

Chapter 06. TCP와 NAT

TCP & UDP 개요

목차

- Transport 계층
- TCP
- UDP
- 비교

Transport 계층

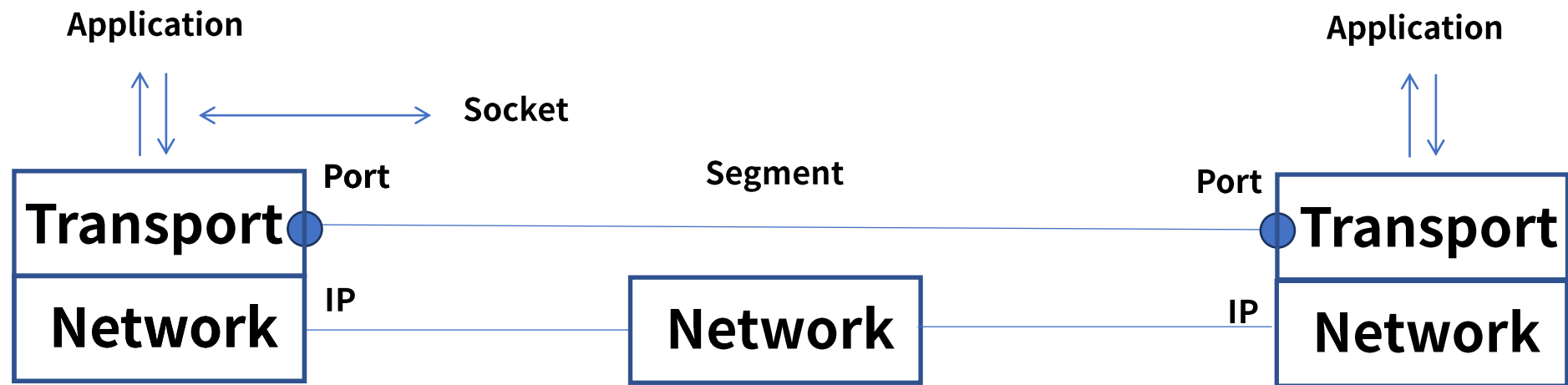
- 역할

End to End 서비스, 커넥션(연결)을 관리

Connection-oriented, Reliability, Flow control, Multiplexing

TCP & UDP, 소켓을 통한 프로세스별 통신

5 tuple = Source IP, Source Port, Dest IP, Dest Port, Protocol



Transport 계층

- Port

전송 계층에서 사용되며 특정 프로세스를 구분하는 단위

0 ~ 65535

0 ~ 1023: well-known port, 1024 ~ 49151: registered port, 49152 ~ 65535: dynamic port

웹 TCP 80, FTP TCP 21

Process
Port
TCP/UDP
IP

```
C:\Users\dkhan>netstat -an
```

활성 연결

프로토콜	로컬 주소	외부 주소	상태
TCP	172.20.10.2:53676	183.111.180.183:80	ESTABLISHED
TCP	172.20.10.2:54349	108.177.125.188:5228	ESTABLISHED
TCP	172.20.10.2:59419	211.115.106.80:80	ESTABLISHED
TCP	172.20.10.2:59450	13.114.157.190:80	ESTABLISHED
TCP	172.20.10.2:59451	13.114.157.190:80	ESTABLISHED
TCP	172.20.10.2:59789	211.115.106.205:80	CLOSE_WAIT
TCP	172.20.10.2:60216	104.244.42.2:443	ESTABLISHED
TCP	172.20.10.2:60217	104.244.42.65:443	ESTABLISHED
TCP	172.20.10.2:60226	151.101.228.157:80	TIME_WAIT

No.	Time	Source	Destination	Protocol	Length	Info
157	2.294829	183.111.180.183	172.20.10.2	TCP	54	80 → 53676 [ACK] Seq=104 Ack=43 Win=1432 Len=0
<						
> Frame 157: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B7158E2F-587B-4D49-AFAA-BA995AC18FAB}, id 0						
> Ethernet II, Src: 76:b5:87:75:83:64 (76:b5:87:75:83:64), Dst: 76:b5:87:57:3a:20 (76:b5:87:57:3a:20)						
> Internet Protocol Version 4, Src: 183.111.180.183, Dst: 172.20.10.2						
> Transmission Control Protocol, Src Port: 80, Dst Port: 53676, Seq: 104, Ack: 43, Len: 0						

TCP

- 정의

TCP(Transmission Control Protocol), 전송 제어 프로토콜

인터넷을 구성하는 핵심 프로토콜, 1981년 RFC 793 릴리즈

신뢰성을 기반으로 데이터를 에러 없이 전송, 1:1 통신

연결 지향, Connection-oriented, 패킷의 상태 정보를 확인하고 유지

에러 발생시 재전송을 요청하고 에러를 복구한다

Segment

TCP
header

Data

Packet

IP
header

Data

TCP

- 헤더 포맷
20바이트

		16	31
Source Port		Dest Port	
Sequence Number			
Acknowledgement Number			
HLEN	Reserved URG, ACK, PSH, RST, SYN, FIN	Window Size	
Checksum		Urgent Pointer	
Option & Padding			

TCP

- 헤더 포맷 - 상세

		16		31	
Source Port			Dest Port		
Sequence Number					
Acknowledgement Number					
HLEN	Reserved		Window Size		
		URG, ACK, PSH, RST, SYN, FIN			
Checksum			Urgent Pointer		
Option & padding					

