

Chapter 06. TCP와 NAT

TELNET & SSH

목차

- TELNET
- SSH

TELNET

- 역할

원격지 호스트 컴퓨터에 접속하기 위해 사용되는 프로토콜

RFC 854, TCP 23번 사용, Terminal 에뮬레이터

장비 관리 또는 서버 접속 시 사용 - Shell - Command Line Interface

클라이언트 소프트웨어인 경우, 포트 테스트 용도로 많이 사용

```
dkhan@dkhan-VirtualBox:/$ telnet www.naver.com 80
Trying 23.51.28.215...
Connected to e6030.a.akamaiedge.net.
Escape character is '^['.
```

```
dkhan@dkhan-VirtualBox:/$ telnet www.naver.com 30000
Trying 23.51.28.215...
^C
```

해당 도메인 또는 IP 주소에 서비스 포트(서비스)가 열려 있는지 확인 가능

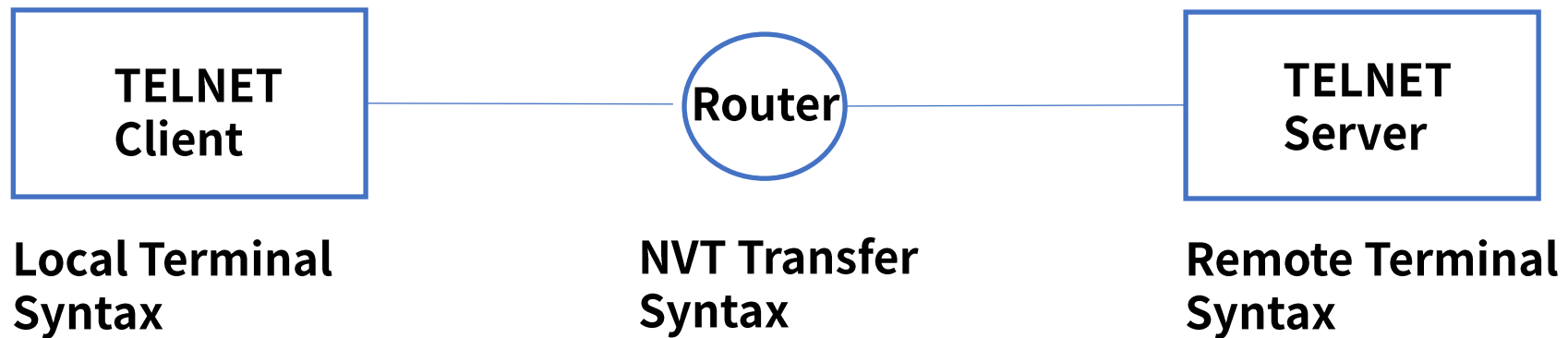
TELNET

- 기능

NVT(Network Virtual Terminals) 지원: 데이터 변환 가상 장치

협상 가능한 옵션

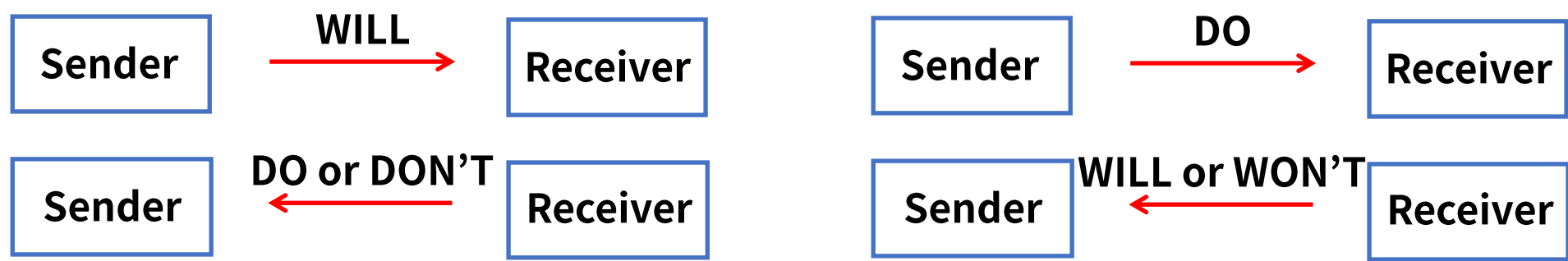
프로세스와 터미널의 1:1 symmetric 관계



TELNET

- Negotiation Commands

WILL -> 옵션 활성화를 원한다, WON'T -> 옵션 활성화를 원하지 않는다
DO -> 옵션 활성화를 요청한다, DON'T -> 옵션 활성화를 요청하지 않는다



1	scho	31	window size
3	suppress go ahead	32	terminal speed
5	status	33	remote floe control
6	timing mark	34	linemode
24	terminal type	36	environment variables

