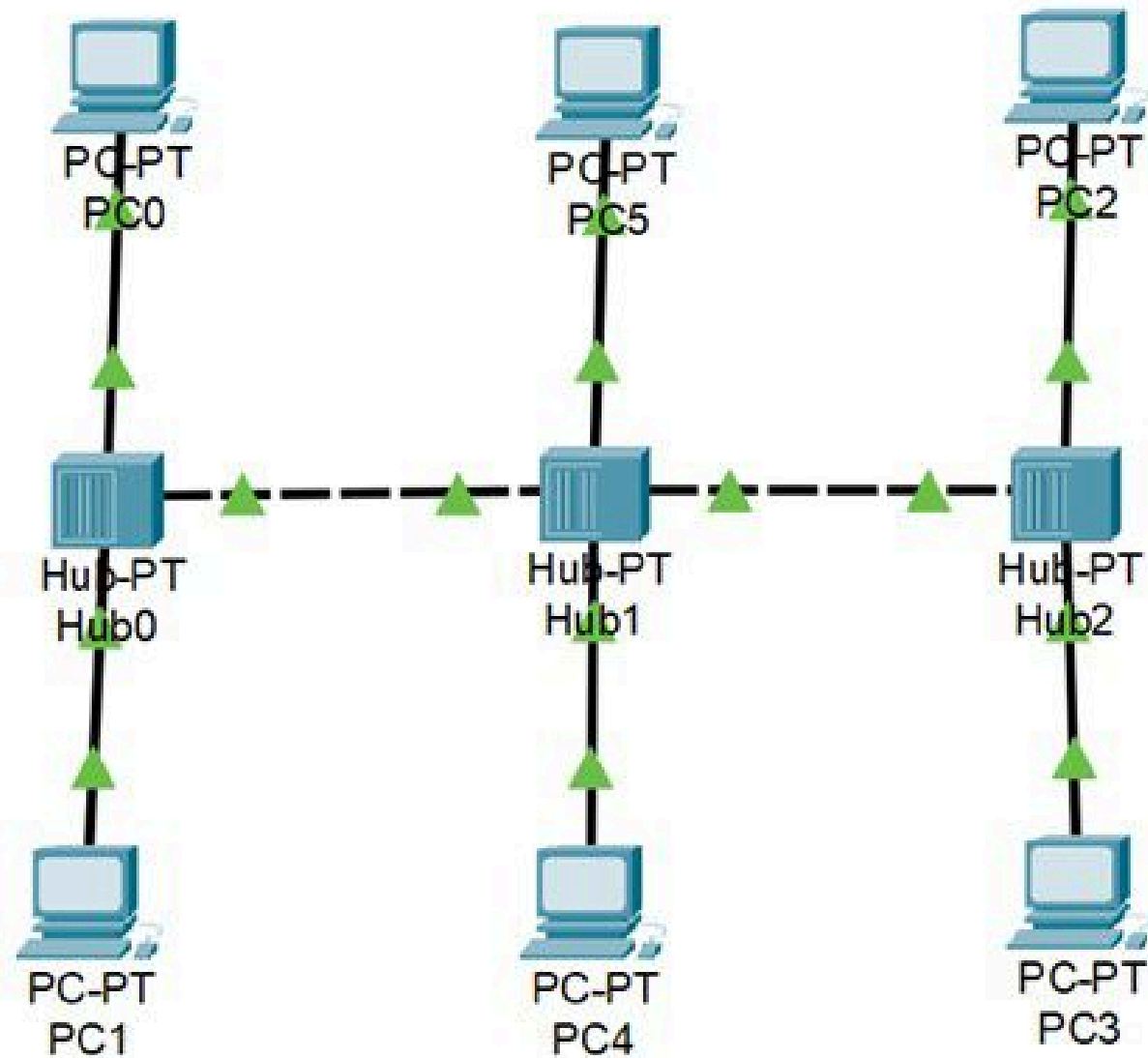
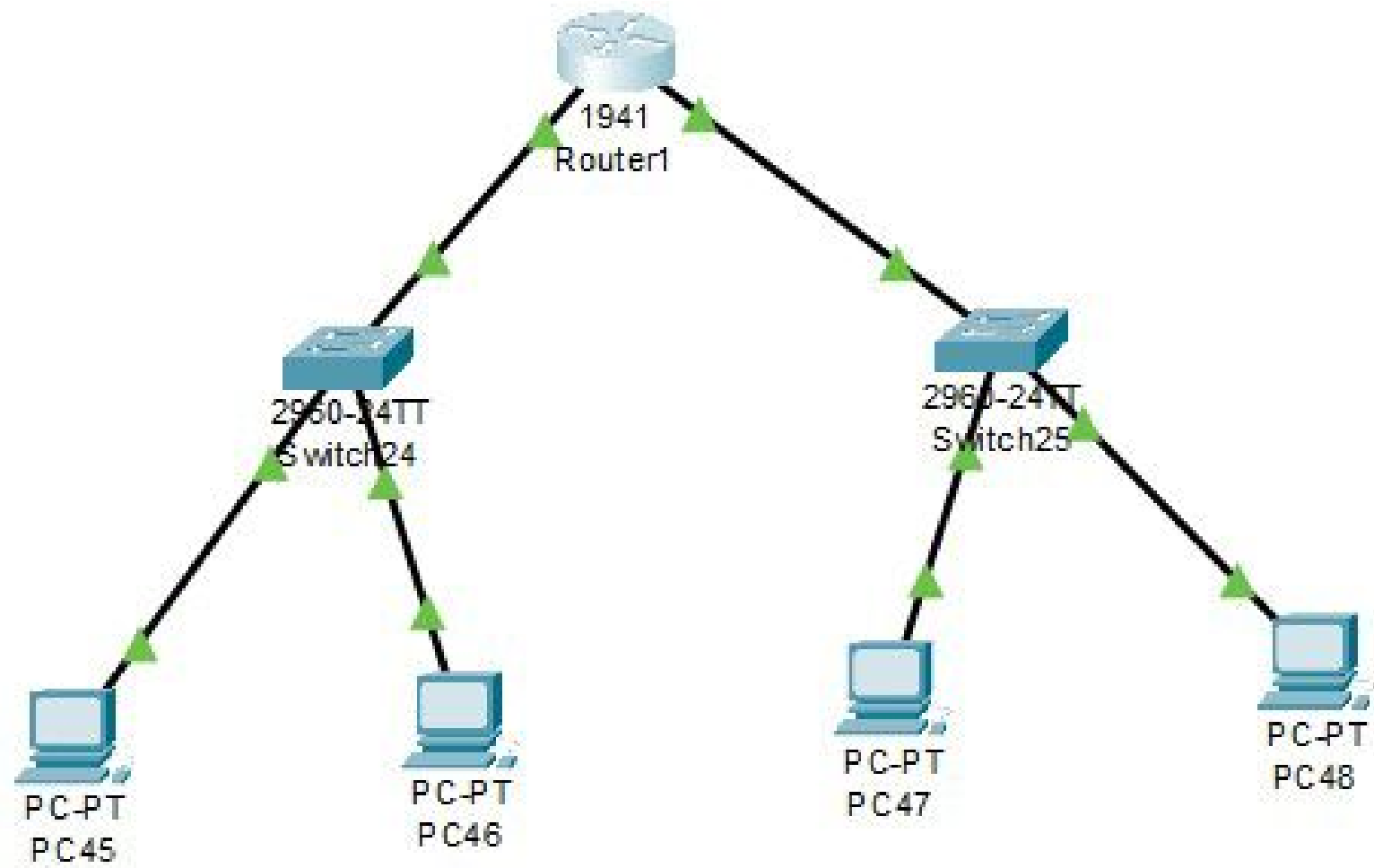


