워크를 지원할 수 있도록 하고 있다. 네트워크 접속 계층은 운영체제의 네트워크 카드와 디바이스 드라이버를 지원하는 계층이다. 데이터 링크 계층의 역할을 하는 TCP/IP 프로토콜에는 이더넷, 802.11x, MAC/LLC, SLIP, PPP 등이 있

다.

– 네트워크 접속 계층의 송신 측 컴퓨터에서는 상위 계층으로부터 전달받은 패킷에 물리 주소 인 MAC 주소 정보가 있는 헤더를 추가해서 프레임을 만들어 하위 계층인 물리 계층에 전달한다. 수신 측 컴퓨터는 데이터 링크 계층에서 추가한 헤더를 제거하고 상위 계층인 네트워크 계층에 전달한다. 이때 프레임의 크기는 네트워크 토폴로지가 결정한다.

네트워크 계층

– 네트워크 계층은 인터넷 계층이라고도 하며, 네트워크의 패킷 전송을 제어한다. 네트워크 계층 프로토콜은 IP, ARP, ICMP, IGMP이다.

– 네트워크 계층의 역할은 데이터그램을 정확한 수신지로 전송하는 것이며, 여기서 데이터그램은 IP 프로토콜에서 다루는 패킷 데이터를 말한다. 데이터그램에 있는 정보는 송신지 주소 와 수신지 주소, 보내는 데이터, 몇 가지 제어 필드 등이다

– 네트워크 계층의 송신 측 컴퓨터에서는 상위 계층으로부터 전달받은 패킷에 논리 주소인 IP 주소를 포함한 헤더를 추가하여 하위 계층인 네트워크 접속 계층에 전달한다. 또한 수 신 측 컴퓨터에서는 하위 계층으로부터 전달받은 프레임의 헤더 정보를 확인한 후 송신 측 컴퓨터의 네트워크 계층에서 추가한 헤더를 제거하고 상위 계층인 전송 계층에 전달한다

전송 계층

– 상위 계층에서 볼 때 전송 계층은 호스트 간의 데이터 전송을 담당하는 계층으로, TCP와 UDP 프로토콜을 사용한다. 전송 계층의 역할은 네트워크 양단의 송수신 호스트 간에 신뢰 성 있는 전송 기능을 제공하는 것이며, OSI 참조 모델의 세션 계층 일부와 전송 계층이 이에 해당한다.

– 전송 계층의 송신 측 컴퓨터에서는 상위 계층으로부터 전달받은 데이터를 효율적으로 전송하기 위해 패킷 단위로 분할한다. 또한 수신 측 컴퓨터에서는 하위 계층으로부터 전달받은 패킷을 원래의 데이터로 재결합한다. 수신 측 컴퓨터의 동작은 다음과 같다.

» 송신 측 컴퓨터에서 패킷을 생성할 때 TCP를 이용하면 해당 패킷에 TCP 헤더 정보가 포함되고, UDP를 이용하면 해당 패킷에 UDP 헤더 정보가 포함된다.

» 수신 측 컴퓨터는 전송받은 패킷의 헤더 정보를 통해 TCP를 이용하여 만든 패킷인지, 아니면 UDP를 이용하여 만든 패킷인지 알아낸다. 그리고 TCP 패킷이면 TCP 프로토콜을 사 용하여 재결합하고, UDP 패킷이면 UDP 프로토콜을 사용하여 재결합한다.

응용 계층

– TCP/IP 프로토콜의 범위에는 응용 계층의 프로토콜까지 포함되며, 이러한 프로토콜은 FTP(파일 전송), SMTP(이메일), SNMP(네트워크 관리) 등이다. TCP/IP 프로토콜을 이용한 응용 프로그램 중에서 우리가 직접 사용하는 인터넷 메일 프로그램(아웃룩 익스프레스)이나 웹 브라우저(인터넷 익스플로러) 등을 응용 계층으로 분류할 수 있다.