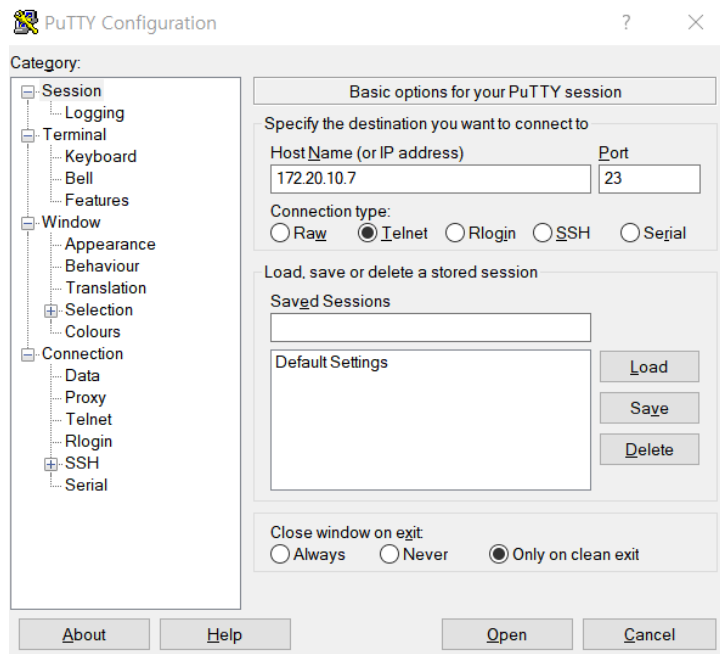
TELNET

- 접속 및 옵션 ID 협상 확인

원격지 IP:Port로 접속 시도 -> ID:Password 입력 -> 원격지 서버에 연결

윈도우 CMD 또는 리눅스 터미널에서 접속 가능

무료 오픈소스인 Putty 프로그램을 많이 사용

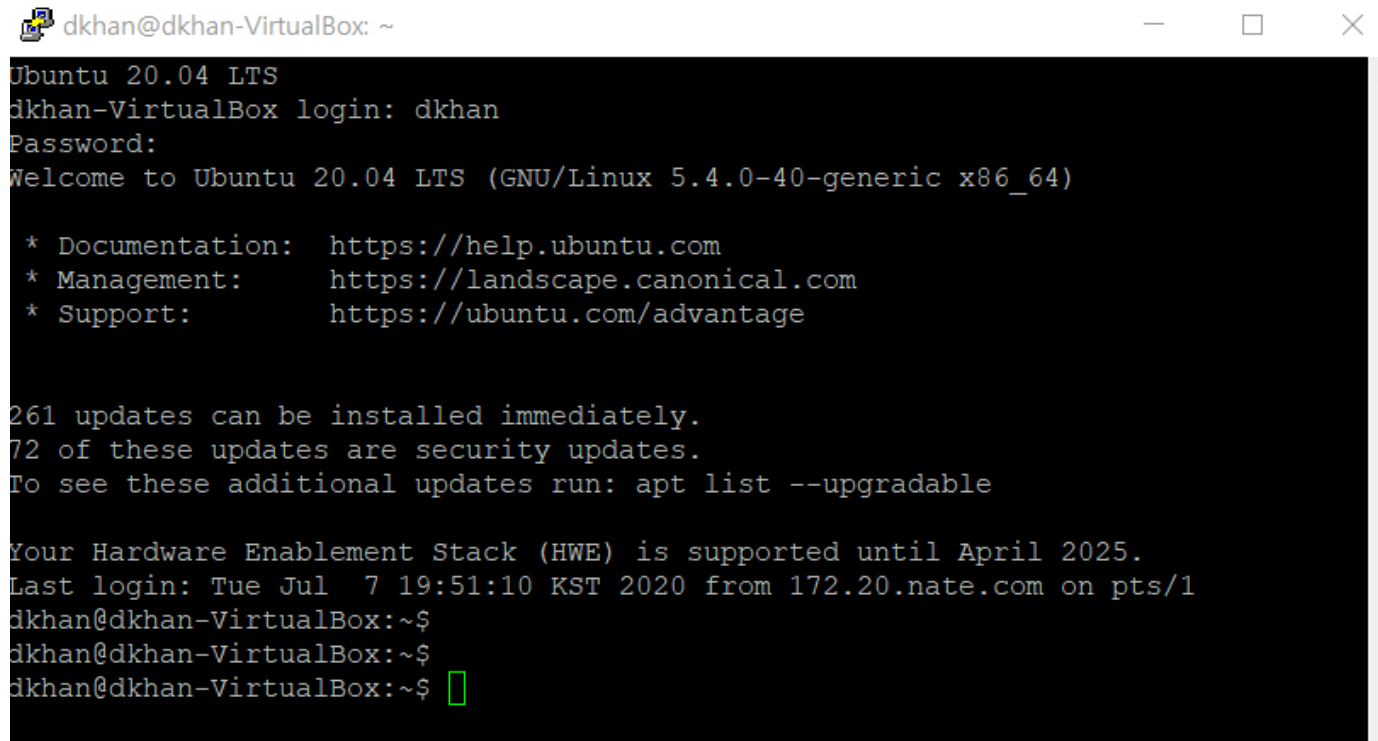


리눅스 셸에서 TELNET 옵션 협상 확인 - tcpdump

```
19:56:10.113808 IP 172.20.10.7.23 > 172.20.10.2.57405: Flags [P.], seq 43:52, a
ck 68, win 502, length 9 [telnet DO ECHO, WILL STATUS] DO LFLOW [telnet]
19:56:10.114608 IP 172.20.10.2.57405 > 172.20.10.7.23: Flags [P.], seq 68:71, a
ck 52, win 4106, length 3 [telnet WONT ECHO] [telnet]
19:56:10.114648 IP 172.20.10.7.23 > 172.20.10.2.57405: Flags [.], ack 71, win 5
02, length 0
19:56:10.114681 IP 172.20.10.2.57405 > 172.20.10.7.23: Flags [P.], seq 71:74, a
ck 52, win 4106, length 3 [telnet DONT STATUS] [telnet]
19:56:10.114688 IP 172.20.10.7.23 > 172.20.10.2.57405: Flags [.], ack 74, win 5
02, length 0
19:56:10.114701 IP 172.20.10.2.57405 > 172.20.10.7.23: Flags [P.], seq 74:77, a
ck 52, win 4106, length 3 [telnet WONT LFLOW] [telnet]
19:56:10.114704 IP 172.20.10.7.23 > 172.20.10.2.57405: Flags [.], ack 77, win 5
02, length 0
```