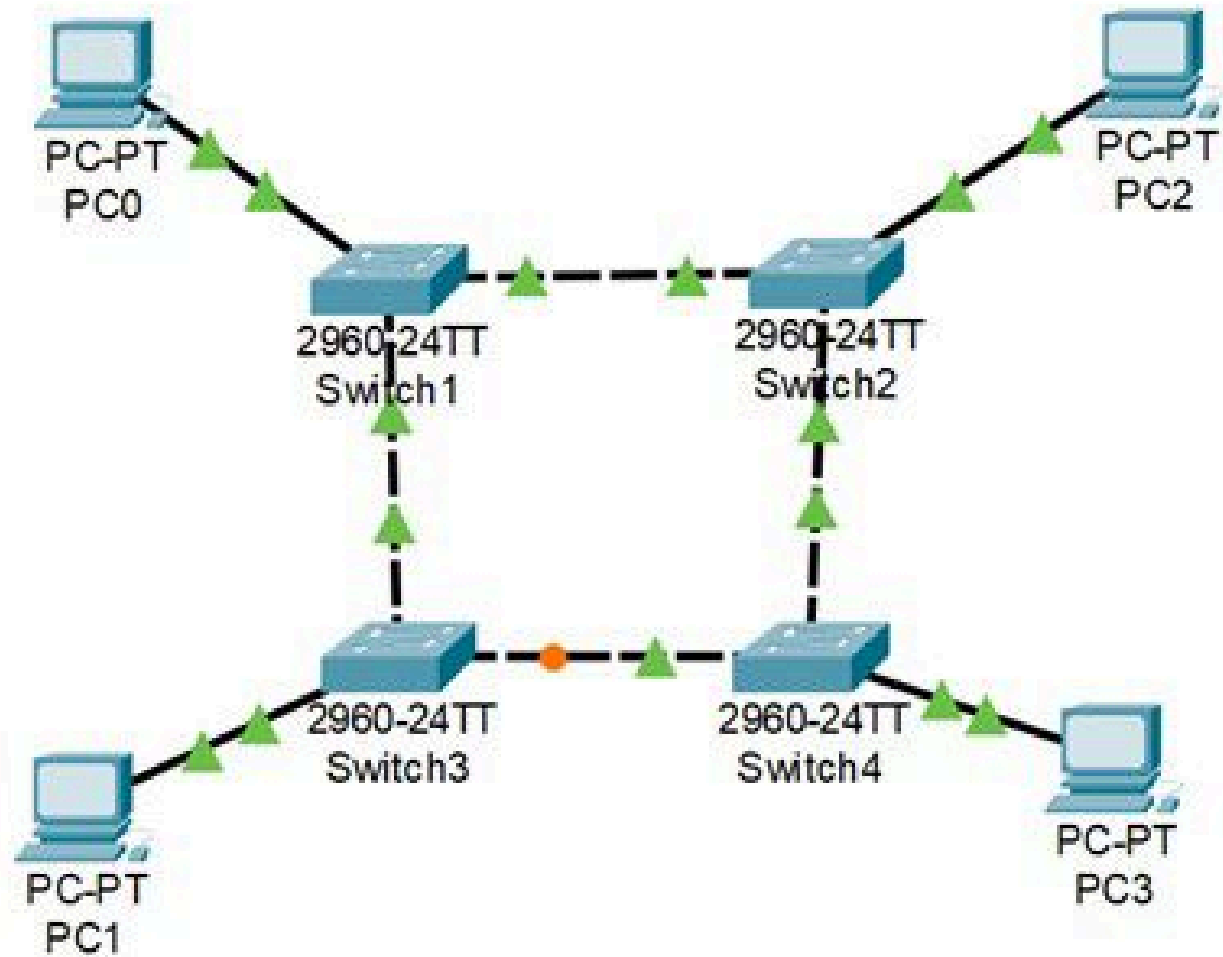
## Bus topology



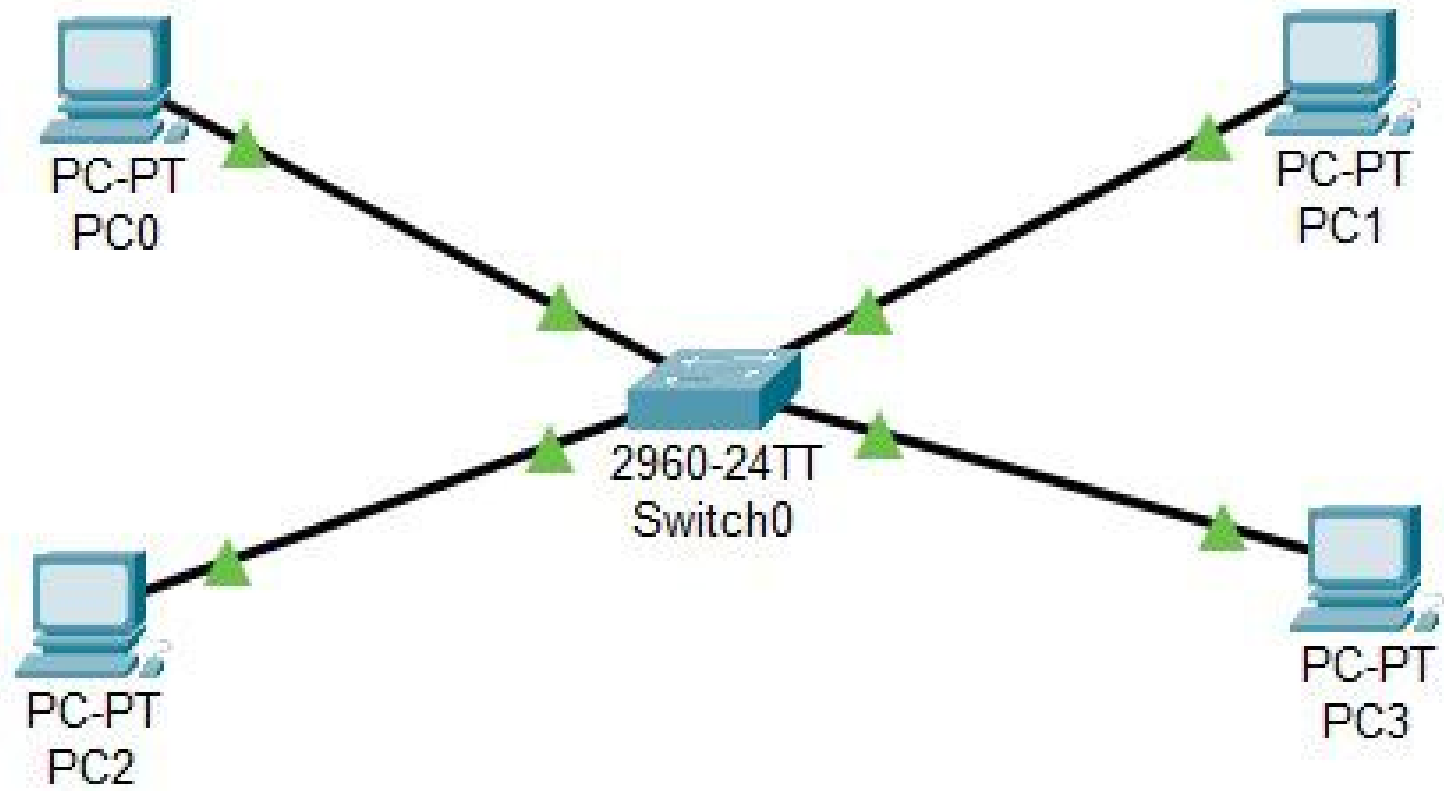
# configuration method



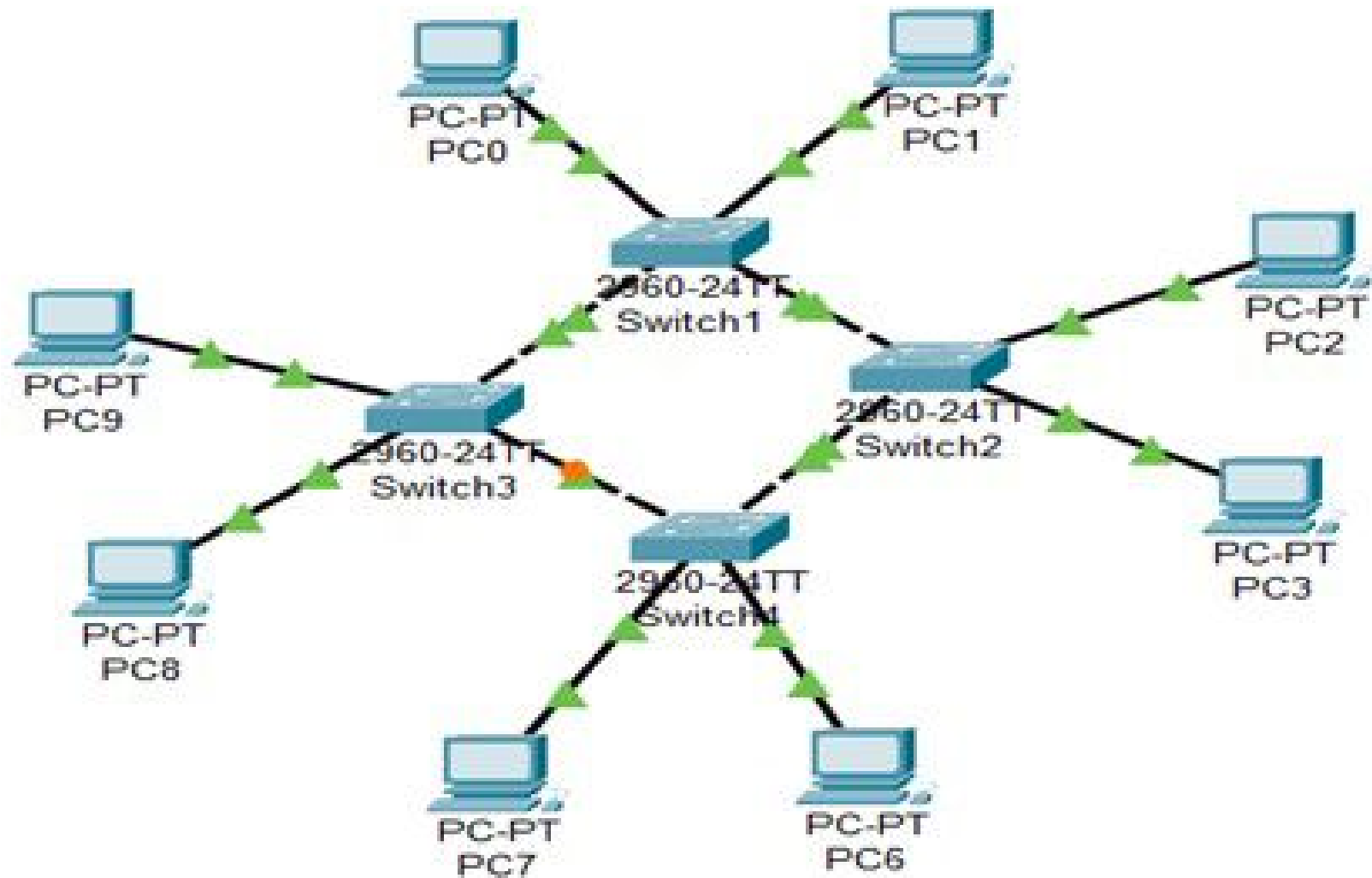
## Ring topology



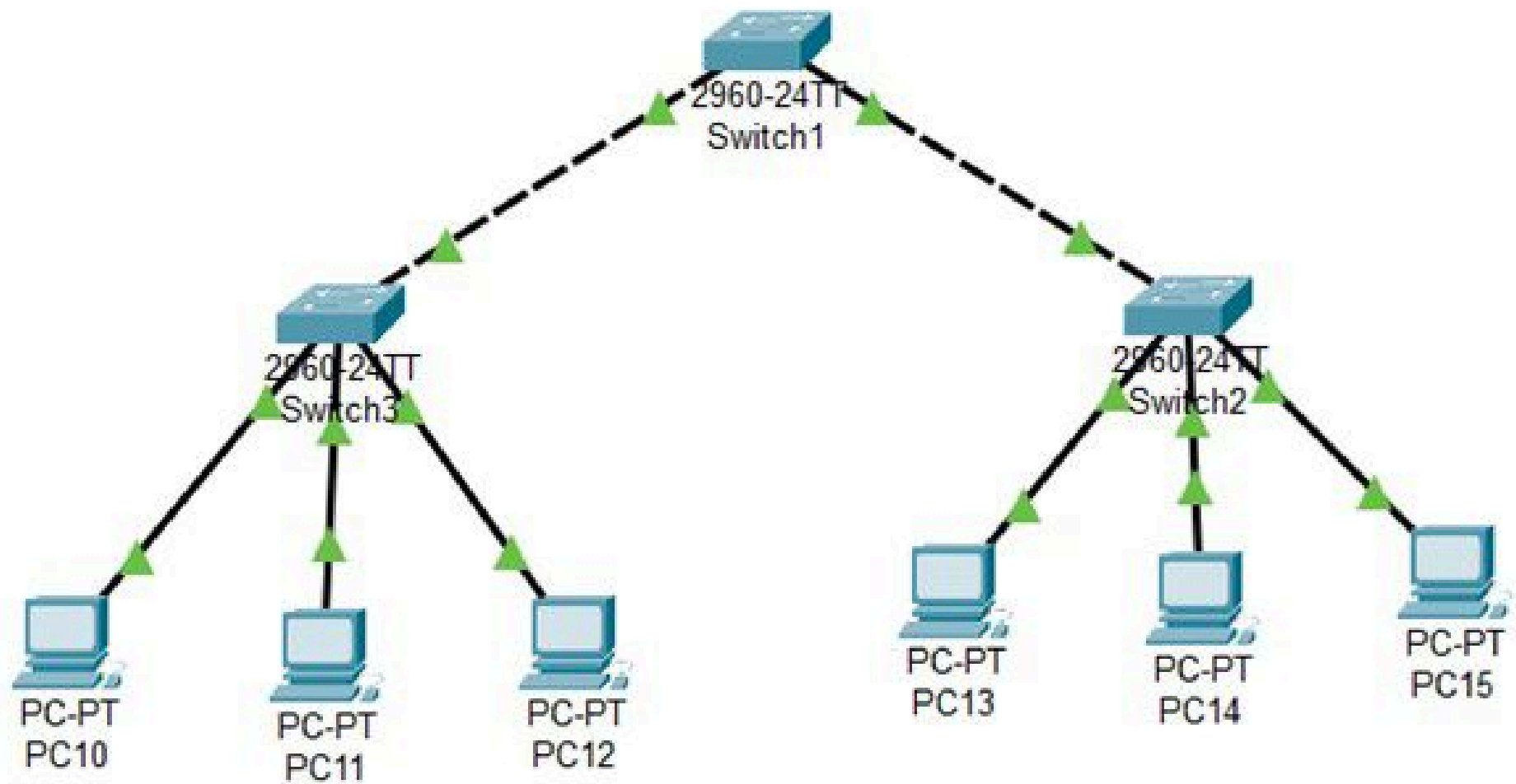
star topology



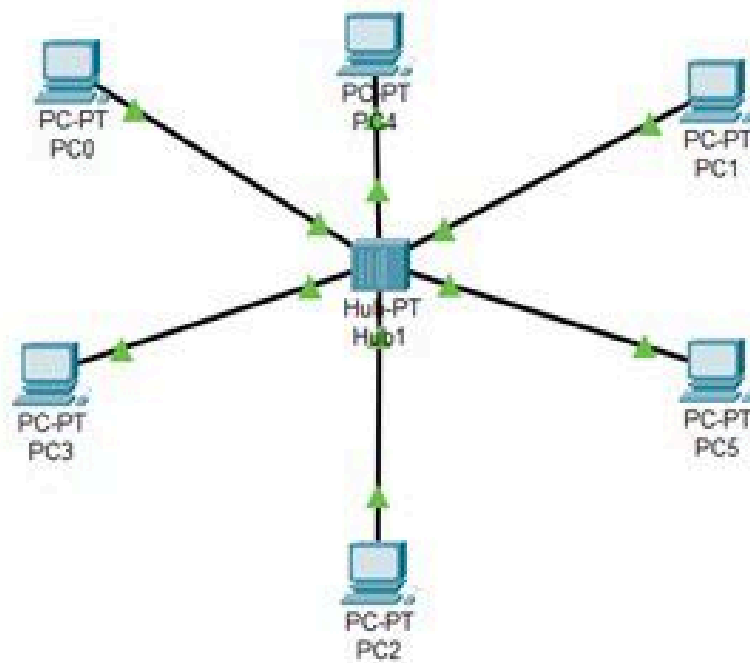
