

전송계층에서 대표적으로 사용되는 프로토콜은 TCP와 UDP이다.

이들 프로토콜은 응용계층 프로토콜을 지원하는 다양한 기능들을 포함하고 있다.

UDP를 사용하는 응용서비스프로토콜 2개, TCP를 사용하는 응용서비스프로토콜 2개를 조사하여

각 프로토콜의 기능에 대해서 설명하시오.

-----

1. TCP의 특징 TCP/IP는 가장 널리 사용되는 정보 전달을 해주는 연결형 프로토콜이다. 널리 사용되는 만큼 가장 신뢰성이 높고 다양한 운영 체제의 네트워킹을 제공한다. TCP/IP는 패킷 교환 방식을 사용하는데, 이 프로토콜을 사용하고 있는 사용자간에 데이터 교환이 가능하다. 일반적으로 TCP는 전자메일이나 www 서비스에서 사용되는데, 출발지 호스트의 포트에서 목적지 호스트의 포트에 데이터 스트림을 전달하는 프로토콜로 응용 프로그램과 IP 사이에서 매개체로 동작한다. TCP는 두 호스트 사이의 데이터 동시 전송이 가능한 양방향 통신을 지원하며, TCP를 사용한 대표적인 응용 프로토콜로는 FTP, telnet, SMTP, HTTP 등이 있으며 각각의 포트 번호를 사용한다. 또한 사용하는 응용 프로그램의 데이터 스트림을 세그먼트로 구성하는데, 데이터 스트림이 하나의 세그먼트로 구성하기 적절하지 않을 경우에는 여러 개의 세그먼트로 나누어 각각의 세그먼트에 번호를 부여한다.

#### 1-1 TCP 프로토콜(SSH)

시큐어 셸(Secure SHell, SSH)은 네트워크 상의 다른 컴퓨터에 로그인하거나 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해 주는 응용 프로그램 또는 그 프로토콜을 가리킨다. 기존의 rsh, rlogin, 텔넷 등을 대체하기 위해 설계되었으며, 강력한 인증 방법 및 안전하지 못한 네트워크에서 안전하게 통신을 할 수 있는 기능을 제공한다. 기본적으로는 22번 포트를 사용한다.

SSH는 암호화 기법을 사용하기 때문에, 통신이 노출된다고 하더라도 이해할 수 없는 암호화된 문자로 보인다.

SSH는 버클리 서비스들(rsh, rcp, rlogin, rexec) 및 telnet, ftp 서비스를 좀 더 보안이 강화된 명령으로 대체하기 위해 만들었다. 1995년 핀란드의 Tatu Ylönen이 개발해 공개했고, 많은 반향을 일으켰다. 1995년 말 Ylönen은 SSH Communications Security사를 설립하고, 상용화되었다. 소스 코드는 공개되었지만 여러 가지 제약이 있었다고 하는데, 이에 SSH 1.2.12 릴리즈를 기반으로 OpenSSH 프로젝트가 결성되고 BSD 라이선스로 개발하기 시작했다. OpenSSH가 처음 선보인 건 1999년 OpenBSD 2.6 릴리즈부터이다. 이후 계속 보완되어 오늘날에 이르게 되었다.

#### 1-2 TCP 프로토콜(HTTP)

HTTP(HyperText Transfer Protocol)는 W3 상에서 정보를 주고받을 수 있는 프로토콜이다. 주로 HTML 문서를 주고받는 데에 쓰인다. 주로 TCP를 사용하고 HTTP/3부터는 UDP를 사용하며, 80번 포트를 사용한다. 1996년 버전 1.0, 그리고 1999년 1.1이 각각 발표되었다.

HTTP는 클라이언트와 서버 사이에 이루어지는 요청/응답(request/response) 프로토콜이다. 예를 들면, 클라이언트인 웹 브라우저가 HTTP를 통하여 서버로부터 웹페이지(HTML)나 그림 정보를 요청하면, 서버는 이 요청에 응답하여 필요한 정보를 해당 사용자에게 전달하게 된다. 이 정보가 모니터와 같은 출력 장치를 통해 사용자에게 나타나는 것이다.