TELNET

- putty 프로그램을 통해서 접속된 화면



```
dkhan@dkhan-VirtualBox: ~  
Ubuntu 20.04 LTS  
dkhan-VirtualBox login: dkhan  
Password:  
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
261 updates can be installed immediately.  
72 of these updates are security updates.  
To see these additional updates run: apt list --upgradable  
  
Your Hardware Enablement Stack (HWE) is supported until April 2025.  
Last login: Tue Jul  7 19:51:10 KST 2020 from 172.20.nate.com on pts/1  
dkhan@dkhan-VirtualBox:~$  
dkhan@dkhan-VirtualBox:~$  
dkhan@dkhan-VirtualBox:~$
```

putty 다운로드

<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

SSH

- **역할**
Secure Shell

TELNET을 대체하기 위해 1995년 개발

원격지에 있는 컴퓨터를 명령어를 통해서 제어

강력한 인증 방법 및 암호화 통신을 제공, TCP 22

OpenSSH - 1999년 OpenBSD팀에서 개발 - GNU Public License

SSHv1, SSHv2

SSH

- **특징**

인증(Authentication): 사용자가 서버 접속시 패스워드 또는 공개키 기반의 인증 방식을 지원

암호화(Encryption): 대칭키 방식 사용 - AES, Blowfish, 3DES

무결성(Integrity): 데이터 위변조 방지 - MAC(Message Authentication Code)

압축(Compression), 다중화 통신

대칭키: 동일한 키로 암호화를 동시에 할수 있는 방식

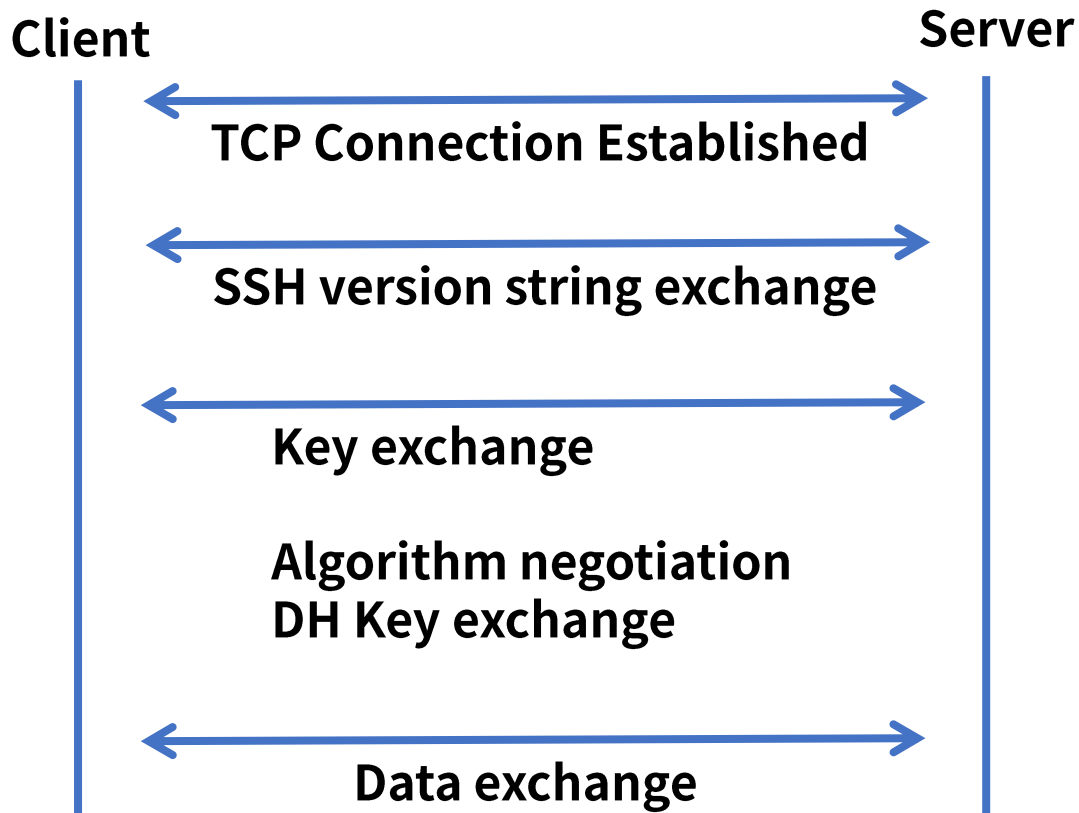
공개키(공개키 + 개인키)방식

공개키 암호화 -> 데이터 보안, 서버의 공개키로 데이터를 암호화 -> 서버의 개인키로 복호화

개인키 암호화 -> 인증 보안, 개인키 소유자가 개인키로 암호화 하고 공개키를 함께 전달
-> 암호화 데이터 + 공개키로 신원 확인 -> 전자서명 방법