## Mesh topology



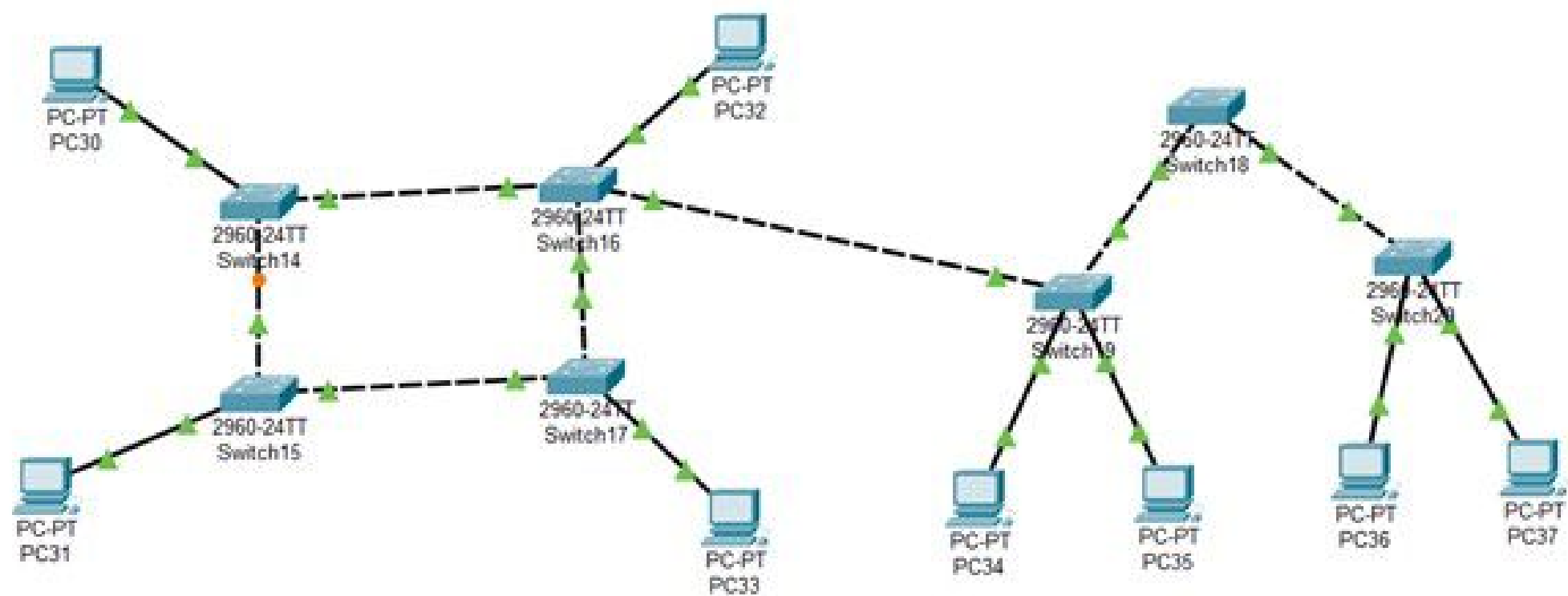
## Tree topology



# CSMA/CD&CSMA/CA

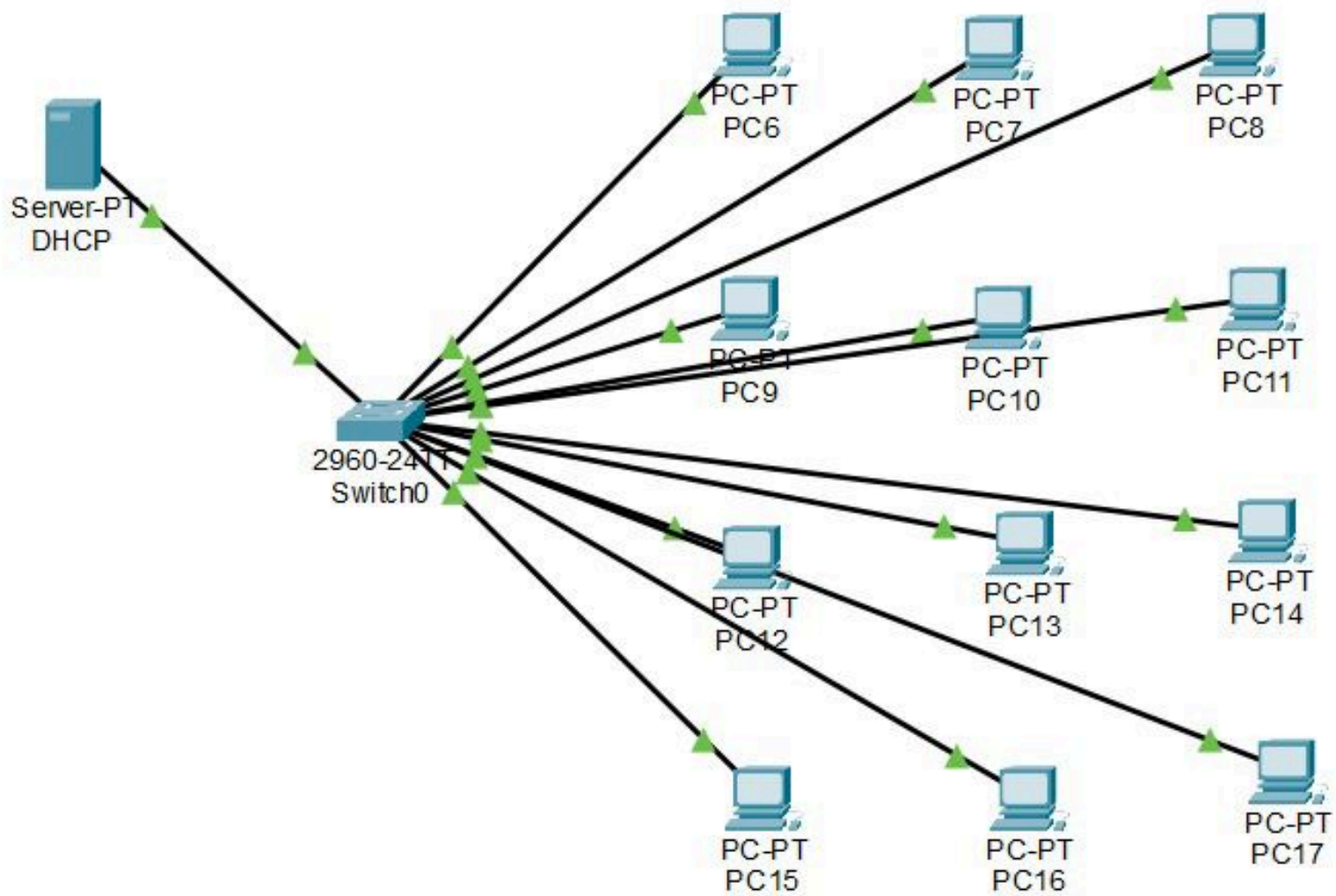


ario 0 ▾	Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
Delete		Successful	PC0	PC2	ICMP		0.000	N	0	(edit)	
		Successful	PC3	PC2	ICMP		0.000	N	1	(edit)	

