

네트워크 보안 과제1

패킷 분석하기

202246109

김기현

2025년 3월 16일

개요

사용 소프트웨어

- VMware workstation 17 Player (Windows 11에서 실행)
- Wireshark (패킷 캡처 및 분석)
- Cisco Packet Tracer(네트워크 시뮬레이터)

실험 환경

Server: Ubuntu 22.04.5 LTS (VMware)

Client: Windows10 (VMware)

네트워크 설정

	Server(Ubuntu)	Client(Windows)
IP address	192.168.220. 128	192.168.220. 129
MAC address	00:0c:29:4c:29:3a	00-0C-29-C8-EC-2C

데이터링크 계층은 직접 연결된 장치들 간의 통신을 담당하는 계층임. 이 계층에서는 랜 카드나 네트워크 장비의 하드웨어 주소 (MAC주소)만으로 통신합니다.

대표적인 프로토콜로 Ethernet 프로토콜이 있습니다.

ARP 프로토콜을 사용해 특정 IP 주소에 대해 MAC주소를 찾을 수 있습니다

```
C:\Users\PC>arp -a

인터페이스: 192.168.220.129 --- 0x5
  인터넷 주소      물리적 주소      유형
192.168.220.2      00-50-56-f8-b3-d4      동적
192.168.220.255    ff-ff-ff-ff-ff-ff      정적
224.0.0.22         01-00-5e-00-00-16      정적
224.0.0.252        01-00-5e-00-00-fc      정적
239.255.255.250    01-00-5e-7f-ff-fa      정적
255.255.255.255    ff-ff-ff-ff-ff-ff      정적
```

1. 패킷 캡처하기

먼저 Client(129)에서 ARP 테이블을 확인

현재 ARP 테이블엔 Server(128)의 IP와 MAC 주소가 없는걸 확인했습니다.

```
C:\Users\PC>ping 192.168.220.128

Ping 192.168.220.128 32바이트 데이터 사용:
192.168.220.128의 응답: 바이트=32 시간<1ms TTL=64
192.168.220.128의 응답: 바이트=32 시간<1ms TTL=64
192.168.220.128의 응답: 바이트=32 시간<1ms TTL=64
192.168.220.128의 응답: 바이트=32 시간<1ms TTL=64

192.168.220.128에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
    왕복 시간(밀리초):
        최소 = 0ms, 최대 = 0ms, 평균 = 0ms
```

Client(129)에서 서버 IP(128)로 ping 명령어를 통해 ICMP 패킷 전송

No.	Time	Source	Destination	Protocol	Length	Info
10	9.122904	VMware_c8:ec:2c	Broadcast	ARP	42	Who has 192.168.220.128? Tell 192.168.220.129
11	9.124367	VMware_4c:29:3a	VMware_c8:ec:2c	ARP	60	192.168.220.128 is at 00:0c:29:4c:29:3a
12	9.124611	192.168.220.129	192.168.220.128	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 13)
13	9.125132	192.168.220.128	192.168.220.129	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=64 (request in 12)
14	10.135074	192.168.220.129	192.168.220.128	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 15)
15	10.138312	192.168.220.128	192.168.220.129	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=64 (request in 14)
16	11.182969	192.168.220.129	192.168.220.128	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 17)
17	11.184959	192.168.220.128	192.168.220.129	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=64 (request in 16)
18	12.245338	192.168.220.129	192.168.220.128	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 19)
19	12.247575	192.168.220.128	192.168.220.129	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=64 (request in 18)

No.	Time	Source	Destination	Protocol	Length	Info
49	13.637518536	VMware_4c:29:3a	Broadcast	ARP	42	Who has 192.168.220.129? Tell 192.168.220.128
50	13.637716478	VMware_c8:ec:2c	VMware_4c:29:3a	ARP	60	192.168.220.129 is at 00:0c:29:c8:ec:2c
51	13.637724883	192.168.220.128	192.168.220.129	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=128
54	14.649260807	192.168.220.129	192.168.220.128	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128
55	14.649284609	192.168.220.128	192.168.220.129	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64
56	15.661761308	192.168.220.129	192.168.220.128	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128
57	15.661784109	192.168.220.128	192.168.220.129	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64
58	16.677733396	192.168.220.129	192.168.220.128	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128
59	16.677756024	192.168.220.128	192.168.220.129	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64

Wireshark를 통해 패킷의 송수신을 확인했습니다.

2. 패킷 분석하기

① ARP를 통해 MAC 주소를 확인을 요청하는 패킷

No.	Time	Source	Destination	Protocol	Length	Info
10	9.122904	VMware_c8:ec:2c	Broadcast	ARP	42	Who has 192.168.220.128? Tell 192.168.220.129
11	9.124367	VMware_4c:29:3a	VMware_c8:ec:2c	ARP	60	192.168.220.128 is at 00:0c:29:4c:29:3a

Frame 10: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{FE3BAD45-E06E-4592-B965-90E472851EAC}, id 0

Ethernet II, Src: VMware_c8:ec:2c (00:0c:29:c8:ec:2c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

.....1. = LG bit: Locally administered address (this is NOT the factory default)

.....1. = IG bit: Group address (multicast/broadcast)

Source: VMware_c8:ec:2c (00:0c:29:c8:ec:2c)

.....0. = LG bit: Globally unique address (factory default)

.....0. = IG bit: Individual address (unicast)

Type: ARP (0x0006)

[Stream index: 2]

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0000)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: VMware_c8:ec:2c (00:0c:29:c8:ec:2c)

