Week 5_ 계층별 프로토콜

Refactoring Study
20.04.11 Kwon Moonjeong

계층 별 프로토콜 (포트번호 무조건 외우기~~)

1-1. 응용 계층 프로토콜 - HTTP, HTTPS

- **HTTP(HyperText Transfer Protocol)**

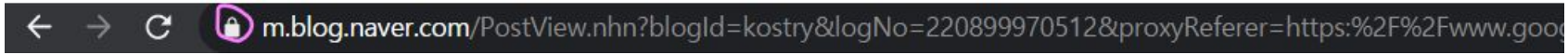
- WWW(World Wide Web) 상에서 정보를 주고 받을 수 있는 프로토콜 (평문으로)
- 주로 **HTML문서**를 주고 받는 데에 쓰이고, **TCP와 UDP를 사용**한다.
- **80번 포트**

- **HTTPS(HyperText Transfer Protocol over Secure Socket Layer)**

- HTTP에 **SSL(Secure Socket Layer)프로토콜** 로 **보안 기능을 추가**한 것. **(443번 포트)**

* **SSL(Secure Socket Layer)** : 인터넷 상에서 정보를 암호화하는 프로토콜

- HTTPS는 **http 메세지(text)를 암호화**하는 것이다. -> **공개키 암호화 방식**
- HTTPS의 **S는 Secure Socket, 보안 통신망**
- 속도가 느려서 모든 사이트에 사용 X, 결제창 등 정보 보호가 필요한 페이지에만 사용



1-2. 응용 계층 프로토콜 - SMTP, POP3, IMAP

	SMTP(Simple Mail Transfer Protocol)	POP3	143
설명	이메일 보낼 때 사용되는 기본 프로토콜**(발송)** **서버로 보냄**	서버-클라이언트간 통신 프로토콜로, 클라이언트에서 서버에 있는 메일을 다운받아 읽도록 해주는 프로토콜 **(수신, 서버->클라이언트)**	POP3의 대체재
특징	클라이언트-서버간 통신, 서버-서버간 통신을 모두 담당	- 구현이 쉽다. 많은 클라이언트에서 지원한다. - **서버로부터 메일을 가져온 후 삭제**한다. 서버에선 더이상 메일 확인 불가	- 메일을 가져와도 **서버에 메일이 그대로 남아있다.** - 서버 트래픽이 많이 쓰인다. -> 보안상 취약
포트 번호	25번	110번	143번

1-3. 응용 계층 프로토콜 - FTP

- **컴퓨터 간 파일을 전송**하는데 사용되는 프로토콜
  : FTP를 이용하면 사용자가 원하는 프로그램이나 각종 데이터를 무료나 저렴한 가격에 살 수 있다.

- **원격 host로 파일을 송수신**
  : 원격 host를 이용할 수 있는 사용자 ID와 Password가 있어야 원하는 원격 host에 접속이 가능.

- FTP Client 프로그램은 여러 파일을 연속으로 송수신해야 하기에,
Server와의 지속적인 응답 메시지 전송을 통해 **연결 상태(세션)을 유지**한다

FTP 프로토콜의 포트	
데이터 전송 포트 : 실제 파일 전송	**데이터 제어(명령) 포트 : 서비스 요청 및 결과 통보**
- 실제 파일 송수신 작업(올리기, 내려받기) 20번 포트	사용자 계정 및 암호 등의 정보나 파일 전송 명령 및 결과 21번 포트

1-4. 응용 계층 프로토콜 - TELNET, SSH

	TELNET	SSH(Secure Shell)
공통점	- **원격 제어** : 네트워크 상의 다른 컴퓨터에 로그인하거나, 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해 주는 응용 프로그램 또는 그 프로토콜 - 프로그램을 실행하는 등 시스템 관리 작업을 할 수 있는 **Virtual Terminal** 기능 수행	
차이점	- 정보 송수신 : **byte스트림** 형식 평문으로 전송 - **보안문제로 사용이 감소**하고 있으며, 원격제어를 위해 **SSH로 대체**	다른 사용자가 세**션을 엿듣지 못하도록 세션을 감싸주는** 텔넷 응용프로그램 : **패스워드가 암호화** 되어서 전송되기 때문에 보안에 적합 (DES, RSA) * DES(Data Encryption Standard) : 데이터 암호 표준. 개인키 사용. * RSA : 공개키 암호 시스템 중 하나. 전자서명 가능
포트 번호	23번	22번