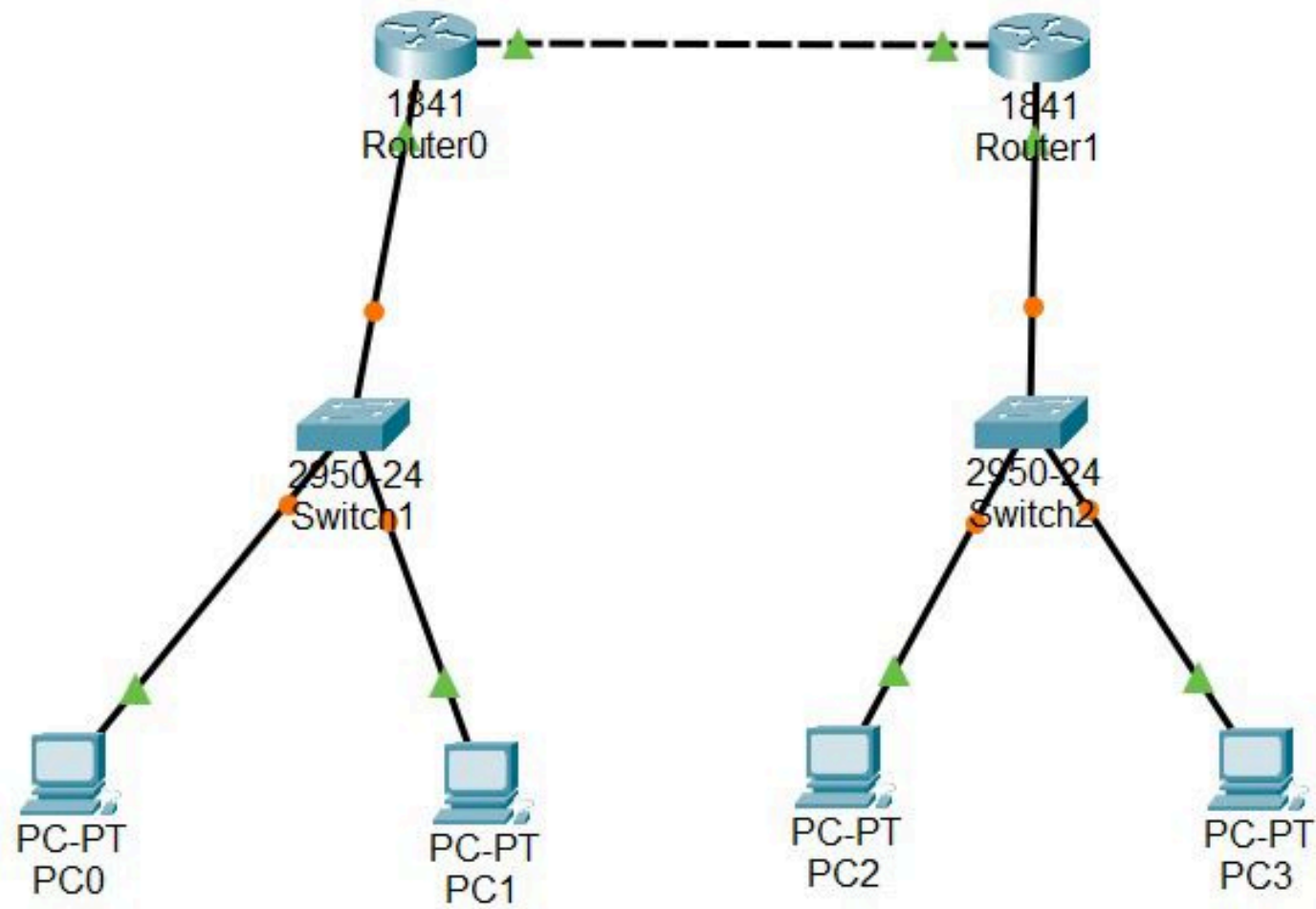


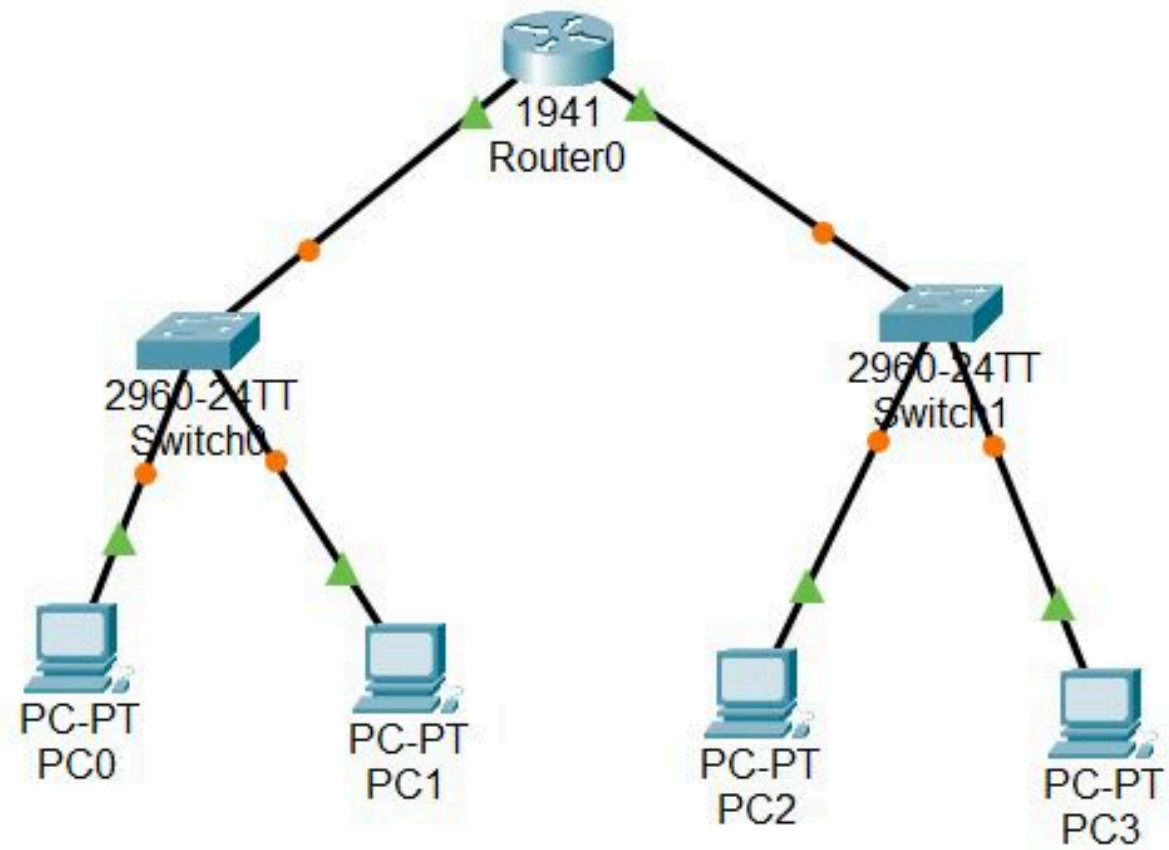


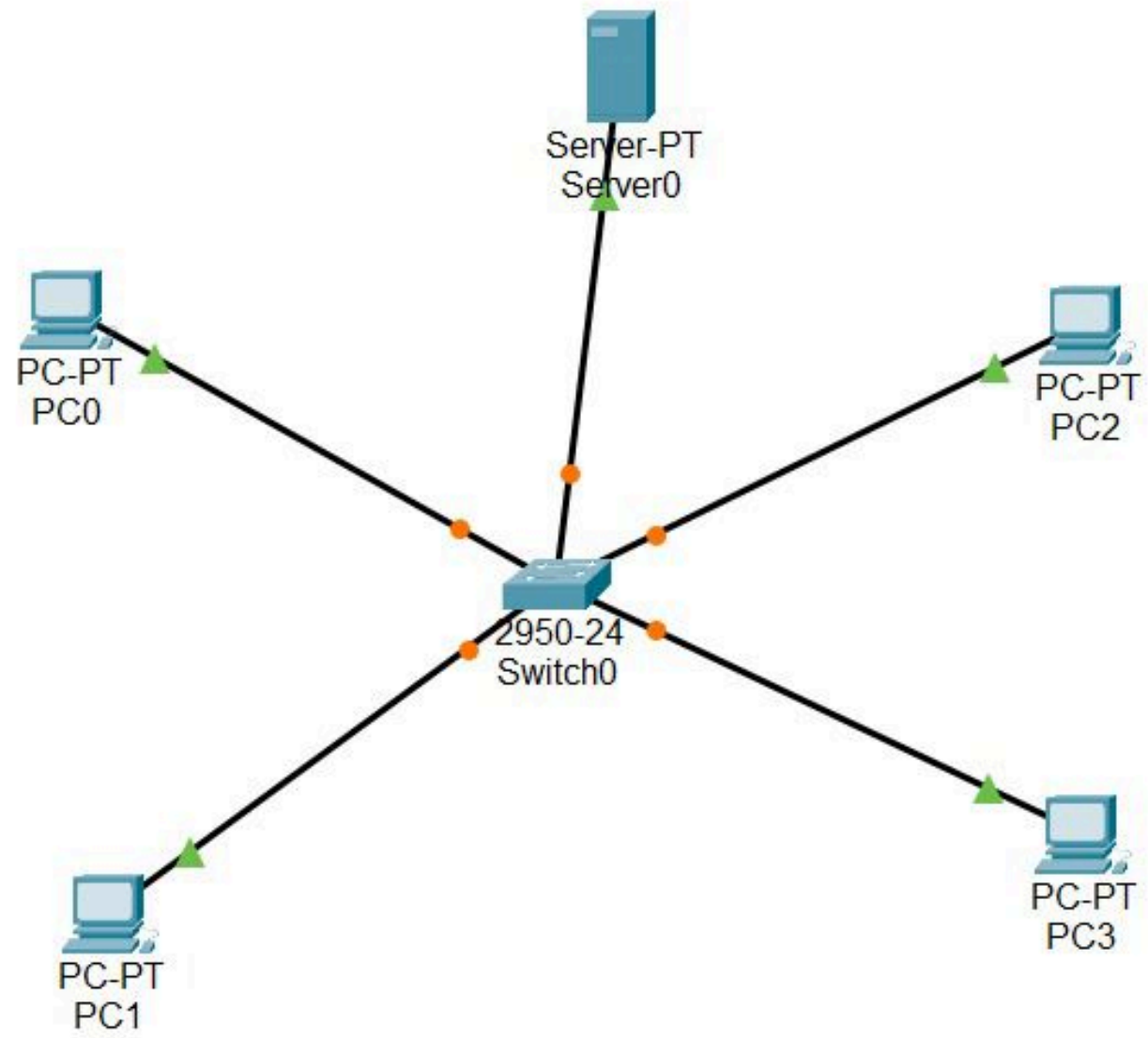
## Computer lab

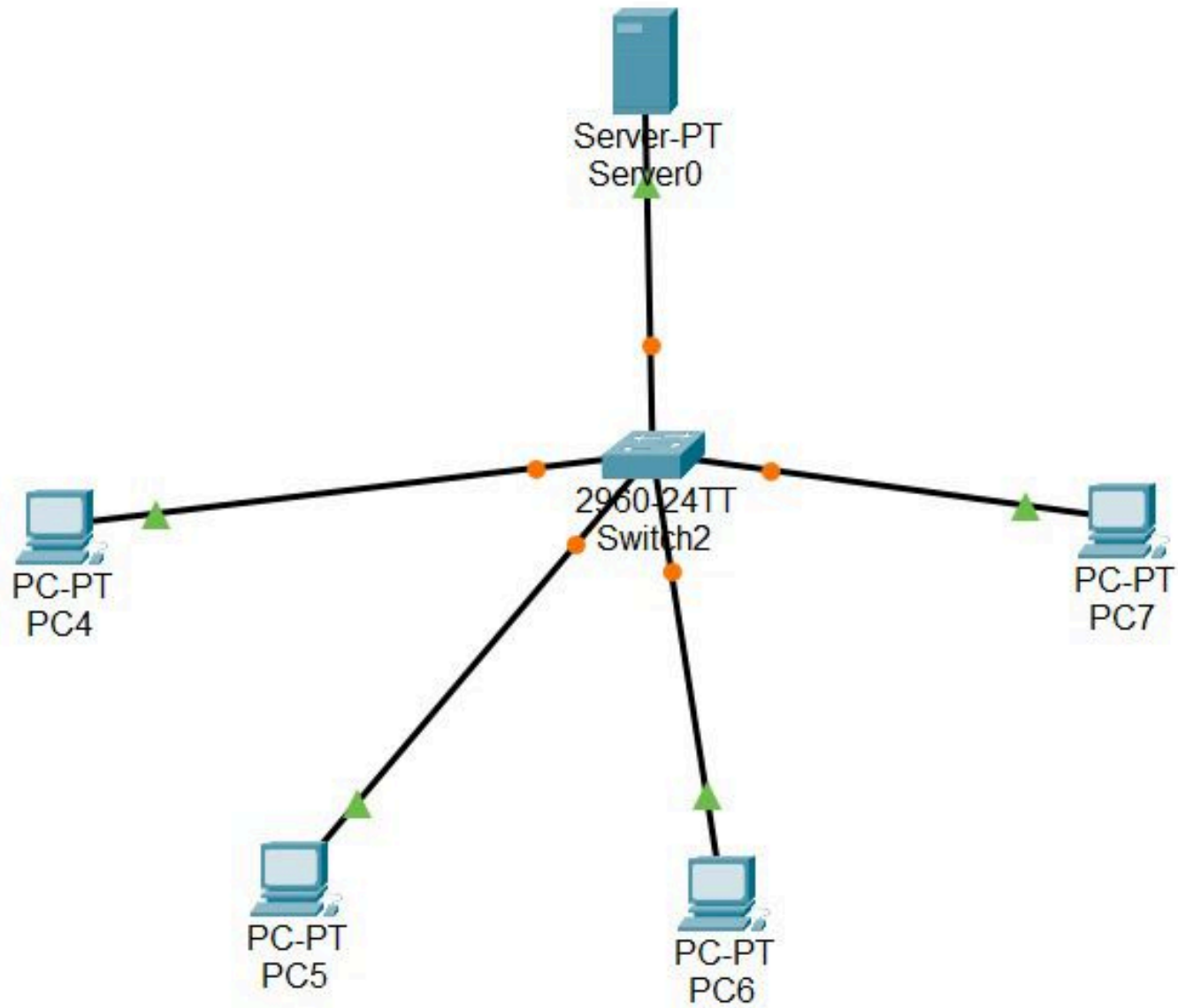


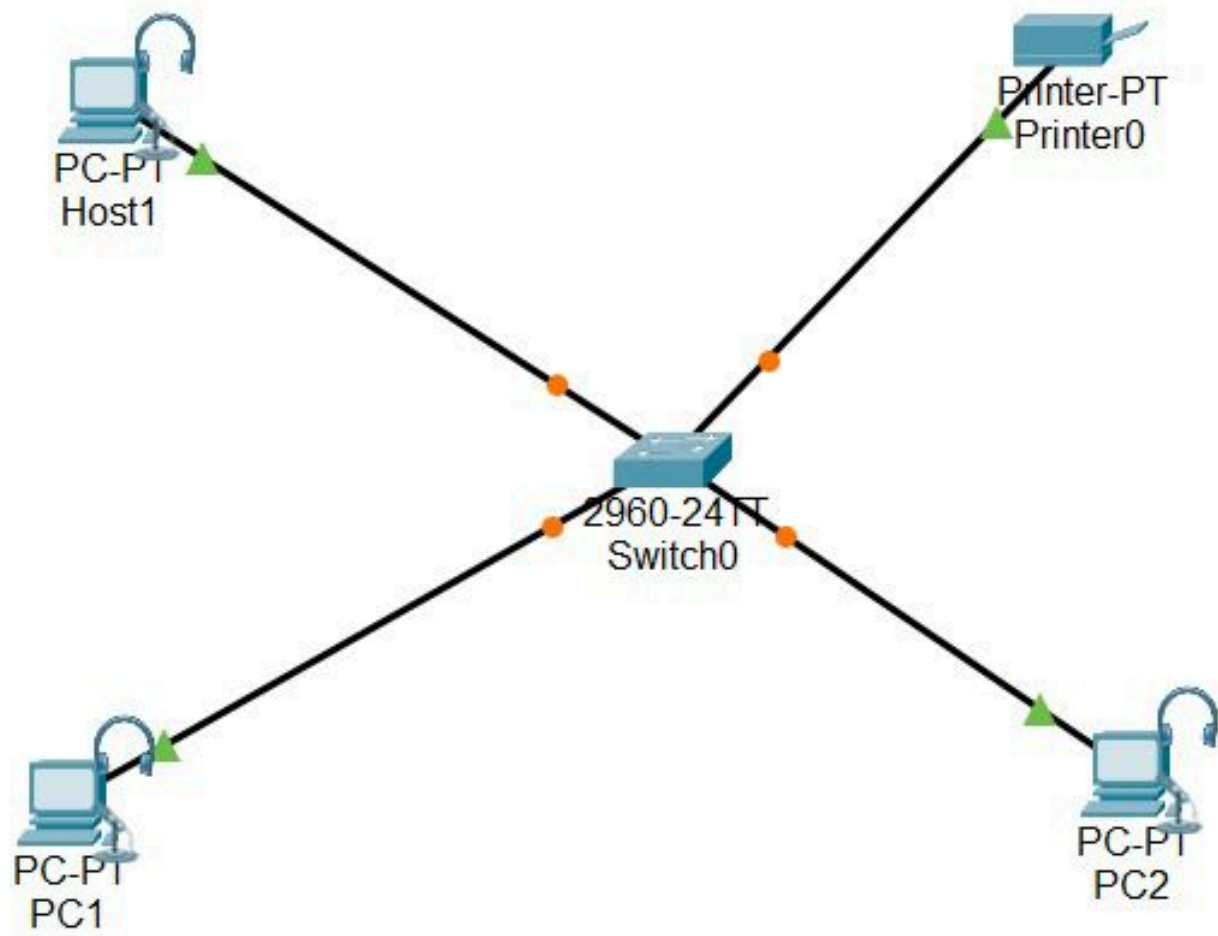
static routing

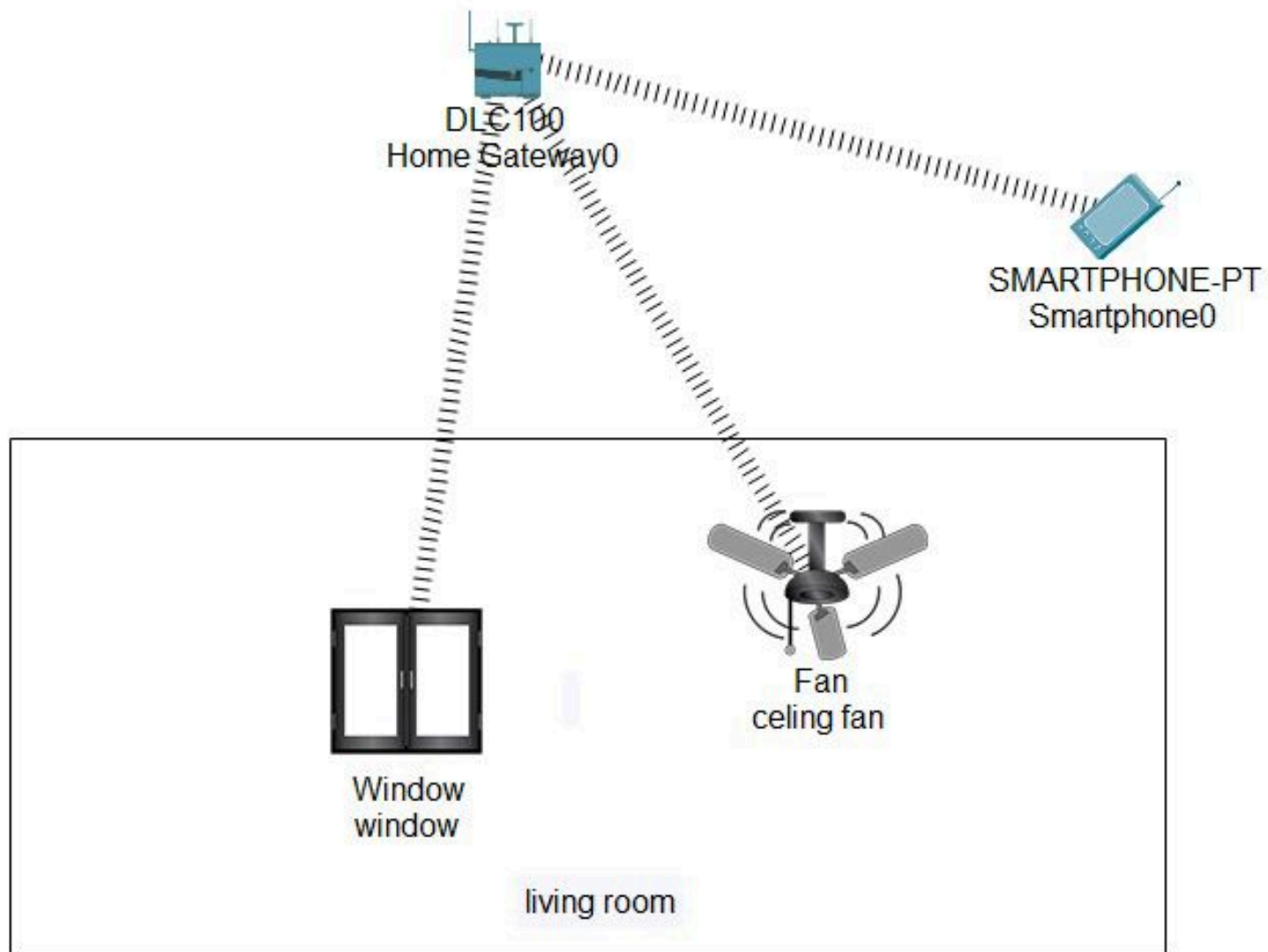


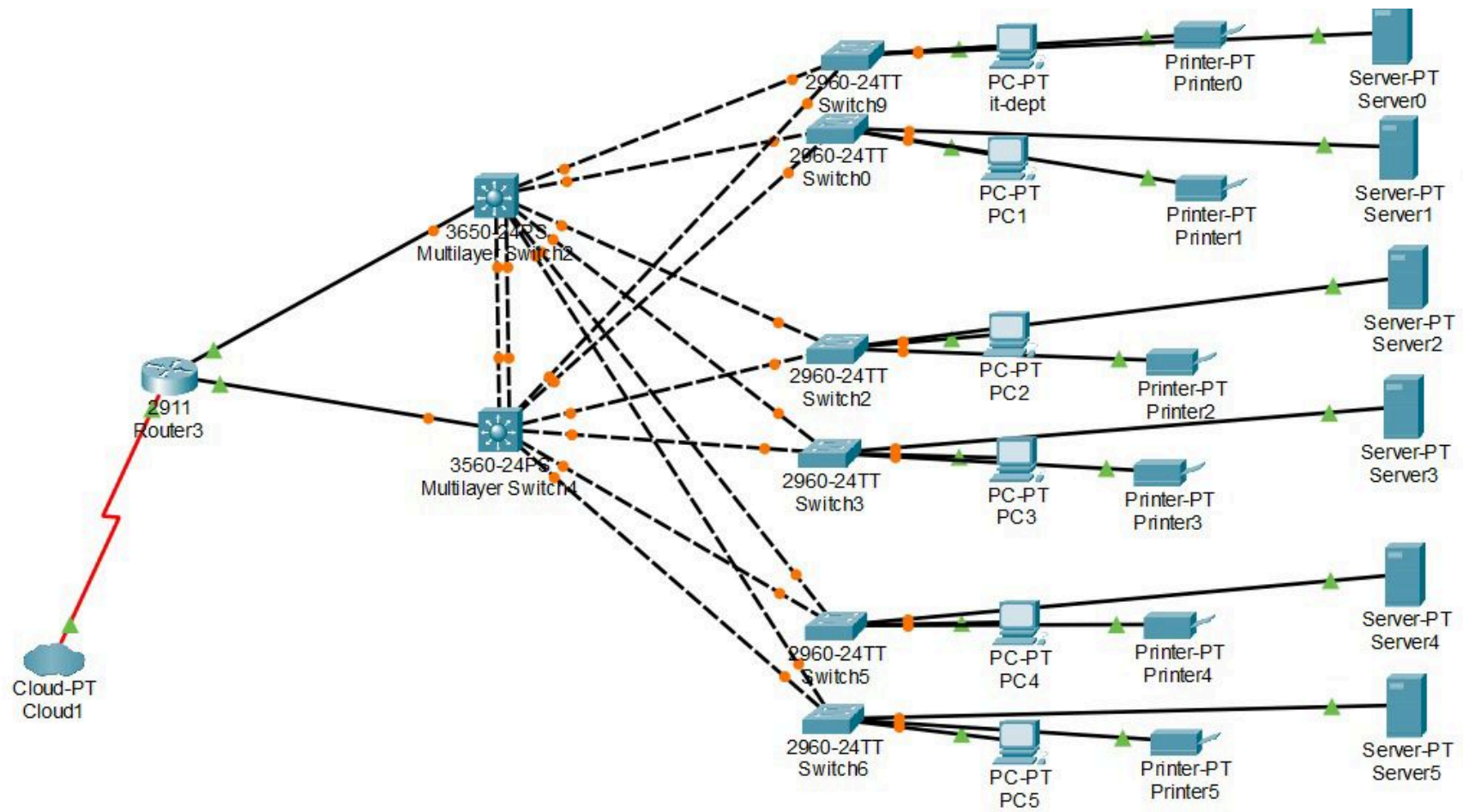






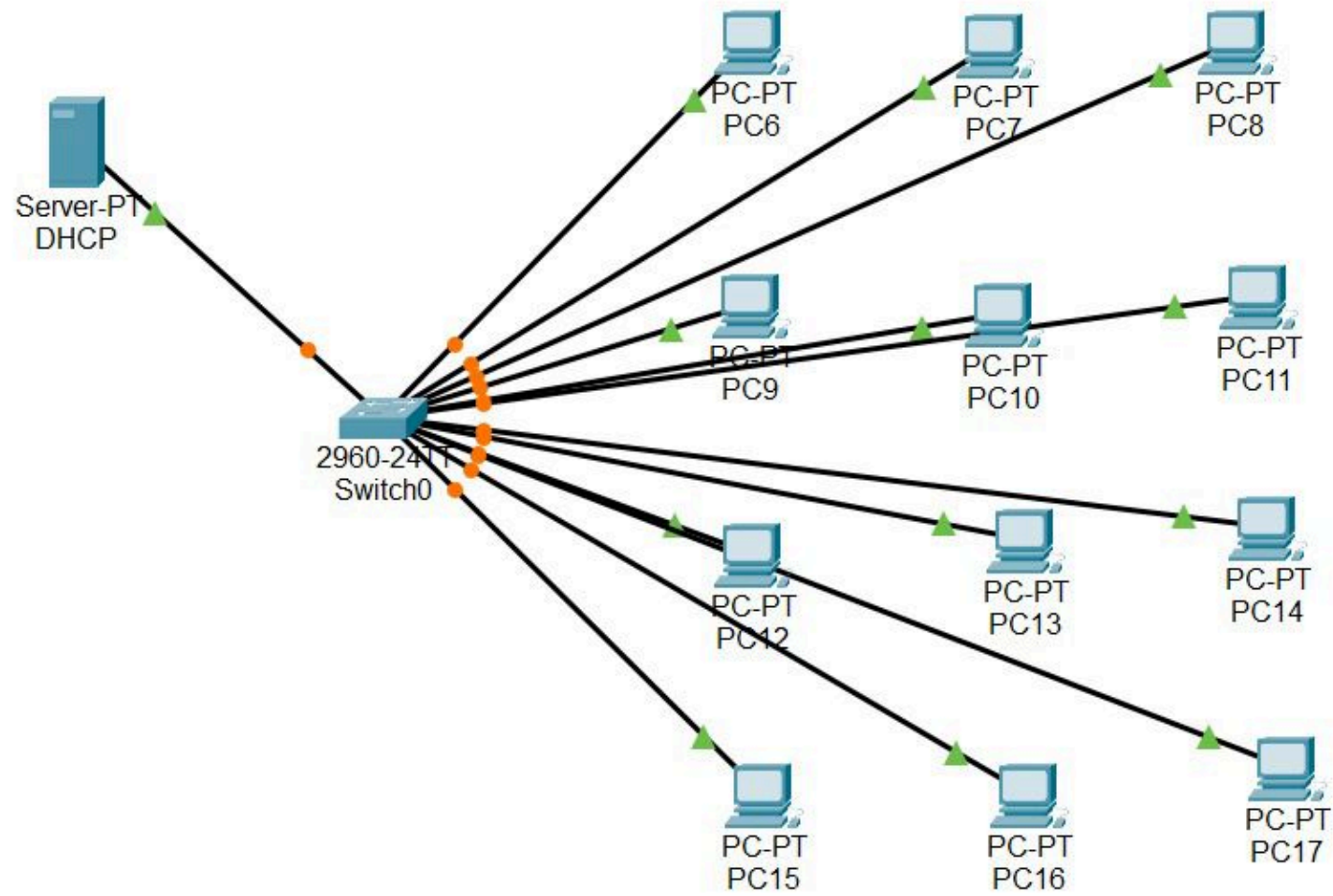


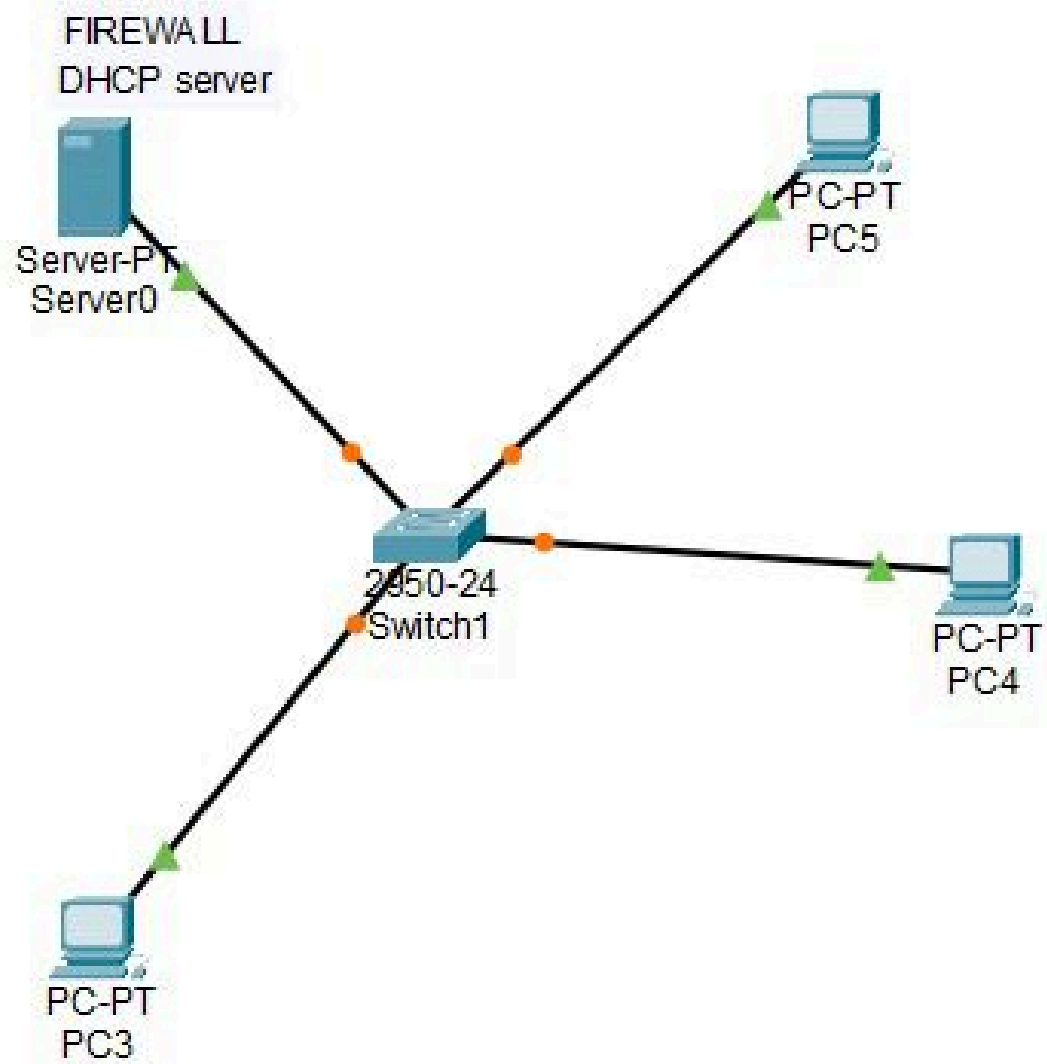


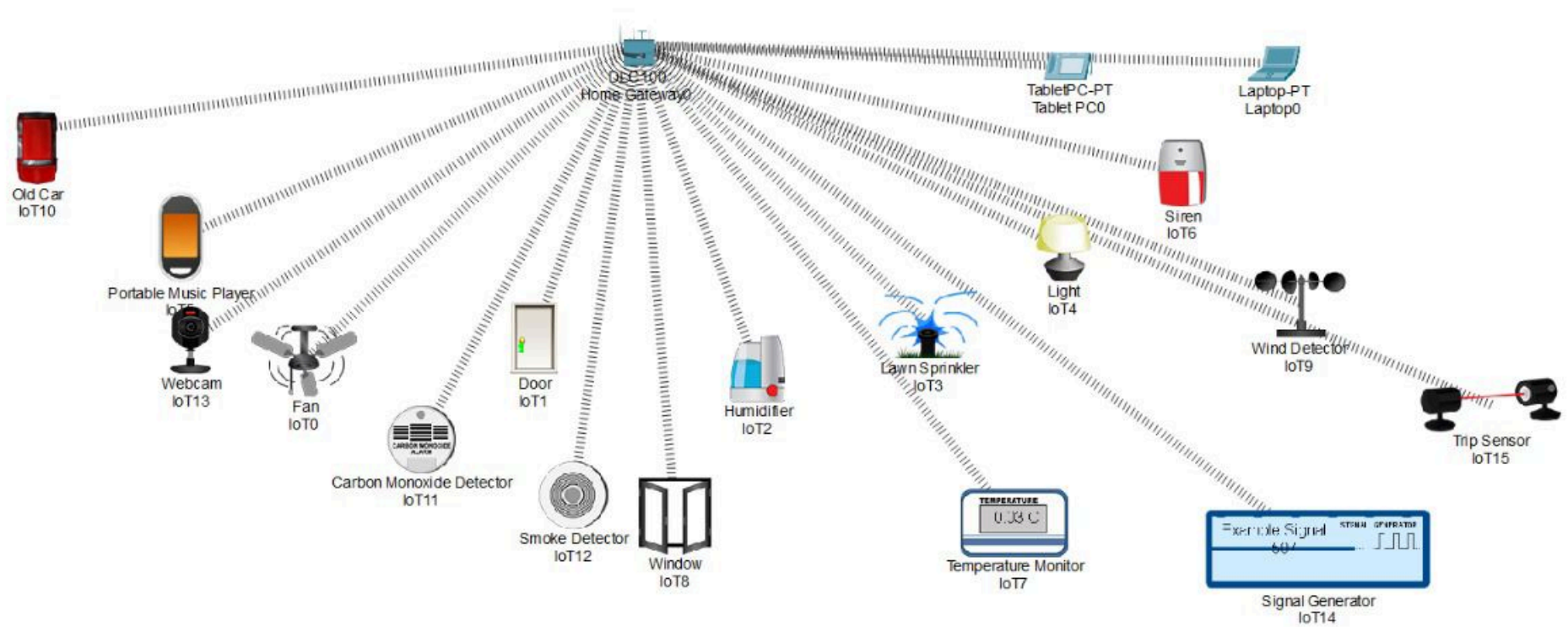


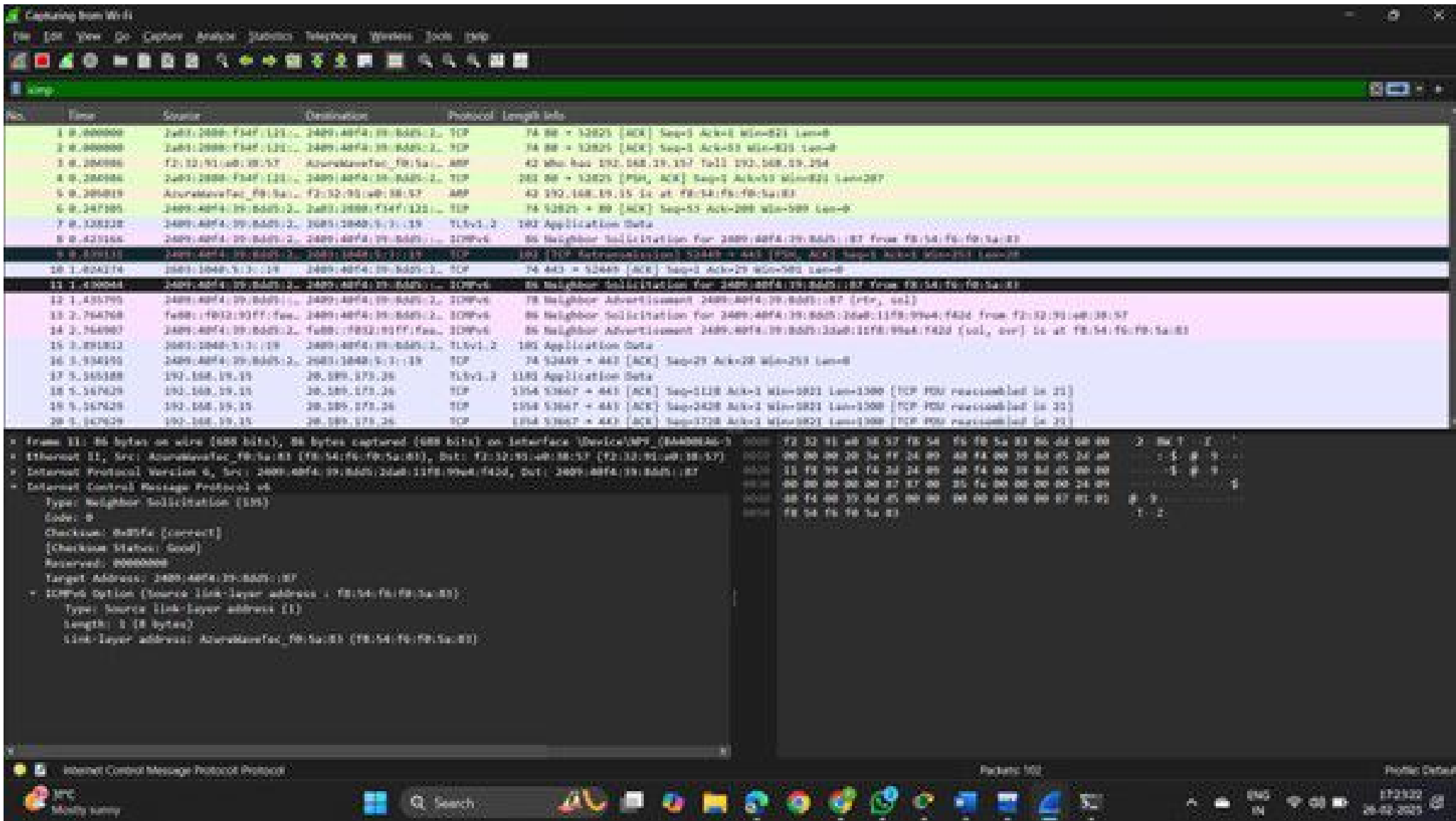


Computer lab









101	0.120645	192.168.186.197	223.196.146.77	UDP	81	62236 → 443	Len=39
102	0.120652	192.168.186.197	223.196.146.77	UDP	80	62236 → 443	Len=38

- Source: AzureWaveTec\_a4:43:01 (a8:41:f4:a4:43:01)  
Type: IPv4 (0x0800)  
[Stream index: 0]

- Internet Protocol Version 4, Src: 192.168.186.197, Dst: 216.239.38.223

- 0100 .... = Version: 4

- .... 0101 = Header Length: 20 bytes (5)

- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

- Total Length: 1195

- Identification: 0x19cd (6605)

- 010. .... = Flags: 0x2, Don't fragment

- ...0 0000 0000 0000 = Fragment Offset: 0

- Time to Live: 62

- Protocol: UDP (17)

- Header Checksum: 0xa338 [validation disabled]

- [Header checksum status: Unverified]

- Source Address: 192.168.186.197

- Destination Address: 216.239.38.223

- [Stream index: 0]

- User Datagram Protocol, Src Port: 62604, Dst Port: 443

- Source Port: 62604

- Destination Port: 443