– TCP/IP 프로토콜을 지원하려면 서버 컴퓨터에 프로토콜을 서버 형태로 서비스하는 '데몬 Damon'이라는 프로그램이 있어야 한다. 또한 서버 프로그램과 연동하여 작업을 수행하는 원격지의 프로그램을 클라이언트라고 하며, 하나의 서비스를 제공하려면 클라이언트의 요청을 처리하는 서버 프로그램, 즉 데몬이 필요한데, 이러한 관계를 보통 '클라이언트/서버 시스템'이라고 한다.

3. 데이터 전달 방식

데이터 전달 방식에 대한 개념은 연결형 통신과 비연결형 통신으로 나뉘며 다음과 같이 설명할 수 있습니다:

- 연결형 통신: 데이터를 신뢰성 있게 순차적으로 전달하기 위해 논리적인 연결을 확립하고 전송하는 방식으로 TCP(Transmission Control Protocol)가 대표적입니다. 오류 제어와 재전송 기능을 통해 데이터의 신뢰성을 보장합니다.
- 비연결형 통신: 연결 절차 없이 데이터를 빠르게 전송하는 방식으로 UDP(User Datagram Protocol)가 이에 해당합니다. 데이터의 신뢰성은 보장되지 않지만, 전송 속도가 빠르다는 장점이 있습니다.

이 두 방식은 **전송 계층(Transport Layer)**에서 이루어지며, TCP는 신뢰성을 우선시하는 반면, UDP는 효율성과 속도를 중시합니다.

4. FTP 서비스 동작방식

FTP는 인터넷에서 파일을 전송하는 기본 프로토콜으로, 파일을 전송하는 접속 대상인 컴퓨터를 서버라 하고, 접속하려는 사용자의 컴퓨터를 클라이언트라한다. FTP를 통해 데이터에 연결할 때는 포트 번호 20을 사용하고, 웹 페이지에 연결할 때는 포트 번호 21을 사용한다. 클라이언트와 서버는 제어 프로세스 속에서 FTP 명령을 주고받으며 동작하게 된다. 이때 인바운드 패킷과 아웃바운드 패킷이 사용되기도 하며, 인바운드는 화이트 리스트 필터링, 아웃바운드 패킷은 블랙 리스트 필터링을 사용한다.

5. OSI 7 Layer 네트워크 계층, 전송계층 [8주차 – 네트워크, 9주차 - 전송]

서로 다른 네트워크 간의 통신을 가능하게 하는 것이 네트워크 계층이고, 네트워크 계층을 통해 다른 네트워크로 데이터를 전송하려면 라우터라는 네트워크 접속 장치가 필요하

다. OSI 참조 모델 7계층 중 네트워크 계층은 세 번째 계층으로, 패킷을 송신 측에서 수신 측으로 전송한다. 전송계층은 프로토콜(TCP, UDP)과 관련된 계층으로 오류 복구와 흐름 제어 등을 담당하며, 두 시스템 간에 신뢰성 있는 데이터를 전송한다. OSI 참조 모델 7계층 중 전송 계층은 네 번째 계층으로 시스템 종단 간에 투명한 데이터를 양방향으로 전송하는 계층이다.

6. ARP 프로토콜 동작방식

논리 주소인 IP 주소를 물리 주소인 MAC 주소로 매핑하는 주소 변환 프로토콜이다. ARP Request (브로드캐스트)와 ARP Reply(유니캐스트)로 동작되고 ARP 요청은 LAN에 연결되어 있는 모든 컴퓨터 중에 "이 IP주소를 사용하는 컴퓨터가 있다면 MAC 주소를 알려주세요." 라고 전체 컴퓨터에 요청하는 것이며, ARP 응답은 ARP요청에 대해 "내가 그 IP주소를 사용하는 컴퓨터입니다. 나의 MAC주소를 알려줄게요." 라고 응답하는 것이다.