1-5. 응용 계층 프로토콜 - DNS, SNMP

- **DNS(Domain Name System)**

- **도메인 네임을 IP 주소로 Mapping** 하는 시스템

- **SNMP(Simple Network Management Protocol)**

- 간이 **네트워크 관리** 프로토콜.
- IP 네트워크상의 장치로부터 정보를 수집 및 관리하거나, 그 정보로 장치의 동작을 변경한다
- 장비 상태 체크, 수집한 정보로 **통계**를 내준다
- 긴급한 문제 발생 -> **트랩 메시지 발송** : 162번 포트
- 평상시 : 161번 포트

2. 표현 계층 프로토콜 - SSL, ASCII

- **SSL(Secure Socket Layer)**

- 네트워크 레이어의 **암호화** 방식
- HTTP 뿐만 아니라, NNTP, FTP 등에도 사용
- **인증, 암호화, 무결성** 보장하는 프로토콜
- 포트 번호 : 443번 (=HTTPS의 포트 번호)

- **ASCII(American Standard Code for Information Interchange)**

- 문자를 사용하는 많은 장치에서 사용되며, 대부분의 **문자 인코딩**이 아스키에 기반
- 7비트 인코딩, 33개의 출력 불가능한 제어 문자들과 공백을 비롯한 95개의 출력 가능한 문자

3. 세션 계층 프로토콜 - NetBIOS, RPC, WinSock

- **NetBIOS**

- **네트워크의 기본적인 입출력**을 정의한 규약

- **RPC(Remote Procedure Call)**

- Windows 운영 체제에서 사용하는 **원격 프로시저 호출** 프로토콜

- **WinSock(Windows Socket)**

유닉스 등에서 **TCP/IP 통신시 사용하는 Socket을 Windows에서 그대로 구현**한 것

4. 전송 계층 - TCP, UDP

- **TCP(Transmission Control Protocol)**

- 전송 제어 프로토콜, 네트워크의 정보전달을 통제하는 프로토콜
- **데이터의 전달을 보증하고(신뢰성 있음) 보낸 순서대로 받게 해줌(순서 보장)**
- **3 Way Handshaking와 4 Way Handshaking** 등을 활용한 신뢰성 있는 전송 가능

- **UDP(User Datagram Protocol)**

- **비연결성이고 신뢰성이 없으며, 순서화되지 않은 Datagram 서비스 제공**
- TCP는 신뢰성이 낮은 프로그램에 적합

5-1. 네트워크 계층 - IP, IGMP, ARP, RARP

- **IP(Internet Protocol)**

- **패킷 교환 네트워크에서 정보를 주고받는데 사용**하는 정보 위주의 규약
- 전송할 데이터에 **주소 지정, 경로 설정, 패킷 분할 및 조립**
- **데이터그램 방식 (비연결형, 신뢰성 보장 X)**

- **IGMP(Internet Group Management Protocol)**

- 인터넷 그룹 관리 프로토콜
- **IP 멀티캐스트**를 실현하기 위한 통신 프로토콜
- PC가 멀티캐스트로 통신할 수 있다는 것을 라우터에 통지/멀티캐스트 그룹 유지

- **ARP(Adress Resolution Protocol)**

- 주소 분석 프로토콜
- 호스트의 **IP 주소를** 호스트와 연결된 네트워크 접속 장치의 **물리적 주소 (MAC Adress)로 바꾼다**

- **RARP(Reverse Adress Resolution Protocol)**

- 역 주소 분석 프로토콜
- ARP와 반대로 **물리적 주소를 IP 주소로 변환**

5-2. 네트워크 계층 - ICMP

- 인터넷 제어 메시지 프로토콜, 헤더는 8Byte
- TCP/IP에서 IP 패킷을 처리할 때 발생되는 오류 보고/처리, 전송 경로 변경 등을 위한 제어 메시지 관리

에러 메시지_1) Destination Unreachable 중요!!

: 이 에러 메시지는 라우터가 원격 시스템으로 가는 경로를 찾지 못한 경우,
목적지 시스템의 특정 포트 번호가 현재 응답할 수 없는 경우,
그리고 기타 여러 가지 문제가 발생한 경우에 생성

- **Network Unreachable :** 라우팅 테이블에서 목적지 네트워크를 위한 경로를 찾지 못한 경우
- **Host Unreachable :** IP 데이터그램이 최종 목적지 시스템에 전달되지 않음
- **Protocol Unreachable :** 목적지 시스템에서 특정 전송 프로토콜을 사용할 수 없음
- **Port Unreachable :** 목적지 시스템에서 특정 목적지 포트 번호가 사용되지 않음

에러 메시지_2) Source Quench 에러 메시지

: 송신 시스템이 목적지 호스트에서 처리하기에 **너무 많은 데이터를 전송**하면,
목적지 시스템은 송신 시스템에 ICMP Source Quench 에러 메시지를 전송하여 **전송 속도를 줄일 것을 요구**한다.
WHY? : 송신 시스템이 전송 속도를 늦추지 않으면 일부 패킷이 혼잡으로 인하여 분실될 가능성이 높다.