Sender IP address: 192.168.220.129

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

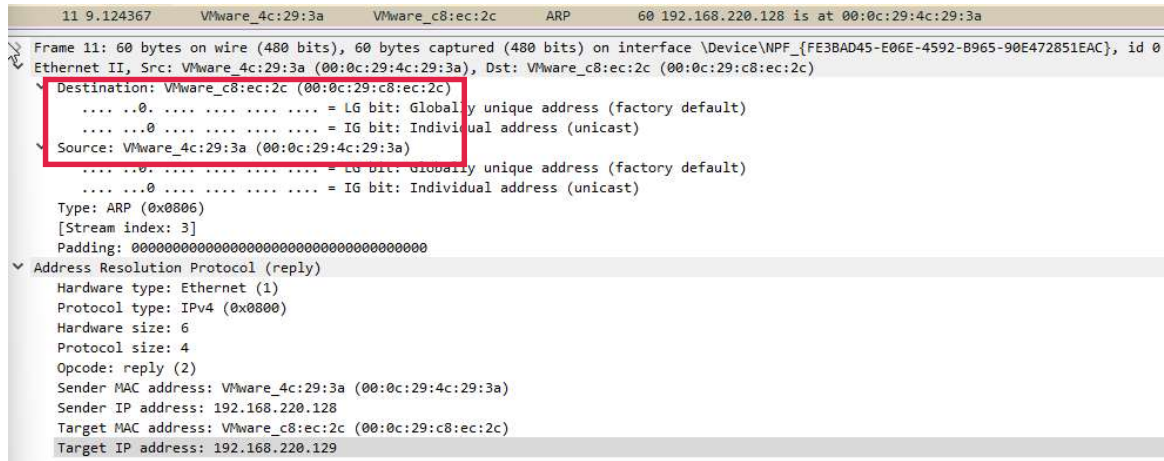
Target IP address: 192.168.220.128

Src: VMware_c8:ec:2c Dst: Broadcast인걸 보아하니

Client(129)가 192.168.220.128이 누구냐고 묻는 브로드캐스팅인걸 확인할수 있습니다.

192.168.220.128의 MAC 주소를 모르기 때문에 Target MAC address가 00:00:00_00:00:00 인걸 확인했습니다.

② ARP를 통해 MAC 주소를 응답하는 패킷



Src: VMware_4c:29:3a Dst: VMware_c8:ec:2c

Server가 응답으로 자신의 MAC 주소를 Client에게 보낸걸 확인했습니다.

③ 서로의 MAC 주소를 확인 후 최초로 전송되는 ICMP 패킷

No.	Time	Source	Destination	Protocol	Lengt	Info
12	9.124611	192.168.220.129	192.168.220.128	ICMP	74	Echo (ping) request
13	9.125132	192.168.220.128	192.168.220.129	ICMP	74	Echo (ping) reply
14	10.135074	192.168.220.129	192.168.220.128	ICMP	74	Echo (ping) request
15	10.138312	192.168.220.128	192.168.220.129	ICMP	74	Echo (ping) reply
16	11.182969	192.168.220.129	192.168.220.128	ICMP	74	Echo (ping) request
17	11.184959	192.168.220.128	192.168.220.129	ICMP	74	Echo (ping) reply
18	12.245338	192.168.220.129	192.168.220.128	ICMP	74	Echo (ping) request
19	12.247575	192.168.220.128	192.168.220.129	ICMP	74	Echo (ping) reply

Internet Control Message Protocol	Internet Control Message Protocol
Type: 8 (Echo (ping) request)	Type: 0 (Echo (ping) reply)
Code: 0	Code: 0
Checksum: 0x4d53 [correct]	Checksum: 0x5553 [correct]
[Checksum Status: Good]	[Checksum Status: Good]
Identifier (BE): 1 (0x0001)	Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)	Identifier (LE): 256 (0x0100)
Sequence Number (BE): 8 (0x0008)	Sequence Number (BE): 8 (0x0008)
Sequence Number (LE): 2048 (0x0800)	Sequence Number (LE): 2048 (0x0800)
<u>[Response frame: 13]</u>	<u>[Request frame: 12]</u>
> Data (32 bytes)	[Response time: 0.521 ms]

Source와 Destination IP를 보면 Client와 Server 상호간 ICMP Echo Request/Reply 메시지를 주고받는걸 볼 수 있습니다.

⑤ ARP 테이블 확인하기

```
C:\Users\PC>arp -a
```

인터페이스: 192.168.220.129 --- 0x5		
인터넷 주소	물리적 주소	유형
192.168.220.2	00-50-56-f8-b3-d4	동적
192.168.220.128	00-0c-29-4c-29-3a	동적
192.168.220.254	00-50-56-f1-89-3a	동적
192.168.220.255	ff-ff-ff-ff-ff-ff	정적
224.0.0.22	01-00-5e-00-00-16	정적
224.0.0.252	01-00-5e-00-00-fc	정적
224.0.0.253	01-00-5e-00-00-fd	정적
239.255.255.250	01-00-5e-7f-ff-fa	정적
255.255.255.255	ff-ff-ff-ff-ff-ff	정적

Client 의 ARP 테이블에 Server(128)에 대한 정보가 추가된 것을 확인 했습니다.

네트워크 계층은 LAN을 벗어난 원격자 간 통신을 하기 위한 핵심 계층입니다.

이 계층에서 가장 중요한 역할은 IP주소를 사용해 패킷이 목적지에 도달하도록 라우팅 하는 것입니다.

대표적인 프로토콜로 IPv4 또는 IPv6가 있습니다.

1. 패킷 캡처하기

The image shows a Wireshark packet capture interface. The top pane displays a list of captured packets. The bottom pane shows the detailed view of the selected packet (No. 70), which is an HTTP GET request.