SSH

- 통신 과정



```
ssh
Nc Tir Info
... Server: Protocol (SSH-2.0-PaloAltoNetworks_0.2)
... Client: Protocol (SSH-2.0-PuTTY_Release_0.61)
... Client: key Exchange Init
... Server: Key Exchange Init
... Client: Diffie-Hellman Group Exchange Request (Old)
... Server: Diffie-Hellman Group Exchange Group
... Client: Diffie-Hellman Group Exchange Init
... Server: Diffie-Hellman Group Exchange Reply
... Client: New Keys
... Server: New Keys
... Client: Encrypted packet (len=52)
... Server: Encrypted packet (len=52)
```

SSH

- 통신 과정

Client

Server



TCP Connection Established



SSH version string exchange



Key exchange

```
✓ SSH Protocol
  Protocol: SSH-2.0-PaloAltoNetworks_0.2
  [Direction: server-to-client]
```

```
✓ SSH Protocol
  Protocol: SSH-2.0-PuTTY_Release_0.61
  [Direction: client-to-server]
```

```
✓ SSH Protocol
  ✓ SSH Version 2 (encryption:aes256-ctr mac:hmac-sha1 compression:none)
    Packet Length: 636
    Padding Length: 6
    ✓ Key Exchange
      Message Code: Key Exchange Init (20)
      > Algorithms
      Padding String: a3de35238e24
    [Direction: client-to-server]
```

```
✓ SSH Version 2 (encryption:aes256-ctr mac:hmac-sha1 compression:none)
  Packet Length: 468
  Padding Length: 11
  ✓ Key Exchange
    Message Code: Key Exchange Init (20)
    > Algorithms
    Padding String: 000000000000000000000000
  [Direction: server-to-client]
```

SSH

- 통신 과정
Algorithm negotiation

▼ Algorithms

```
Cookie: 7c005f51c262d05b54082012f827b14d
kex_algorithms length: 71
kex_algorithms string: diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1
server_host_key_algorithms length: 15
server_host_key_algorithms string: ssh-rsa,ssh-dss
encryption_algorithms_client_to_server length: 65
encryption_algorithms_client_to_server string: aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc
encryption_algorithms_server_to_client length: 65
encryption_algorithms_server_to_client string: aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc
mac_algorithms_client_to_server length: 85
mac_algorithms_client_to_server string: hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
mac_algorithms_server_to_client length: 85
mac_algorithms_server_to_client string: hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
compression_algorithms_client_to_server length: 4
compression_algorithms_client_to_server string: none
compression_algorithms_server_to_client length: 4
compression_algorithms_server_to_client string: none
```

