### \*\*UDP 프로토콜\*\*

#### 정의

* User Datagram Protocol. IP를 사용하는 네트워크 내에서 컴퓨터들 간에 메시지들이 교환될 때 제한된 서비스만을 제공하는 통신 프로토콜

#### 특징

* 단순한 전송방식
* 비연결지향형
* 신뢰성이 낮음
* 오류의 검사와 수정이 필요 없는 프로그램에서 주로 사용

#### UDP를 사용하는 프로그램

* DNS 서버
* TFTP : FTP보다 간단한 네트워크 애플리케이션. 사용자 인증이 불필요하고, 디렉토리를 보여주지 않아도 되는 곳에 사용
* 동영상 스트리밍
* RIP(라우팅 정보 프로토콜) : 경유할 가능성이 있는 라우터를 홉수로 수치화하여, DVA(Distance Vector Algorithm)라는 알고리즘으로 인접 호스트와의 경로를 동적으로 교환하는 일

### \*\*UDP 프로토콜 구조\*\*

* Source Port(2byte) : 출발지 포트번호
* Destination Port(2byte) : 도착지 포트번호
* Length(2byte) : UDP프로토콜 헤더 + 페이로드 길이
* Checksum(2byte)

### \*\*TCP 프로토콜\*\*

#### 정의

* IP 네트워크의 두 컴퓨터 간의 연결 지향 통신을 위한 전송 계층 호스트 간 프로토콜

#### 특징

* 안정적, 순서대로, 에러없이 전송
* UDP보단 느림(체감할 수 있을 정도는 아님)

### \*\*TCP 프로토콜 구조\*\*

* Source Port(2byte) : 출발지 포트번호
* Destination Port(2byte) : 도착지 포트번호
* Sequence Number(4byte) : 데이터를 주고받을 때 사용하는 번호
* Acknowledgement Number(4byte) : 데이터를 주고받을 때 사용하는 번호
* Offset(0.5byte) : 헤더의 길이/4
* Reserved(0.5byte) : 예약된 필드로 사용하지 않음
* TCP Flags(1byte) : 플래그 세팅값에 따라 TCP의 기능이 달라짐
* C
* E
* Urgent : 해당 값이 1이면 처리 우선순위가 높음을 의미 / Urgent Pointer와 함께 사용
* (중요)Acknowledgement : 응답 플래그/승인을 해줄 때 사용하는 플래그
* Push : 버퍼가 채워지기를 기다리지 않고 받는 즉시 전달

버퍼링 없이 7 Layer Application Layer의 응용프로그램에게 바로 전달하는 플래그

* Reset : 비정상적인 세션을 끊기위해 연결을 재설정
* Synchronization : 통신 시작 시 세션을 연결하기 위한 플래그
* Finish : 더 이상 전송할 데이터가 없고 세션 연결을 종료시키겠다는 플래그

[참고](https://hongpossible.tistory.com/entry/TCP-Flag%EB%9E%80)

♨ 가상머신 포트포워딩

### TCP 통신과정

#### 3Way Handshake

* TCP 통신 전 프로세스를 연결하기 위해 수행되는 과정
* 최초의 Sequence number만 클라이언트와 서버 각각에서 랜덤으로 설정됨.
* 이후 동일한 규칙에 따라서 진행.

1.클라이언트->서버 요청패킷

Eth+IPv4+TCP(연결 수립 과정이기 때문에 페이로드는 딱히 없음)

Flag : SYN

Sequence Number:100(클라이언트 마음대로 랜덤세팅) Acknowledgement Number:0

2.서버->클라이언트 요청을 수락하는 패킷

Flag : SYN+ACK

S:2000(서버 마음대로 랜덤세팅) A:101(받은 Seq+1)

3.클라이언트->서버 최종 수락 패킷

Flag : ACK

S:101(받은 Ack) A:2001(받은 Seq+1)

위 단계로부터 연결 수립상태가 되고, 이후 데이터 송수신.

데이터 송수신 시에는

1.보낸 쪽에서 또 보낼 때는 S와 A번호가 그대로

Eth+IPv4+TCP+Data(100)

Flag : PSH + ACK

S:101 A:2001

2.받는 쪽에서 S번호는 받은 A번호가 된다

3.받는 쪽에서 A번호는 받은 Seq+페이로드 크기

Flag : PSH + ACK

S:2001 A:201

### TCP 상태전이도

#### TCP 연결 상태의 변화

* Listen : 서버 쪽에서 프로그램이 포트 번호를 사용하고있는 상태/클라이언트의 요청을 듣고있음
* Established : 연결이 서로 수립이 된 상태

3Way Handshake

1.클라이언트->서버 요청패킷

클라 : CLOSE -> SYN\_SENT

서버 : LISTENING -> SYN\_RECEIVED

2.서버->클라이언트 요청을 수락하는 패킷

클라 : SYN\_SENT

서버 : SYN\_RECEIVED

3.클라이언트->서버 최종 수락 패킷

클라 : SYN\_SENT -> ESTABLISHED

서버 : SYN\_RECEIVED -> ESTABLISHED

### \*\*NAT\*\*

#### 정의

Network Address Translation.IP 패킷의 TCP/UDP 포트 숫자와 소스 및 목적지의 IP 주소 등을 재기록하면서 라우터를 통해 네트워크 트래픽을 주고 받는 기술

#### 특징

* 사설IP를 공인IP로 변환 하는 데에만 사용하는 것은 아님
* 사설IP 대역 사이에서 통신할 때 공유기의 NAT테이블에 각 기기의 통신기록이 작성됨

### Port Forwarding

#### 정의

패킷이 라우터나 방화벽과 같은 네트워크 장비를 가로지르는 동안 특정 IP 주소와 포트 번호의 통신 요청을 특정 다른 IP와 포트 번호로 넘겨주는 NAT의 응용

#### 특징

TCP의 80번 포트와 UDP의 80번 포트는 다르다