No.	Time	Source	Destination	Protocol	Length
66	3.500079	192.168.220.129	210.117.181.249	TCP	60
67	3.512710	192.168.220.129	210.117.181.249	TCP	60
68	3.517137	210.117.181.249	192.168.220.129	TCP	60
69	3.517291	192.168.220.129	210.117.181.249	TCP	60
70	3.519417	192.168.220.129	210.117.181.249	HTTP	60
71	3.519674	210.117.181.249	192.168.220.129	TCP	60
72	3.523749	210.117.181.249	192.168.220.129	HTTP	40

Detailed view of packet 70:

- Frame 70: 620 bytes on wire (4960 bits), 620 bytes captured (4960 bits) on interface 0
- Ethernet II, Src: VMware_c8:ec:2c (00:0c:29:c8:ec:2c), Dst: VMware_f8:b3:c4:a1 (00:0c:29:f8:b3:c4:a1)
- Internet Protocol Version 4, Src: 192.168.220.129, Dst: 210.117.181.249
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 606
 - Identification: 0x5b0c (23308)
 - 010. = Flags: 0x2, Don't fragment
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 128
 - Protocol: TCP (6)
 - Header Checksum: 0x0000 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.220.129
 - Destination Address: 210.117.181.249
 - [Stream index: 5]
- Transmission Control Protocol, Src Port: 50364, Dst Port: 18880, Seq: 1, Win: 0, Len: 0
- Hypertext Transfer Protocol

패킷이 성공적으로 송수신될 걸 확인할 수 있습니다.

2. 패킷 분석하기

웹 서버에 접속 할 땐 TCP통신을 위해 3-way handshake과정을 거치는데

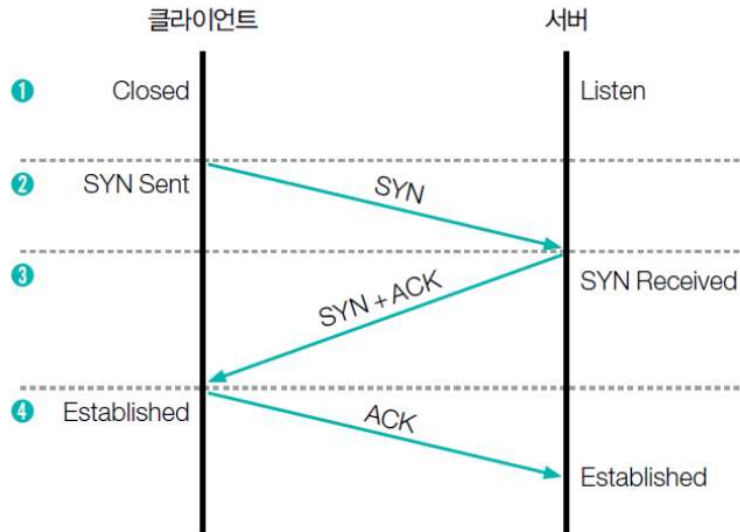


그림 2-32 TCP에서 연결 생성 과정

클라이언트가 서버와 연결을 위해 SYN패킷을 보내고
SYN패킷을 수신한 서버는 SYN+ACK패킷을 보내고
SYN+ACK패킷을 수신한 클라이언트는 ACK패킷을 전송합니다.

이제 직접 확인해 보겠습니다.

실제로 SYN, SYN+ACK, ACK패킷을 볼 수 있습니다.

No.	Time	Source	Destination	Protocol	Length	Info
67	3.512710	192.168.220.129	210.117.181.249	TCP	60	[50365 → 18880 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM]
68	3.517137	210.117.181.249	192.168.220.129	TCP	60	18880 → 50365 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
69	3.517291	192.168.220.129	210.117.181.249	TCP	54	50365 → 18880 [ACK] Seq=1 Ack=1 Win=64240 Len=0
70	3.519417	192.168.220.129	210.117.181.249	HTTP	620	GET / HTTP/1.1
71	3.519674	210.117.181.249	192.168.220.129	TCP	60	18880 → 50364 [ACK] Seq=1 Ack=567 Win=64240 Len=0
72	3.523749	210.117.181.249	192.168.220.129	HTTP	416	HTTP/1.1 304 Not Modified
73	3.574001	192.168.220.129	210.117.181.249	TCP	54	50364 → 18880 [ACK] Seq=567 Ack=363 Win=63878 Len=0

① SYN

```
[Header: Stream Seq: 2158760287, Offset: 0]
Source Address: 192.168.220.129
Destination Address: 210.117.181.249
[Stream index: 5]
Transmission Control Protocol, Src Port: 50365, Dst Port: 18880, Seq
Source Port: 50365
Destination Port: 18880
[Stream index: 2]
[Stream Packet Number: 1]
> [Conversation completeness: Incomplete, ESTABLISHED (7)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2158760287
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
> Flags: 0x002 (SYN)
Window: 8192
[Calculated window size: 8192]
Checksum: 0x25c0 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (12 bytes), Maximum segment size, No-Operation (NOP), W
> [Timestamps]
```

Client가 Web server의 18880포트로 SYN패킷을 보냈습니다.

② SYN+ACK

```
Source Address: 210.117.181.249
Destination Address: 192.168.220.129
[Stream index: 5]
Transmission Control Protocol, Src Port: 18880, Dst Port: 50365
Source Port: 18880
Destination Port: 50365
[Stream index: 2]
[Stream Packet Number: 2]
> [Conversation completeness: Incomplete, ESTABLISHED (7)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2019757414
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2158760288
0110 .... = Header Length: 24 bytes (6)
> Flags: 0x012 (SYN, ACK)
Window: 64240
[Calculated window size: 64240]
Checksum: 0x5138 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (4 bytes), Maximum segment size
> [Timestamps]
> [SEQ/ACK analysis]
```

SYN패킷을 받은 Web server가 Client에게 연결을 해도 좋다고 SYN+ACK 패킷을 보냈습니다.