7. TCP/IP 주소의 구조

TCP/IP 주소는 물리 주소, 인터넷 주소 (IP), 포트 주소로 구성된다. 물리 주소는 MAC 주소로도 불리며 이더넷 카드에 개별적으로 부여되는 고유한 식별 번호이다. 인터넷 주소는 물리 주소와는 별도로 인터넷에서 호스트를 식별할 수 있는 32비트 주소 체계이다. 또한 인터넷 주소를 IP 주소를 중복해서 사용할 수 없다. 포트 주소는 동시에 발생하는 프로세스를 처리하기 위한 식별 주소의 역할을 한다.

8. 방화벽

방화벽은 외부 네트워크에서 내부 네트워크로 접근하기 위해서는 반드시 방화벽을 통과하도록 하여 내부 네트워크의 자원 및 정보를 보호하는 시스템이다. 불법적인 트래픽을 거부하거나 막을 수 있으며, 투명성을 보장하지는 않는다. 방화벽은 네트워크 정책, 방화벽 사용자 인증 시스템, 패킷 필터링, 응용 계층 게이트웨이로 구성된다.

9. 네트워크 관리 기능 5가지

네트워크 관리 기능에는 네트워크 구성 요소에 문제가 발생하거나 비정상적으로 작동할 때 이를 검출하여 수정하는 장애 관리, 네트워크 구성에 관한 정보를 수집하고 이러한 정보를 바탕으로 하는 구성 관리, 성능 저하가 장애로 이어지지 않도록 방지하는 성능 관리, 네트워크 자원에 접근하는 사용자의 권한을 관리하는 계정 관리, 위험을 방지하여 네트워크 관리가 올바로 이루어지게 하는 보안 관리 기능이 있다. 이들은 네트워크 관리 도구와 함께 사용되기도 한다.

10. 네트워크 보안 위협

송신 측에서 수신 측에 메시지를 전송할 경우에 네트워크의 보안 위협에는 다음이 있을

수 있다. 전송 차단, 가로채기, 변조, 위조.

네트워크 위협에는 SMS에 피싱 URL을 첨부하여 공격하는 스미싱과 시스템을 잠그거나 데이터를 암호화하고 이를 인질로 금전을 요구하는 랜섬웨어, 보안 설정이 안되어 있는 무선 LAN을 외부에서 공격하는 공유기 보안 위협이 있다. 이 외에도 DDos, Malware 등도 위협이 될 수 있다.

11. TCP 프로토콜

TCP (Transmission Control Protocol)는 전송 계층의 연결 지향형 프로토콜로, 3-way handshake를 통해 연결을 설정한 후 데이터를 전송하며, 패킷의 순서 보장, 오류 검출 및 재전송, 흐름 제어(수신 버퍼에 맞춘 전송)와 혼잡 제어(네트워크 상태 기반 전송 조절)를 통해 신뢰성 있고 안정적인 통신을 제공하고, 주로 HTTP, FTP, SMTP 등 신뢰성이 필요한 애플리케이션에서 사용된다.

12. 로컬통신과 원격통신 차이 및 관련 Layer

로컬 통신은 동일한 네트워크 또는 물리적 범위 안에서 통신이 이루어지는 경우로 일반적으로 **LAN (Local Area Network)** 환경에서의 통신을 의미한다. 원격 통신은 물리적 거리와 상관없이 네트워크를 통해 먼 위치의 장치들 간의 통신이 이루어지는 경우로 주로 **WAN (Wide Area Network)** 또는 **인터넷**을 기반으로 한다. 로컬 통신에는 OSI 7 Layer에서 1~3계층이, 원격 통신에는 3~7계층이 관련되어 있다.

13. well-known port 종류 10가지

POP3 (110번), FTP (20번 ,21번), HTTP (80번), 텔넷 (23번), SMTP (25번), IMAP (143번), DHCP (67, 68번), SNMP (161번), SSH (22번), RPC (111번), BOOTP