SSH

• 통신 과정

Client

Server

← TCP Connection Established →

← SSH version string exchange →

← Key exchange →

DH Key exchange

대칭키 공유 -> 이산 로그 방식 이용
상대방의 공개키와 자신의 개인키를 사용
-> 비밀키 생성 -> 데이터 암호화

```

  ✓ Key Exchange
    Message Code: Diffie-Hellman Group Exchange Request (Old) (30)
    DH GEX Number of Bits: 4096
    Padding String: ce0ef24378ba
    [Direction: client-to-server]

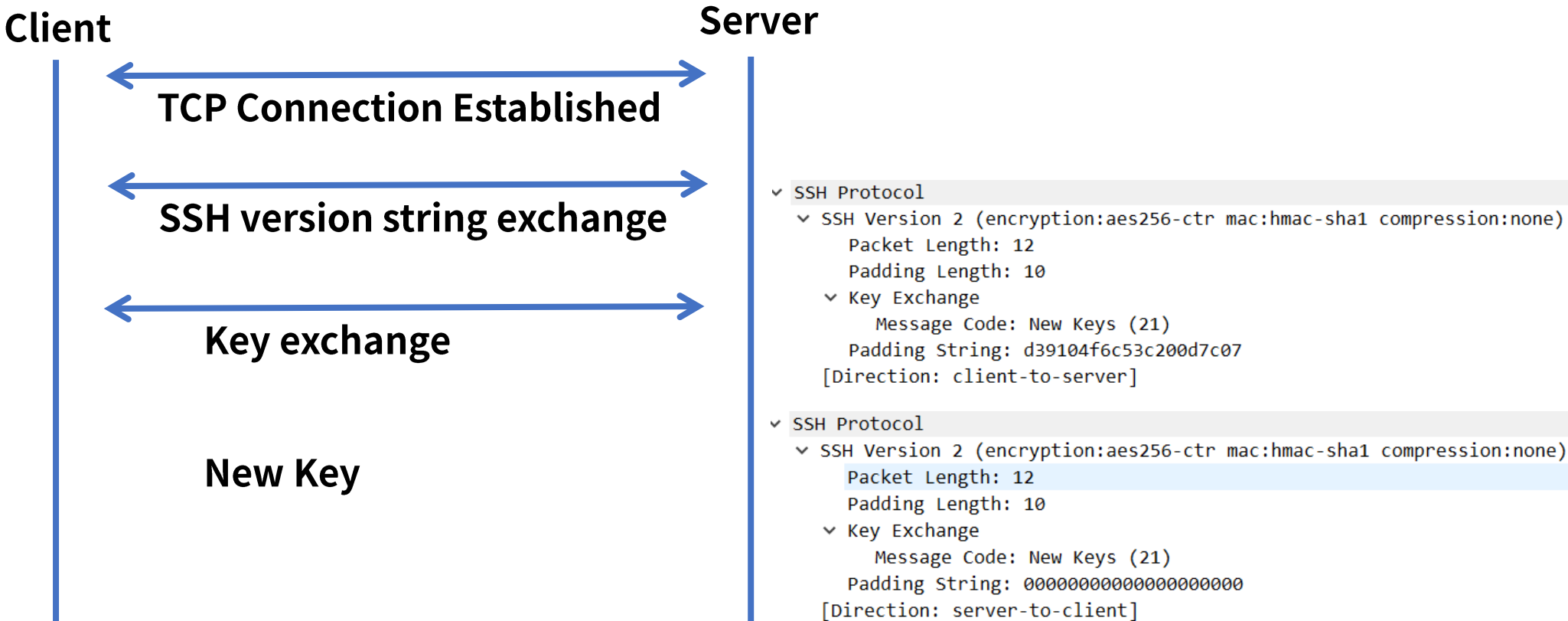
  ✓ Key Exchange
    Message Code: Diffie-Hellman Group Exchange Group (31)
    Multi Precision Integer Length: 257
    DH GEX modulus (P): 00fffffffffffffffffc90fdaa22168c234c4c6628b80dc1c...
    Multi Precision Integer Length: 1
    DH GEX base (G): 02
    Padding String: 0000000000000000
    [Direction: server-to-client]

  ✓ Key Exchange
    Message Code: Diffie-Hellman Group Exchange Init (32)
    Multi Precision Integer Length: 256
    DH client e: 5e0ac808a94086cf6ddd092ff754c073c987f8ddd89dd3e3...
    Padding String: 2d465687f6de
    [Direction: client-to-server]

  ✓ Key Exchange
    Message Code: Diffie-Hellman Group Exchange Reply (33)
    > KEX host key (type: ssh-rsa)
    Multi Precision Integer Length: 257
    DH server f: 00e75be5de96a74d14221e79fa6df5d82e391cc1e3dd6415...
    KEX H signature length: 271
    KEX H signature: 000000077373682d727361000001004af3a4e8aaae036e04...
    Padding String: 0000000000000000
    [Direction: server-to-client]
  