5-2. 네트워크 계층 - ICMP

에러 메시지_3) Time Exceeded 에러 메시지 중요!!

: 포워딩이나 재배열 작업이 너무 오래 걸려 보고하는 장비가 데이터를 소멸시킴

- Time-to-Live Exceeded in Transit : IP 데이터그램이 최종 목적지에 전달되기 이전에
  데이터그램의 활성화 시간 (Time-to-Live) 값이 0에 도달하였을 때 사용된다.

* Time-to-Live 필드가 데이터그램이 거칠 수있는 최대 단계의 수를 나타내므로
  라우터는 활성화 시간 값이 0인 데이터그램을 전달하지 못하며, 대신 데이터그램을 소멸시켜야 한다.

- Fragment Reassembly(리엄셈블리) Time Exceeded : 이 에러 메시지는 데이터그램이 분열되었으나,
  목적지 시스템이 주어진 시간(Unix에서는 대부분 60초로 설정되는)안에 모든 조각을 수신하지 못했을 때 사용된다.

어떤 조각이 전송 과정에서 분실되었으며, 목적지 시스템은 현재가지 수신한 모든조각을 소멸시킨다는 의미를 갖는다.

5-2. 네트워크 계층 - ICMP

에러 메시지_4) Redirect 에러 메시지 중요!!:
Redirect 에러 메시지는 라우터가 송신 시스템에서 특정 목적지로 가는 데 짧은 경로를 알리고자 할 때마다 사용된다.
여러 개의 라우터가 존재하는 네트워크에서 사용자가 하나의 기본 경로만을 정의한 다음,
기본 라우터 외의 다른 라우터를 통해 특정 네트워크에 데이터그램을 전송하는 경우에 나타난다.
사용자가 '더 나은' 라우터로 데이터그램을 전송하지 않으면,
기본 라우터는 Redirect(리다이렉트)에러 메시지를 통해 송신 시스템에 사용되어야 할 올바른 라우터를 알려준다.

- Redirect for Destination Network : 특정 목적지 네트워크를 위한 모든 트래픽이 다른 라우터를 통해 전송되어야 할 때 사용된다.
- Redirect for Destination Network Based on Type-of-Service : 송신 시스템이 어떤 목적지를 위해 특정한 서비스 종류를 요구하고, 목적지 네트워크를 위한 트래픽 가운데 그 서비스 종류를 가진 것이 다른 라우터를 통해 전송되어야 하는 경우에 사용된다.

에러 메시지_5) Parameter Problem
: IP 데이터그램 자체에 문제가 있어 소멸된다는 것을 나타낸다.
Parameter Problem 오류는 항상 IP옵션을 잘못 사용한 경우에 나타난다.

6. 데이터 링크 계층

- **Ethernet**

- 비연결성(connectionless)모드, 전송속도 10Mbps 이상, LAN 구현 방식

- **HDLC(High-Level Data-Link Control)**

- 고속 데이터 전송에 적합, 비트 전송을 기본으로 하는 범용의 데이터 링크 전송 제어절차

- **PPP(Point-to-Point Protocol)**

- 전화선 같이 양단간 비동기 직렬 링크를 사용하는 두 컴퓨터간의 통신을 지원하는 프로토콜
- 두 대의 컴퓨터가 직렬 인터페이스를 이용하여 통신을 할 때 필요한 프로토콜

7. 물리 계층

- **RS-232**

- 보통 15m이하 단거리에서 38400bps까지 전송을 위한 직렬 인터페이스

- **X.25 / X.21**

- X.25는 패킷교환망, X.21은 회선교환망에 대한 액세스 표준

References

- **네트워크 계층별 프로토콜(Layer Protocol)** https://needjarvis.tistory.com/158, 시나공 정보처리기사 필기2
- **HTTPS** https://jeong-pro.tistory.com/89
- **SNMP, SSH** 위키피디아
- **SMTP, POP3, IMAP 메일 관련 프로토콜** https://raisonde.tistory.com/entry/SMTP-POP3-IMAP-메일-관련-프로토콜
- **ICMP 오류 메세지의 종류** https://raisonde.tistory.com/entry/ICMP-%EC%98%A4%EB%A5%98-%EB%A9%94%EC%84%B8%EC%A7%80%EC%9D%98-%EC%A2%85%EB%A5%98