- Length: 1175

- Checksum: 0xe7dc [unverified]

- [Checksum Status: Unverified]

- [Stream index: 0]

- [Stream Packet Number: 3]

- [Timestamps]

- UDP payload (1167 bytes)

- Data (1167 bytes)

- Data [...]: 45f48b9ec6180490719e858ebad1ae4f96227fd4808946eecf178cb9b7c4d4b7d0f6a5a5b1a9e9c6af67ae7a7

- [Length: 1167]

Wireshark interface showing a packet capture. The top pane displays a list of network packets. The middle pane shows the details of the selected packet (No. 22883). The bottom pane shows the raw packet data in hexadecimal and ASCII.

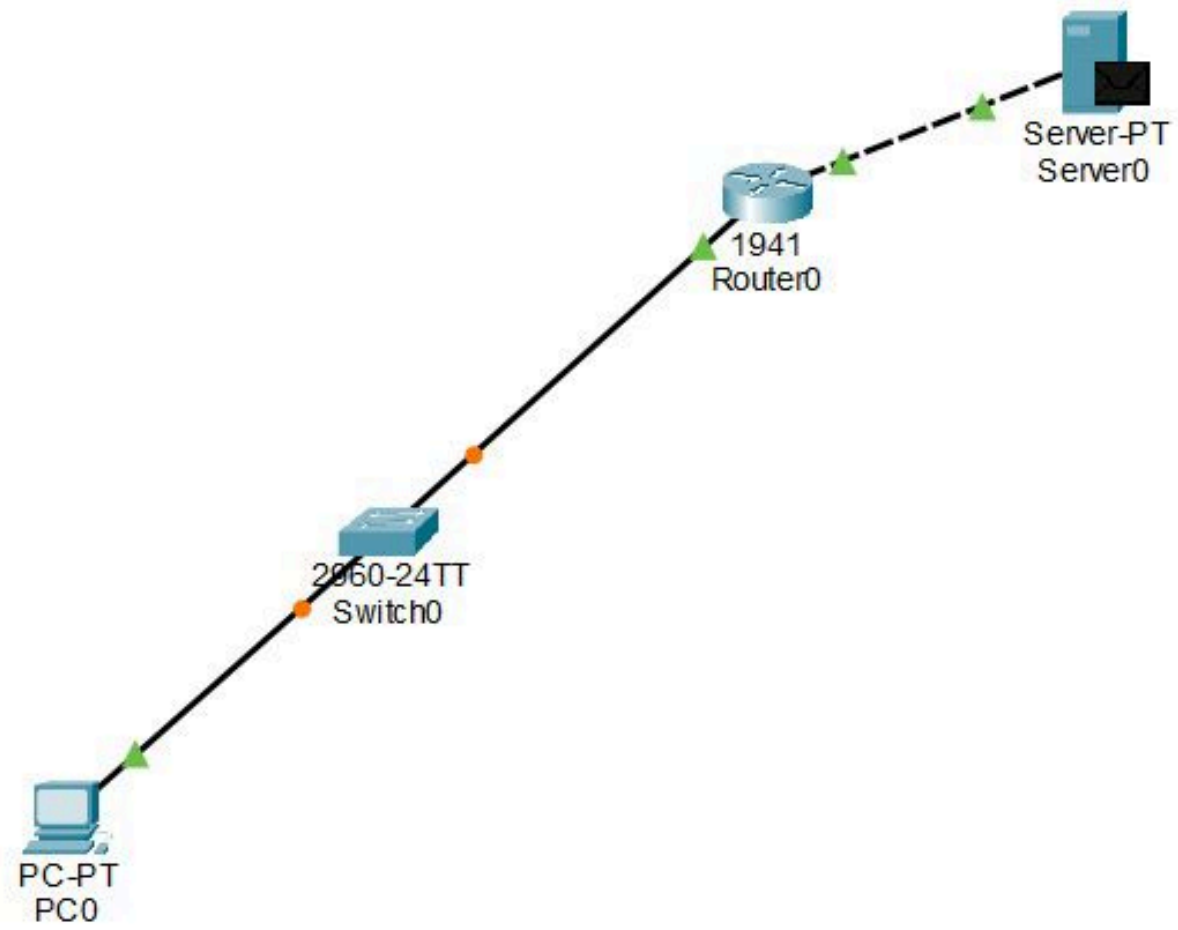
No.	Time	Source	Destination	Protocol	Length	Info
22794	359.795142	43.174.32.117	192.168.19.15	TCP	60	80 → 51786 [SYN, ACK] Seq=0 Ack=281 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=128
22795	359.798993	192.168.19.15	43.174.32.117	TCP	54	51786 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
22796	359.801286	192.168.19.15	43.174.32.117	HTTP	396	GET /msdownload/update/v1/static/trustedfr/en/authrootst1.cab?1551799364708f4c HTTP/1.1
22797	359.804836	28.249.168.26	192.168.19.15	Telnet	181	Application Data
22798	359.804836	43.174.32.117	192.168.19.15	TCP	54	80 → 51786 [ACK] Seq=1 Ack=281 Win=523904 Len=0
22799	359.804836	43.174.32.117	192.168.19.15	HTTP	357	HTTP/1.1 204 Not Modified
22800	359.806855	43.174.32.117	192.168.19.15	TCP	54	80 → 51786 [FIN, ACK] Seq=384 Ack=281 Win=523904 Len=0