③ ACK

```
Source Address: 192.168.220.129
Destination Address: 210.117.181.249
[Stream index: 5]
Transmission Control Protocol, Src Port: 50365, Dst Port: 18880,
Source Port: 50365
Destination Port: 18880
[Stream index: 2]
[Stream Packet Number: 3]
> [Conversation completeness: Incomplete, ESTABLISHED (7)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2158760288
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2019757415
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x010 (ACK)
Window: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x25b4 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
```

클라이언트가 서버의 응답을 확인했다는 의미로 ACK패킷을 서버로 보냈습니다.

이렇게 직접 3-way handshake 과정을 확인 할 수 있었습니다.

계층별 패킷 구조 분석

3-way handshake 과정 후에 캡처된 HTTP패킷으로 계층별 패킷 구조를 분석해보겠습니다.

The image shows a Wireshark packet capture of an HTTP GET request. The packet list shows frame 70 as the selected packet. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

2계층(Data Link Layer) 이더넷 패킷 헤더 분석하기

0000 00 50 56 f8 b3 d4 00 0c 29 c8 ec 2c 08 00 45 00	·PV·...· }·...·E·	구분	HEX	Binary
0010 02 5e 5b 0c 40 00 80 06 00 00 c0 a8 dc 81 d2 75	·A[@·...· ····u	2계층	00 50 56 f8 b3 d4 00 0c 29 c8 ec 2c 08 00	00000000 01010000 01010110 11111000 10110011 11010100 00000000 00001100 00101001 11001000 00101100 00001000 00000000
0020 b5 f9 c4 bc 49 c0 c4 7c 2e 37 22 e6 0b 3c 50 18	·...I· ·7"·<P·			
0030 fa f0 27 ea 00 00 47 45 54 20 2f 20 48 54 54 50	·...·GE T / HTTP			
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 32 31 30 2e	/1.1·Ho st: 210.			
0050 31 31 37 2e 31 38 31 2e 32 34 39 3a 31 38 38 38	117.181. 249:1888	Destination MAC Address		
0060 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b	0·Conne ction: k			
0070 65 65 70 2d 61 6c 69 76 65 0d 0a 43 61 63 68 65	ee-p-aliv e·Cache			
0080 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67	-Control : max-ag			
0090 65 3d 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73	e=0·Upg rade-Ins	Source MAC Address		
00a0 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20	ecure-Re quests:			
00b0 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d	1·User- Agent: M			
00c0 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64	ozilla/5 .0 (Wind			
00d0 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e	ows NT 1 0.0; Win	Type		
00e0 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65	64; x64) AppleWe			
00f0 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54	bKit/537 .36 (KHT			
0100 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20	ML, like Gecko)			
0110 43 68 72 6f 6d 65 2f 31 33 34 2e 30 2e 30 2e 30	Chrome/1 34.0.0.0	Destination MAC Address		
0120 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20 45	Safari/ 537.36 E			
0130 64 67 2f 31 33 34 2e 30 2e 30 2e 30 0d 0a 41 63	dg/134.0 .0.0·Ac			
0140 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c	cept: te xt/html,			
0150 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d	applicat ion/xhtm	Source MAC Address		
0160 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f	l+xml,ap plicatio			
0170 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67	n/xml;q= 0.9,imag			
0180 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62	e/avif,i mage/web			
0190 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a	p,image/ apng;/*	Type		
01a0 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69	;q=0.8,a pplicati			
01b0 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 6e	on/sign e-dexchan			
01c0 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a 41	ge;v=b3; q=0.7·A			
01d0 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20	ccept-En coding:	Destination MAC Address		
01e0 6f 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41	gzip, de flate·A			
01f0 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20	ccept-La nguage:			
0200 6b 6f 2c 65 6e 3b 71 3d 30 2e 39 2c 65 6e 2d 55	ko,en;q= 0.9,en-U			
0210 53 3b 71 3d 30 2e 38 0d 0a 49 66 2d 4e 6f 6e 65	S;q=0.8·If-None	Source MAC Address		
0220 2d 4d 61 74 63 68 3a 20 22 36 37 64 33 63 33 39	-Match: "67d3c39			
0230 65 2d 31 30 30 22 0d 0a 49 66 2d 4d 6f 64 69 66	e-100"·If-Modif			
0240 65 2d 31 30 30 22 0d 0a 49 66 2d 4d 6f 64 69 66	ied-Sinc e: Fri,			
0250 69 65 64 2d 53 69 6e 63 65 3a 20 46 72 69 2c 20	14 Mar 2 025.05:5	Type		
0260 30 3a 32 32 20 47 4d 54 0d 0a 0d 0a 0d 0a	0:22 GMT·...·E·			