HTTP를 통해 전달되는 자료는 http:로 시작하는 URL(인터넷 주소)로 조회할 수 있다.

2. UDP의 특징 UDP는 실시간 전송이 요구되는 비 연결형 프로토콜이다. 주로 IP전화나 스트리밍 서비스 등에 사용되는데, 데이터의 안정된 전송을 보장하지는 못한다. 대부분 적은 양의 데이터를 전달하고자 할 때 사용되며 브로드캐스팅, 멀티캐스팅에 사용된다. UDP를 사용하는 응용 프로토콜로는 TFTP, SNMP 등이 있는데 연결 방식은 TCP와 달리 세션이 성립할 필요가 없으며 송신 호스트는 수신 호스트의 포트 정보를 포함한 UDP 패킷을 보낸다. 만약 발신 호스트의 응답이 필요하면 송신 호스트의 포트 정보를 포함시키기도 한다.

#### 2-1 UTP 프로토콜(DNS)

도메인 네임 시스템(Domain Name System, DNS)은 호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그 반대의 변환을 수행할 수 있도록 하기 위해 개발되었다. 특정 컴퓨터(또는 네트워크로 연결된 임의의 장치)의 주소를 찾기 위해, 사람이 이해하기 쉬운 도메인 이름을 숫자로 된 식별 번호(IP 주소)로 변환해 준다. 도메인 네임 시스템은 흔히 "전화번호부"에 비유된다. 인터넷 도메인 주소 체계로서 TCP/IP의 응용에서, www.example.com과 같은 주 컴퓨터의 도메인 이름을 192.168.1.0과 같은 IP 주소로 변환하고 라우팅 정보를 제공하는 분산형 데이터베이스 시스템이다.

인터넷은 2개의 주요 이름공간을 관리하는데, 하나는 도메인 네임 계층, 다른 하나는 인터넷 프로토콜(IP) 주소 공간이다. 도메인 네임 시스템은 도메인 네임 계층을 관리하며 해당 네임 계층과 주소 공간 간의 변환 서비스를 제공한다. 인터넷 네임 서버와 통신 프로토콜은 도메인 네임 시스템을 구현한다. DNS 네임 서버는 도메인을 위한 DNS 레코드를 저장하는 서버이다. DNS 네임 서버는 데이터베이스에 대한 쿼리의 응답 정보와 함께 응답한다.

#### 2-2 UTP 프로토콜(SNMP)

간이 망 관리 프로토콜(Simple Network Management Protocol, SNMP)은 IP 네트워크상의 장치로부터 정보를 수집 및 관리하며, 또한 정보를 수정하여 장치의 동작을 변경하는 데에 사용되는 인터넷 표준 프로토콜이다. SNMP를 지원하는 대표적인 장치에는 라우터, 스위치, 서버, 워크스테이션, 프린터, 모뎀 랙 등이 포함된다.

SNMP는 네트워크 모니터링의 목적으로 네트워크 관리에서 널리 사용된다. SNMP는 관리 정보 베이스(Management Information Base) 상에 관리 중인 시스템의 상태와 설정을 변수의 형태로 관리할 수 있게 해준다. 이러한 변수들은 관리 프로그램에 의해 원격에서 질의될 수 있으며, 경우에 따라서는 원격에서 값을 설정할 수도 있다.

현재 사용되는 SNMP의 주요 버전은 세 가지로, SNMPv1이 가장 초기 버전이며 이후 개발된

SNMPv2와 SNMPv3는 성능 및 유연성, 보안성 면에서 향상된 버전이다.

SNMP는 국제 인터넷 표준화 기구에 의해 정의된 인터넷 프로토콜 스위트의 일부분이다. 인터넷 프로토콜 스위트는 응용 계층 프로토콜, 데이터베이스 명세, 데이터 객체 집합 등을 포함하는 네트워크 관리용 표준들로 구성되어 있다.