22801	359.807639	192.168.19.15	43.174.32.117	TCP	54	51786 → 80 [FIN, ACK] Seq=281 Ack=384 Win=65535 Len=0
22802	359.917636	192.168.19.15	43.174.32.117	TCP	54	51786 → 80 [ACK] Seq=384 Ack=385 Win=65535 Len=0
22803	359.943652	43.174.32.117	192.168.19.15	TCP	54	[TCP Spurious Retransmission] 80 → 51786 [PSH, ACK] Seq=382 Ack=281 Win=523904 Len=1
22804	359.943987	192.168.19.15	28.249.168.26	TCP	54	52434 → 443 [ACK] Seq=487 Ack=330 Win=251 Len=0
22805	359.945593	192.168.19.15	43.174.32.117	TCP	66	[TCP Dup ACK 22803] 51786 → 80 [ACK] Seq=284 Ack=385 Win=65535 Len=0 501-382 501-383
22806	359.957993	43.174.32.117	192.168.19.15	TCP	54	[TCP Spurious Retransmission] 80 → 51786 [PSH, ACK] Seq=380 Ack=281 Win=523904 Len=1
22807	359.957993	43.174.32.117	192.168.19.15	TCP	54	80 → 51786 [ACK] Seq=385 Ack=284 Win=523904 Len=0
22808	359.958732	192.168.19.15	43.174.32.117	TCP	66	[TCP Dup ACK 22807] 51786 → 80 [ACK] Seq=384 Ack=385 Win=65535 Len=0 501-380 501-381
22809	370.215073	2489:40f4:39:8dd5::2	2489:1048:5:3::19	TLSv1.3	102	Application Data
22810	370.441637	2489:1048:5:3::19	2489:40f4:39:8dd5::2	TCP	74	443 → 51776 [ACK] Seq=4884 Ack=3018 Win=64128 Len=0
22811	372.515398	2489:40f4:39:8dd5::2	2489:1048:5:3::19	TLSv1.3	105	Application Data
22812	372.480382	2489:1048:5:3::19	2489:40f4:39:8dd5::2	TCP	74	443 → 51776 [ACK] Seq=4884 Ack=3049 Win=64128 Len=0
22813	372.817793	2489:1048:5:3::19	2489:40f4:39:8dd5::2	TLSv1.3	181	Application Data