3계층(Network Layer) IPv4

0000	00 50 56 f8 b3 d4 00 0c 29 c8 ec 2c 08 00 45 00	..PV.....).....E-
0010	02 5e 5b 0c 40 00 80 06 00 00 c0 a8 dc 81 d2 75	...I... .7"...<P-
0020	b5 f9 c4 bc 49 c0 c4 7c 2e 37 22 e6 0b 3c 50 18	...["@... ..u
0030	fa f0 27 ea 00 00 47 45 54 20 2f 20 48 54 54 50	...GE T / HTTP
0040	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 32 31 30 2e	/1.1..Ho st: 210.
0050	31 31 37 2e 31 38 31 2e 32 34 39 3a 31 38 38 38	117.181. 249:1888
0060	30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b	0..Conne ction: k
0070	65 65 70 2d 61 6c 69 76 65 0d 0a 43 61 63 68 65	ee-p-aliv e..Cache
0080	2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67	-Control : max-ag
0090	65 3d 3b 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73	e=0..Upg rade-Ins
00a0	65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20	ecure-Re quests:
00b0	31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d	1..User- Agent: M
00c0	6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64	ozilla/5 .0 (Wind
00d0	6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e	ows NT 1 0.0; Win
00e0	36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65	64; x64) AppleWe
00f0	62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54	bKit/537 .36 (KHT
0100	4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20	ML, like Gecko)
0110	43 68 72 6f 6d 65 2f 31 33 34 2e 30 2e 30 2e 30	Chrome/1 34.0.0.0
0120	20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20 45	Safari/ 537.36 E
0130	64 67 2f 31 33 34 2e 30 2e 30 2e 30 0d 0a 41 63	dg/134.0 .0.0..Ac
0140	63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c	cept: te xt/html,
0150	61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d	applicat ion/xhtm
0160	6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f	l+xml,ap plicatio
0170	6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67	n/xml;q= 0.9,imag
0180	65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62	e/avif,i mage/web
0190	70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a	p,image/ apng,*/*
01a0	3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69	;q=0.8,a pplicati
01b0	6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 6e	on/signe d-exchan
01c0	67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a 41	ge;v=b3; q=0.7..A
01d0	63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20	ccept-En coding:
01e0	67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41	gzip, de flate..A
01f0	63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20	ccept-La nguage:
0200	6b 6f 2c 65 6e 3b 71 3d 30 2e 39 2c 65 6e 2d 55	ko,en;q= 0.9,en-U
0210	53 3b 71 3d 30 2e 38 0d 0a 49 66 2d 4e 6f 6e 65	S;q=0.8. .If-None
0220	2d 4d 61 74 63 68 3a 20 22 36 37 64 33 63 33 39	-Match: "67d3c39
0230	65 2d 31 30 30 22 0d 0a 49 66 2d 4d 6f 64 69 66	e-100"... If-Modif
0240	69 65 64 2d 53 69 6e 63 65 3a 20 46 72 69 2c 20	ied-Sinc e: Fri,
0250	31 34 20 4d 61 72 20 32 30 32 35 20 30 35 3a 35	14 Mar 2 025 05:5
0260	30 3a 32 32 20 47 4d 54 0d 0a 0d 0a	0:22 GMT

구분	HEX	Binary
3계층	45 00 02 5e 5b 0c 40 00 80 06 00 00 c0 a8 dc 81 d2 75 b5 f9	01000101 00000000 01011110 01011011 00001100 01000000 00000000 10000000 00000110 00000000 00000000 11000000 10101000 11011100 10000001 11010010 01110101 00000000 11111001 11000100

Version	IHL	Type Of Service	Total Length
0100	0101	0000 0000	0000 0010 0101 1110
Identification		Flag	Fragment Offset
0101 1011 0000 1100		010	0 0000 0000 0000
Time To Live	Protocol	Header Checksum	
1000 0000	0000 0110	0000 0000 0000 0000	
Source Address			
1100 0000 1010 1000 1101 1100 1000 0001			
Destination Address			
1101 0010 0111 0101 1011 0101 1111 1001			

4계층(Transport Layer) TCP

0000	00 50 56 f8 b3 d4 00 0c 29 c8 ec 2c 08 00 45 00	·PV· · · · · ·) · · · ·
0010	02 5e 5b 0c 40 00 80 06 00 00 c0 a8 dc 81 d2 75	·^· [·@· · · · · · · · · ·
0020	b5 f9 c4 bc 49 e0 c4 7c 2e 37 22 e6 0b 3c 50 18	·· · · · · I· · · · · · · · · · 7· · · ·
0030	fa f0 27 ea 00 00 47 45 54 20 2f 20 48 54 54 50	· · · · · · GE T / H
0040	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 32 31 30 2e	/1.1· · · · · · Host: 2
0050	31 31 37 2e 31 38 31 2e 32 34 39 3a 31 38 38 38	117.181. 249:1
0060	30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b	0· · · · · · Conne ction
0070	65 65 70 2d 61 6c 69 76 65 0d 0a 43 61 63 68 65	eep-aliv e· · · · · · Ca
0080	2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67	-Control : max
0090	65 3d 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73	e=0· · · · · · Upg rade·
00a0	65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20	ecure-Re quest
00b0	31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d	1· · · · · · User- Agent
00c0	6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64	ozilla/5 .0 (W
00d0	6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e	ows NT 1 0.0;
00e0	36 34 3b 20 78 36 3a 29 20 41 70 70 6c 65 57 65	64; x64) Appl
00f0	62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54	bKit/537 .36 (
0100	4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20	ML, like Geck
0110	43 68 72 6f 6d 65 2f 31 33 34 2e 30 2e 30 2e 30	Chrome/1 34.0.
0120	20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20 45	Safari/ 537.3
0130	64 67 2f 31 33 34 2e 30 2e 30 2e 30 0d 0a 41 63	dg/134.0 .0.0·
0140	63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c	cept: te xt/ht
0150	61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d	applicat ion/x
0160	6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f	l+xml,ap plica
0170	6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67	n/xml;q= 0.9,i
0180	65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62	e/avif,i mage/
0190	70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a	p,image/ apng,
01a0	3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69	;q=0.8,a pplic
01b0	6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 6e	on/signe d-exc
01c0	67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a 41	ge;v=b3; q=0.7
01d0	63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20	ccept-En codin
01e0	67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41	gzip, de flate
01f0	63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20	ccept-La nguag
0200	6b 6f 2c 65 6e 3b 71 3d 30 2e 39 2c 65 6e 2d 55	ko,en;q= 0.9,e
0210	53 3b 71 3d 30 2e 38 0d 0a 49 66 2d 4e 6f 6e 65	S;q=0.8· · · · · · If-N
0220	2d 4d 61 74 63 68 3a 20 22 36 37 64 33 63 33 39	-Match: "67d3
0230	65 2d 31 30 30 22 0d 0a 49 66 2d 4d 6f 64 69 66	e-100"· · · · · · If-Mo
0240	69 65 64 2d 53 69 6e 63 65 3a 20 46 72 69 2c 20	ied-Sinc e: Fr
0250	31 34 20 4d 61 72 20 32 30 32 35 20 30 35 3a 35	14 Mar 2 025 0
0260	30 3a 32 32 20 47 4d 54 0d 0a 0d 0a	0:22 GMT · · · · ·