```

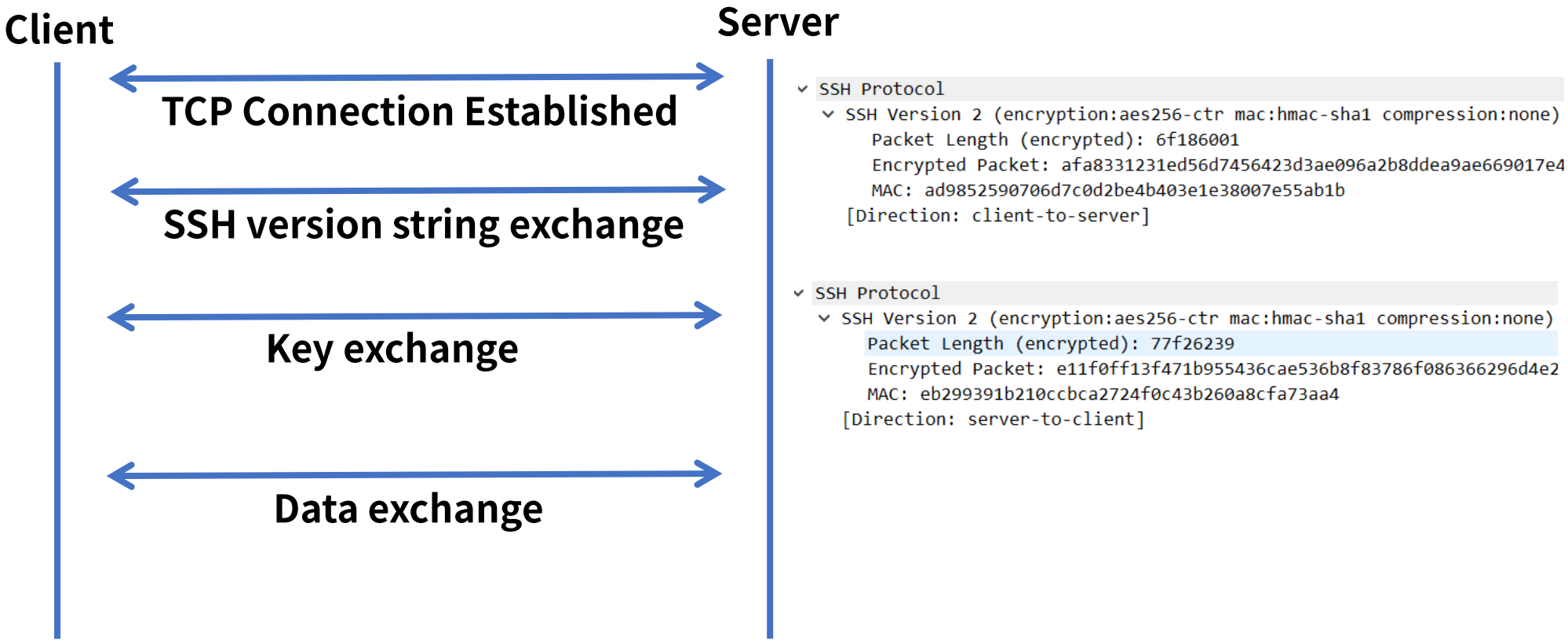
SSH

- 통신 과정



SSH

- 통신 과정



Wrap up

- TELNET은 원격지 호스트 컴퓨터에 접속하기 위해 사용되는 프로토콜로 TCP 23 사용
- 주요 기능으로 NVT(Network Virtual Terminals), 협상 가능한 옵션, 1:1 symmetric 관계
- SSH(Secure Shell)는 TELNET을 대체하기 위해 개발, 강력한 인증 방법 & 암호화 통신을 제공 TCP 22 사용
- SSH 특징으로 인증, 암호화, 무결성, 압축 등이 있다