Frame 22803: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF\_{...} Ethernet II, Src: F2:32:9D:A0:10:57 (F2:32:9D:A0:10:57), Dst: AzureWaveTec\_F0:54:1F:70:5... Internet Protocol Version 4, Src: 43.174.32.117, Dst: 192.168.19.15 Transmission Control Protocol, Src Port: 80, Dst Port: 51786, Seq: 382, Ack: 281, Len: 1

Source Port: 80  
Destination Port: 51786  
[Stream index: 92]  
[Stream Packet Number: 10]  
[Conversation completeness: Complete, WITH\_DATA [91]]  
[TCP Segment Len: 1]  
Sequence Number: 382 (relative sequence number)  
Sequence Number (raw): 827054389  
[Next Sequence Number: 393 (relative sequence number)]  
Acknowledgment Number: 281 (relative ack number)  
Acknowledgment number (raw): 486155773  
0001 ..... = Header Length: 20 bytes (5)  
Flags: 0x018 [PSH, ACK]  
Window: 4883  
[Calculated window size: 523904]  
[Window size scaling factor: 128]  
[...]

Packets: 27358 - Displayed: 5241 (19.0%) - Dropped: 0 (0.0%) Profile: Default

AFD - ENG Live



C:\Users\gustaf\OneDrive\Doc x + v - □ x

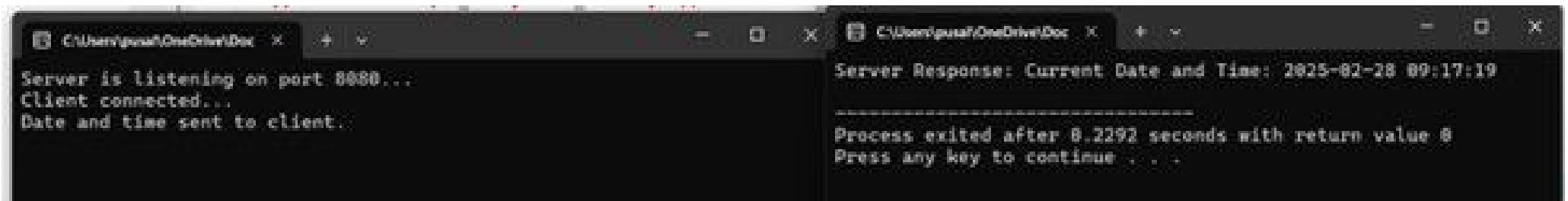
```
DNS Server listening on port 8080...  
Received request for domain: google.com  
Resolved IP: 142.250.183.238  
|
```

C:\Users\gustaf\OneDrive\Doc x + v

```
Enter domain name: google.com  
Resolved IP: 142.250.183.238
```

```
-----  
Process exited after 16.29 seconds with return value 0  
Press any key to continue . . .
```





The image shows two side-by-side Windows command prompt windows. The left window, titled 'C:\Users\guaf\OneDrive\Doc', contains the following text: 'Server is listening on port 8080...', 'Client connected...', and 'Date and time sent to client.'. The right window, titled 'C:\Users\guaf\OneDrive\Doc', contains the following text: 'Server Response: Current Date and Time: 2025-02-28 09:17:19', a separator line of dashes, 'Process exited after 8.2292 seconds with return value 0', and 'Press any key to continue . . .'. Both windows have standard Windows window controls (minimize, maximize, close) in their title bars.

```
C:\Users\guaf\OneDrive\Doc > Server is listening on port 8080...
C:\Users\guaf\OneDrive\Doc > Client connected...
C:\Users\guaf\OneDrive\Doc > Date and time sent to client.

C:\Users\guaf\OneDrive\Doc > Server Response: Current Date and Time: 2025-02-28 09:17:19
C:\Users\guaf\OneDrive\Doc > -----
C:\Users\guaf\OneDrive\Doc > Process exited after 8.2292 seconds with return value 0
C:\Users\guaf\OneDrive\Doc > Press any key to continue . . .
```

Capturing from Wi-Fi

File Edit View Go Capture Analysis Statistics Telephony Windows Tools Help

Wi-Fi

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.147 (12)	192.168.1.1 (1)	TCP	74	80 → 52825 [ACK] Seq=5 Ack=83 Win=824 Len=0
2	0.000000	192.168.1.147 (12)	192.168.1.1 (1)	TCP	74	80 → 52825 [ACK] Seq=5 Ack=83 Win=824 Len=0
3	0.000000	F2:32:9D:40:38:57	AzureWaveFec_F0:54:76:F0:54:83	ARP	42	who has 192.168.1.1? TxID 192.168.1.1.154
4	0.000000	192.168.1.147 (12)	192.168.1.1 (1)	TCP	74	80 → 52825 [PSH, ACK] Seq=5 Ack=83 Win=824 Len=287
5	0.000000	AzureWaveFec_F0:54:76:F0:54:83	F2:32:9D:40:38:57	ARP	42	192.168.1.1.154 is at F0:54:76:F0:54:83
6	0.000000	192.168.1.1 (1)	192.168.1.147 (12)	TCP	74	52825 → 80 [ACK] Seq=57 Ack=288 Win=569 Len=0
7	0.000000	192.168.1.1 (1)	192.168.1.147 (12)	TCP	182	Application Data
8	0.000000	192.168.1.1 (1)	192.168.1.147 (12)	TCP	86	Neighbor Solicitation for 192.168.1.147 from F0:54:76:F0:54:83
9	0.000000	192.168.1.1 (1)	192.168.1.147 (12)	TCP	182	TCP Retransmission 52825 → 443 [PSH, ACK] Seq=5 Ack=1 Win=256 Len=28
10	0.000000	192.168.1.1 (1)	192.168.1.147 (12)	TCP	74	443 → 52825 [ACK] Seq=27 Ack=28 Win=569 Len=0
11	0.000000	192.168.1.1 (1)	192.168.1.147 (12)	TCP	86	Neighbor Solicitation for 192.168.1.147 from F0:54:76:F0:54:83
12	0.000000	192.168.1.1 (1)	192.168.1.147 (12)	TCP	78	Neighbor Advertisement 192.168.1.147 (rtr, v2)
13	0.000000	F0:54:76:F0:54:83	192.168.1.147 (12)	TCP	86	Neighbor Solicitation for 192.168.1.147 from F2:32:9D:40:38:57
14	0.000000	192.168.1.1 (1)	F0:54:76:F0:54:83	TCP	86	Neighbor Advertisement 192.168.1.147 (v2, v2) is at F0:54:76:F0:54:83
15	0.000000	192.168.1.1 (1)	192.168.1.147 (12)	TCP	182	Application Data
16	0.000000	192.168.1.1 (1)	192.168.1.147 (12)	TCP	74	52825 → 443 [ACK] Seq=27 Ack=28 Win=256 Len=0
17	0.000000	192.168.1.1 (1)	192.168.1.147 (12)	TCP	1182	Application Data
18	0.000000	192.168.1.1 (1)	192.168.1.147 (12)	TCP	1184	52827 → 443 [ACK] Seq=2128 Ack=1 Win=824 Len=1000 [TCP RST received in 21]
19	0.000000	192.168.1.1 (1)	192.168.1.147 (12)	TCP	1184	52827 → 443 [ACK] Seq=2428 Ack=1 Win=824 Len=1000 [TCP RST received in 22]
20	0.000000	192.168.1.1 (1)	192.168.1.147 (12)	TCP	1184	52827 → 443 [ACK] Seq=2728 Ack=1 Win=824 Len=1000 [TCP RST received in 23]

Frame 9: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 10vnet0/80 [8A000000-8F]

Ethernet II, Src: AzureWaveFec\_F0:54:76:F0:54:83, Dst: F2:32:9D:40:38:57 (F2:32:9D:40:38:57)

Address Resolution Protocol (reply)

Hardware type: Ethernet II

Protocol type: IPv4 (800000)

Hardware size: 6

Protocol size: 8

Opcode: reply (2)

Sender MAC address: AzureWaveFec\_F0:54:76:F0:54:83

Sender IP address: 192.168.1.1

Target MAC address: F2:32:9D:40:38:57 (F2:32:9D:40:38:57)

Target IP address: 192.168.1.147

Address Resolution Protocol Protocol

Packets: 1000

Profile: Default

100% Mostly empty

Search

17:24:11 26-02-2025



C:\Users\pusal\OneDrive\Doc



Usage: C:\Users\pusal\OneDrive\Documents\28.exe <hostname>

-----

Process exited after 0.2221 seconds with return value 1

Press any key to continue . . . |



C:\Users\pusal\OneDrive\Doc X



Enter target IP address: 192.168.1.1

MAC Address of 192.168.1.1: 24:D5:E4:6D:C0:D7

-----

Process exited after 4.804 seconds with return value 0

Press any key to continue . . . |

Wireshark interface showing a network capture. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, and Length. The middle pane shows the details of the selected packet (No. 22799), including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The bottom pane displays the raw packet data in hexadecimal and ASCII. The status bar at the bottom indicates the current packet count and profile.