1. Source & Dest Port: 소스 포트와 목적지 포트
2. Sequence Number: 순서 번호, 패킷 순서화와 중복 패킷 방지
3. Acknowledgement Number: 승인 번호, 수신측에서 수신 확인하고 다음 송신 데이터 요청
4. HLEN: 20 ~ 60
5. TCP 제어 플래그: TCP 회선 및 제어 관리
6. Window Size: TCP 흐름 제어, 수신 버퍼의 여유 용량을 통보
7. Checksum: 데이터 무결성 확인
8. Urgent Pointer: 긴급 데이터를 알림
9. Option & Padding: 옵션, MSS 조절이나 타임스탬프

TCP

- TCP 제어 플래그

6가지로 구성되며 활성화 되는 값을 비트 “1”로 표현

URG	ACK	PSH	RST	SYN	FIN
-----	-----	-----	-----	-----	-----

1. URG: 긴급함을 알림, 긴급 데이터로 우선 순위를 높여 먼저 송신
2. ACK: 확인, 수신측에서 송신된 패킷을 정상적으로 받았음을 알림
3. PSH: 버퍼링 되지 않고 바로 송신
4. RST: 비정상 상황에서 연결을 끊음
5. SYN: 연결을 맺기 위해 보내는 패킷 000010
6. FIN: 정상 종료, 송신측에서 수신측에 연결 종료 요청

UDP

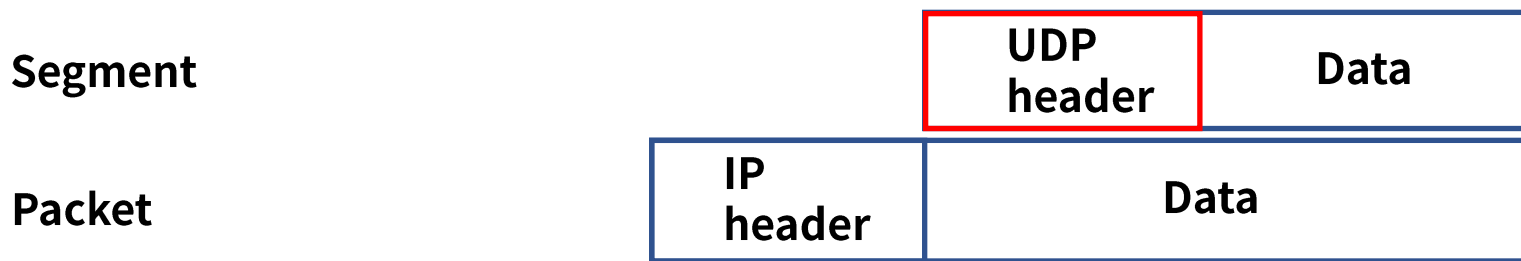
- 정의
UDP(User Datagram Protocol)

신뢰성은 낮으나 데이터 전송이 빠르다, 1980년 RFC 768 릴리즈

송신측은 일반적으로 데이터를 보내고 확인 안함, 1:n 통신 가능

Connectionless, 재전송 불가, 실시간 데이터 전송에 적합

스트리밍 서비스의 경우 전송 문제가 발생해도 재전송 보다는 실시간 데이터 전송이 중요



UDP

- 헤더 포맷

16		31	
Source Port		Dest Port	
Length		Checksum	

1. Source Port: 출발지 포트
2. Dest Port: 목적지 포트
3. Length: 전체 데이터 길이 (header + data)
4. Checksum: 데이터 무결성 확인

비교

• 헤더 포맷 - PCAP

▼ Transmission Control Protocol, Src Port: 56176, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

Source Port: 56176

Destination Port: 443

[Stream index: 11]

[TCP Segment Len: 0]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 1662365292

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 159938476

0101 = Header Length: 20 bytes (5)

> Flags: 0x010 (ACK)

Window size value: 514

[Calculated window size: 131584]

[Window size scaling factor: 256]

Checksum: 0x2f0f [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

> [SEQ/ACK analysis]

> [Timestamps]

▼ User Datagram Protocol, Src Port: 443, Dst Port: 59513

Source Port: 443

Destination Port: 59513

Length: 197

Checksum: 0xe6f2 [unverified]

[Checksum Status: Unverified]

[Stream index: 2]

> [Timestamps]

비교

- TCP & UDP

16		31	
Source Port		Dest Port	
Sequence Number			
Acknowledgement Number			
HLEN	Reserved URG, ACK, PSH, RST, SYN, FIN	Window Size	
Checksum		Urgent Pointer	
Option & Padding			

Source Port	Dest Port
Length	Checksum

	TCP 20 Byte	UDP 8 Byte
Protocol ID	6	17
순서 확인	가능	불가능
신뢰성	높음	낮음
연결성	Connection-oriented	Connectionless
제어	흐름 & 혼잡 제어 가능	없음
속도	느리다	빠르다

Wrap up

- Transport 계층은 소프트웨어 레벨로 End to End 서비스로 부르며 커넥션을 관리
- 대표적인 프로토콜로 TCP & UDP가 있으며 소켓을 통한 프로세스 별 통신
- 포트는 전송 계층에서 사용되는 특정 프로세스를 구분하는 단위로 범위는 0 ~ 65535 이다
- UDP(User Datagram Protocol)는 1980년 RFC 768 릴리즈, 1:n 가능 및 비 신뢰성 통신
- TCP(Transmission Control Protocol)는 1981년 RFC 793 릴리즈, 1:1 신뢰성 기반 통신

	TCP 20Byte	UDP 8Byte
Protocol ID	6	17
순서 확인	가능	불가능
신뢰성	높음	낮음
연결성	Connection-oriented	Connectionless
제어	흐름 & 혼잡 제어 가능	없음
속도	느리다	빠르다