구분	HEX	Binary
4계층	c4 bc 49 c0 c4 7c 2e 37 22 e6 0b 3c 50 18 fa f0 27 ea 00 00	10111100 01001001 11000000 11000100 01111100 00101110 00110111 00100010 11100110 00001011 00111100 01010000 00011000 00000000 11110000 00100111 11101010 00000000 00000000 01000111

Source Port(S.Port)		Destination Port	
1100 0100 1011 1100		0100 1001 1100 0000	
Sequence Number			
1100 0100 0111 1100 0010 1110 0011 0111			
Acknowledgment Number			
0010 0010 1110 0110 0000 1011 0011 1100			
Data Offset	Reserved	Control Bit	Window
0101	0000 00	01 1000	1111 1010 1111 0000
Checksum		Urgent Pointer	
0010 0111 1110 1010		0000 0000 0000 0000	

7계층(Application Layer)

0000	00 50 56 f8 b3 d4 00 0c 29 c8 ec 2c 08 00 45 00	·PV·····)··,··
0010	02 5e 5b 0c 40 00 80 06 00 00 c0 a8 dc 81 d2 75	·^[·@··· ······
0020	b5 f9 c4 bc 49 c0 c4 7c 2e 37 22 e6 0b 3c 50 18	·····I··· .7"··<
0030	fa f0 27 ea 00 00 47 45 54 20 2f 20 48 54 54 50	·····GE T / HT
0040	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 32 31 30 2e	/1.1··Ho st: 21
0050	31 31 37 2e 31 38 31 2e 32 34 39 3a 31 38 38 38	117.181. 249:18
0060	30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b	0··Conne ction:
0070	65 65 70 2d 61 6c 69 76 65 0d 0a 43 61 63 68 65	eeep-aliv e··Cad
0080	2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67	-Control : max-
0090	65 3d 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73	e=0··Upg rade-I
00a0	65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20	ecure-Re quests
00b0	31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d	1··User- Agent:
00c0	6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64	ozilla/5 .0 (Wi
00d0	6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e	ows NT 1 0.0; W
00e0	36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65	64; x64) Apple
00f0	62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54	bKit/537 .36 (K
0100	4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20	ML, like Gecko
0110	43 68 72 6f 6d 65 2f 31 33 34 2e 30 2e 30 2e 30	Chrome/1 34.0.6
0120	20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20 45	Safari/ 537.36
0130	64 67 2f 31 33 34 2e 30 2e 30 2e 30 0d 0a 41 63	dg/134.0 .0.0··
0140	63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c	cept: te xt/htm
0150	61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d	applicat ion/xh
0160	6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f	l+xml,ap plicat
0170	6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67	n/xml;q= 0.9,in
0180	65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62	e/avif,i mage/w
0190	70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a	p,image/ apng,*
01a0	3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69	;q=0.8,a pplica
01b0	6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 6e	on/signe d-exch
01c0	67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a 41	ge;v=b3; q=0.7·
01d0	63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20	ccept-En coding
01e0	67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41	gzip, de flate·
01f0	63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20	ccept-La nguage
0200	6b 6f 2c 65 6e 3b 71 3d 30 2e 39 2c 65 6e 2d 55	ko,en;q= 0.9,er
0210	53 3b 71 3d 30 2e 38 0d 0a 49 66 2d 4e 6f 6e 65	S;q=0.8· ·If-No
0220	2d 4d 61 74 63 68 3a 20 22 36 37 64 33 63 33 39	-Match: "67d3c
0230	65 2d 31 30 30 22 0d 0a 49 66 2d 4d 6f 64 69 66	e-100"·· If-Mod
0240	69 65 64 2d 53 69 6e 63 65 3a 20 46 72 69 2c 20	ied-Sinc e: Fri
0250	31 34 20 4d 61 72 20 32 30 32 35 20 30 35 3a 35	14 Mar 2 025 05
0260	30 3a 32 32 20 47 4d 54 0d 0a 0d 0a	0:22 GMT ····

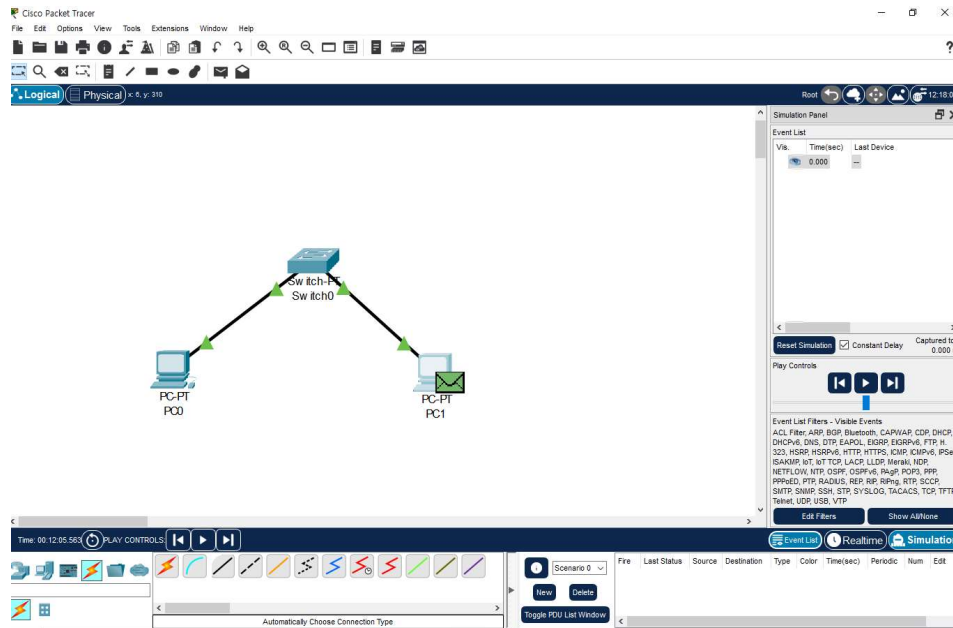
Hypertext Transfer Protocol

```
> GET / HTTP/1.1\r\n
Host: 210.117.181.249:18880\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ko,en;q=0.9,en-US;q=0.8\r\n
If-None-Match: "67d3c39e-100"\r\n
If-Modified-Since: Fri, 14 Mar 2025 05:50:22 GMT\r\n
\r\n
[Response in frame: 72]
[Full request URI: http://210.117.181.249:18880/]
```


1. 데이터 링크 계층에 사용되는 장치 연결

데이터 링크 계층에서 사용되는 스위치 허브와 PC 2대를 연결했습니다.

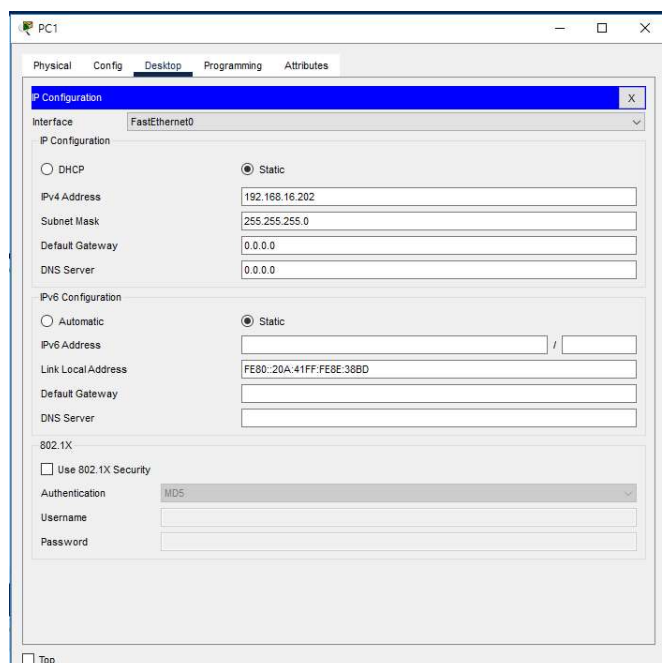
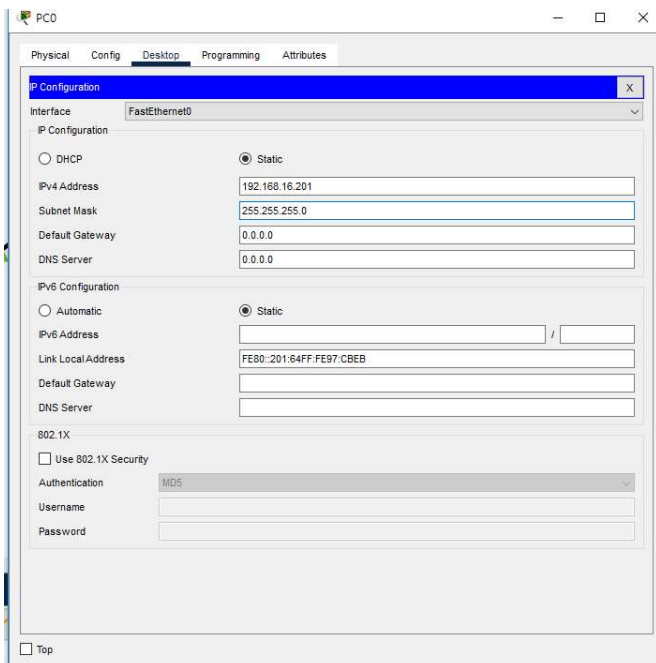
파란불이 들어오며 연결된 걸 확인할 수 있습니다.



2. IP 주소 설정

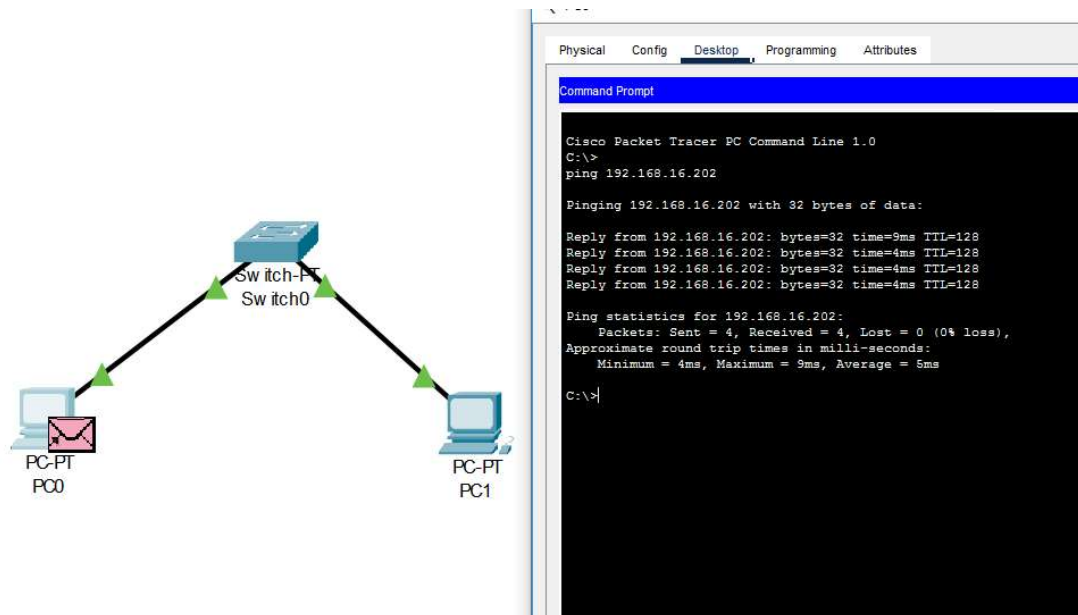
PC0의 IP주소를 192.168.16.201로

PC1의 IP주소를 192.168.16.202로 설정했습니다.

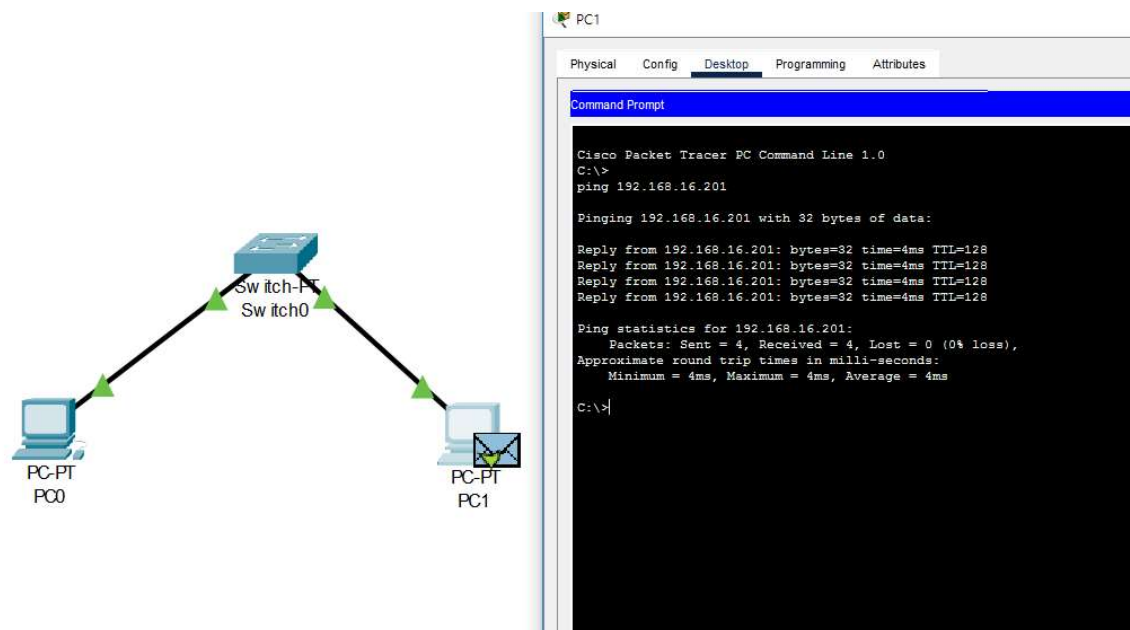


3. 연결 확인

PC0 -> PC1 Ping명령어를 실행해 Reply가 성공적으로 온걸 확인했습니다.

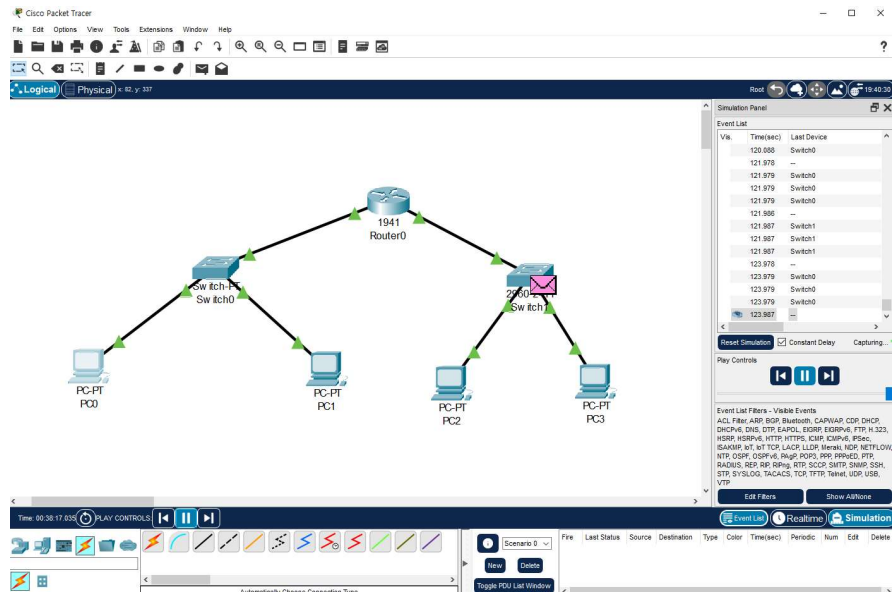


마찬가지로 PC1 -> PC0 도 Reply를 확인했습니다.



결과적으로 스위치와 연결된 PC0 <-> PC1의 연결이 정상적으로 이루어짐을 확인했습니다.

1. 네트워크 장치 연결



구분	장치	IP Address	Default Gateway IP Address
네트워크 1	PC0	192.168.16.201	192.168.16.200
	PC1	192.168.16.202	192.168.16.200
네트워크 2	PC2	192.168.15.201	192.168.15.200
	PC3	192.168.15.202	192.168.15.200

위와 같이 세팅했습니다.

2. 연결 확인하기

tracert 명령어를 통해 PC0 -> Router -> PC3으로 흘러가는지 확인해보겠습니다.

```
C:\>tracert 192.168.15.202

Tracing route to 192.168.15.202 over a maximum of 30 hops:

  1  8 ms      4 ms      4 ms      192.168.16.200
  2  *          8 ms      8 ms      192.168.15.202

Trace complete.
```

tracert 명령어가 정상적으로 실행되었으며, PC0에서 Router를 거쳐 PC3으로 패킷이 전달됨을 확인할 수 있습니다