No.	Time	Source	Destination	Protocol	Length	Info
22789	359.474526	192.168.19.15	43.174.32.117	TCP	60	51786 → 80 [SYN] Seq=8 win=65535 len=0 MSS=1460 WS=256 SACK_PERM
22790	359.705485	192.168.19.15	28.249.248.26	HTTP/1.1	112	Application Data
22791	359.742849	2489.4894.39.8425...	2489.4894.39.8425...2	DNS	212	Standard query response 0x0fac AAAA ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com.delivery.microsoft.com CNAME ws-b-net-
22792	359.742849	2489.4894.39.8425...	2489.4894.39.8425...2	DNS	212	Standard query response 0x0fac A ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com.delivery.microsoft.com CNAME ws-b-net-
22793	359.742947	2489.4894.39.8425...	2489.4894.39.8425...	DNS	48	Destination unreachable (Port unreachable)
22794	359.795543	43.174.32.117	192.168.19.15	TCP	60	80 → 51786 [SYN, ACK] Seq=8 Ack=3 win=65535 len=0 MSS=1460 SACK_PERM WS=256
22795	359.798993	192.168.19.15	43.174.32.117	TCP	60	51786 → 80 [ACK] Seq=1 Ack=3 win=65535 len=0
22796	359.801286	192.168.19.15	43.174.32.117	HTTP	108	GET /windowsupdate/v3/static/trustadw/en/authroastd1.cab?35179934098fa HTTP/1.1
22797	359.894836	28.249.248.26	192.168.19.15	HTTP/1.1	180	Application Data
22798	359.894836	43.174.32.117	192.168.19.15	TCP	60	80 → 51786 [ACK] Seq=1 Ack=281 win=527984 len=0
22799	359.894836	43.174.32.117	192.168.19.15	HTTP	252	HTTP/1.1 204 Not Modified
22800	359.896855	43.174.32.117	192.168.19.15	TCP	60	80 → 51786 [FIN, ACK] Seq=284 Ack=281 win=527984 len=0
22801	359.897439	192.168.19.15	43.174.32.117	TCP	60	51786 → 80 [FIN, ACK] Seq=285 Ack=284 win=65535 len=0
22802	359.907636	192.168.19.15	43.174.32.117	TCP	60	51786 → 80 [ACK] Seq=284 Ack=285 win=527984 len=0
22803	359.943632	43.174.32.117	192.168.19.15	TCP	15	212 Standard query response 0x0fac A ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com.delivery.microsoft.com CNAME ws-b-net-
22804	359.943632	192.168.19.15	28.249.248.26	TCP	60	51786 → 80 [ACK] Seq=287 Ack=281 win=527984 len=0
22805	359.943632	192.168.19.15	43.174.32.117	TCP	60	51786 → 80 [ACK] Seq=284 Ack=285 win=527984 len=0
22806	359.943632	43.174.32.117	192.168.19.15	TCP	15	212 Standard query response 0x0fac A ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com.delivery.microsoft.com CNAME ws-b-net-
22807	359.943632	43.174.32.117	192.168.19.15	TCP	60	80 → 51786 [ACK] Seq=285 Ack=284 win=527984 len=0
22808	359.943632	192.168.19.15	43.174.32.117	TCP	60	51786 → 80 [ACK] Seq=284 Ack=285 win=527984 len=0

Frame 22799: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface Wireshark (0x000000000000) [Ethernet II, Src: 72:53:00:00:00:00, Dst: 08:00:27:00:00:00] [Internet Protocol Version 4, Src: 43.174.32.117, Dst: 192.168.19.15] [Transmission Control Protocol, Src Port: 80, Dst Port: 51786, Seq: 1, Ack: 281, Len: 252] [Hypertext Transfer Protocol]

HTTP/1.1 204 Not Modified

Cache-Control: public, max-age=300

Content-Type: application/vnd.ms-cab-compressed

Date: Tue, 29 Feb 2022 19:22:48 GMT

X-MS-CDN-UUID: 1176688527256676

Connection: close

Server: IIS/10.0

X-Cache-Lookup: Cache Hit

X-Cache: Hit

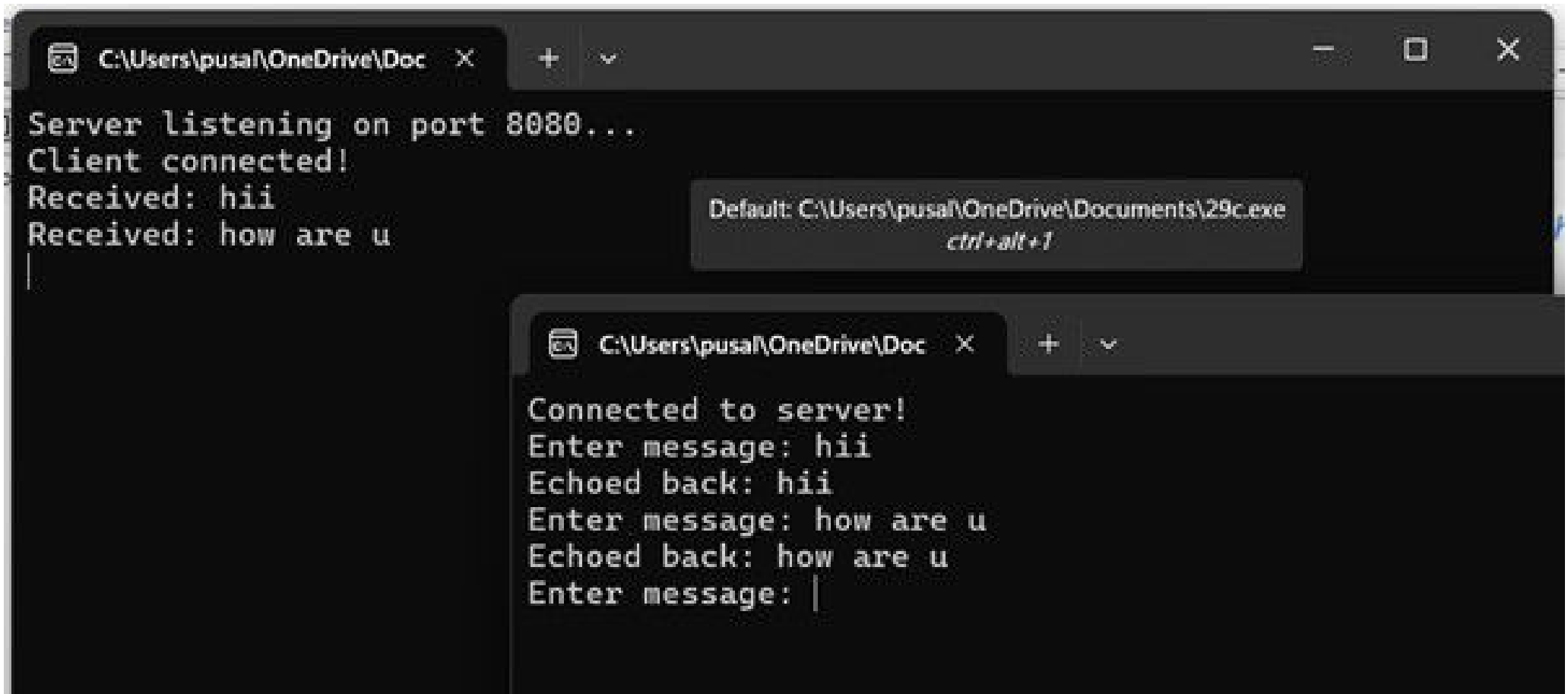
X-Content-Type: application/vnd.ms-cab-compressed

[Time since request: 0.000000000 seconds]

[Request URI: /windowsupdate/v3/static/trustadw/en/authroastd1.cab?35179934098fa]

Packets: 27256 - Dropped: 0 (0.0%)

Profile: Default

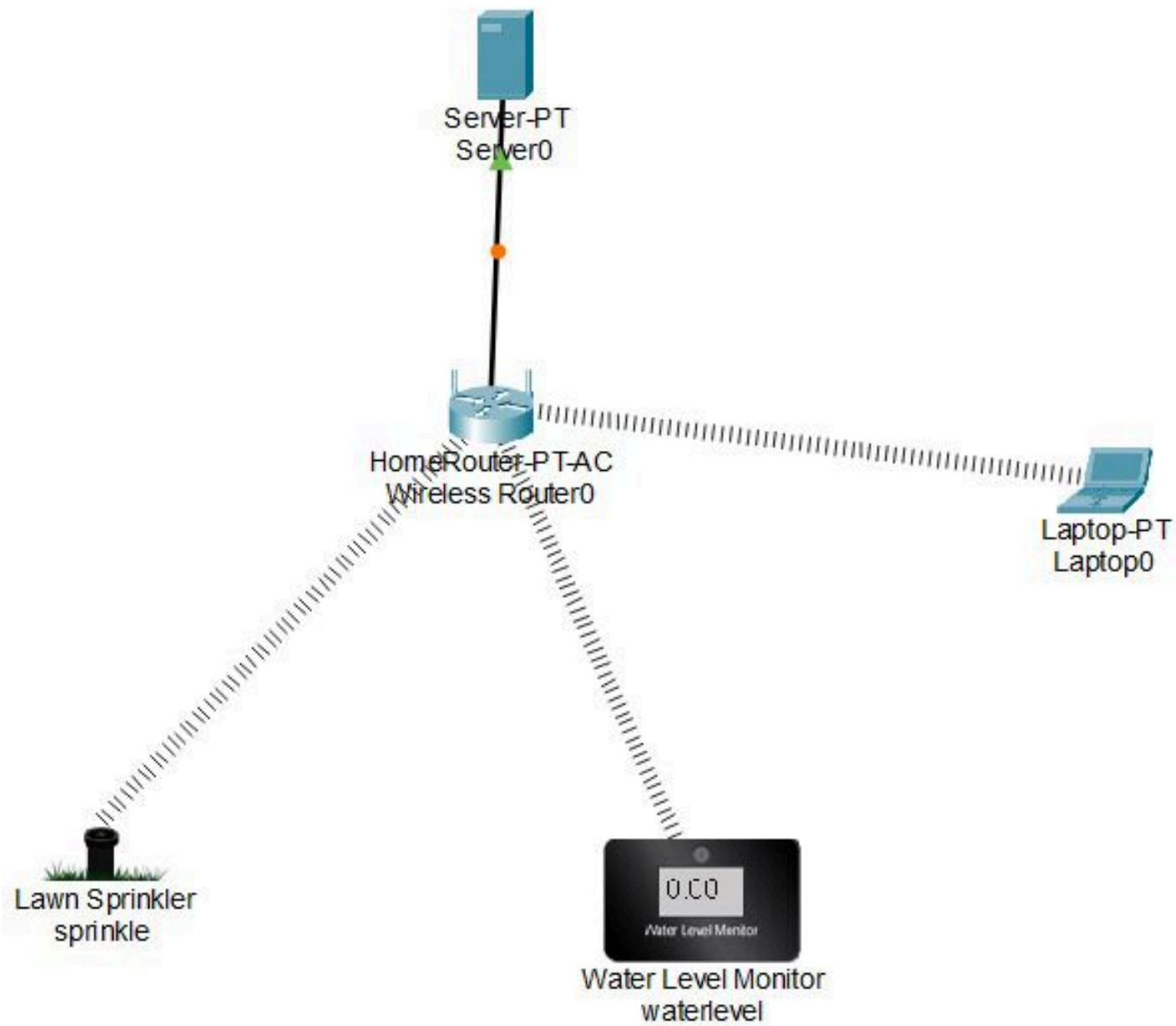


The image shows two overlapping terminal windows. The top window, titled 'C:\Users\pusa\OneDrive\Doc', displays server-side logs: 'Server listening on port 8080...', 'Client connected!', 'Received: hii', and 'Received: how are u'. A tooltip above it shows 'Default: C:\Users\pusa\OneDrive\Documents\29c.exe' and 'ctrl+alt+1'. The bottom window, also titled 'C:\Users\pusa\OneDrive\Doc', displays client-side logs: 'Connected to server!', 'Enter message: hii', 'Echoed back: hii', 'Enter message: how are u', 'Echoed back: how are u', and 'Enter message: '.

```
C:\Users\pusa\OneDrive\Doc X + - □ X
Server listening on port 8080...
Client connected!
Received: hii
Received: how are u
|

Default: C:\Users\pusa\OneDrive\Documents\29c.exe
ctrl+alt+1

C:\Users\pusa\OneDrive\Doc X + - □ X
Connected to server!
Enter message: hii
Echoed back: hii
Enter message: how are u
Echoed back: how are u
Enter message: |
```



Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

100%

No.	Time	Source	Destination	Protocol	Length	Info
68	8.704753	2404:6800:4002:815::	2409:40f4:39:8405:2::	QUIC	182	Protected Payload (KPB)
69	8.704753	2404:6800:4002:815::	2409:40f4:39:8405:2::	QUIC	87	Protected Payload (KPB)
70	8.712005	2409:40f4:39:8405:2::	2404:6800:4002:815::	QUIC	94	Protected Payload (KPB), CCID=sha3757dec31621
71	8.806133	2404:6800:4002:815::	2409:40f4:39:8405:2::	QUIC	1292	Protected Payload (KPB)
72	8.806882	2409:40f4:39:8405:2::	2404:6800:4002:815::	QUIC	95	Protected Payload (KPB), CCID=sha3757dec31621
73	9.062811	192.168.19.15	28.189.173.14	TCP	55	53685 → 443 [ACK] Seq=1 A/R=1 Win=256 Len=0
74	9.728514	28.189.173.14	192.168.19.15	TCP	64	443 → 53685 [ACK] Seq=1 Ack=2 Win=16384 Len=0 MSS=1 MSS=2
75	11.715218	2409:40f4:39:8405:2::	2603:1040:a03:9:11b6	TLSv1.2	125	Application Data
76	12.908988	2603:1040:a03:9:11b6	2409:40f4:39:8405:2::	TLSv1.2	124	Application Data
77	12.831660	2409:40f4:39:8405:2::	2603:1040:a03:9:11b6	TCP	74	53685 → 443 [ACK] Seq=32 Ack=41 Win=253 Len=0
78	14.828688	f400::f802:91ff:fe00::f402::1	f402::1	ICMPv6	142	Router Advertisement from f2:32:91:a0:38:57
79	15.053331	2603:1040:3282:14::3	2409:40f4:39:8405:2::	TLSv1.2	187	Application Data
80	15.184234	2409:40f4:39:8405:2::	2603:1040:3282:14::3	TCP	74	52938 → 443 [ACK] Seq=1 Ack=47 Win=253 Len=0
81	15.667754	2405:200:1687:1731::	2409:40f4:39:8405:2::	UDP	93	443 → 62483 Len=31
82	15.696104	2409:40f4:39:8405:2::	2405:200:1687:1731::	UDP	94	62483 → 443 Len=32
83	16.316584	192.168.19.15	13.187.42.32	TCP	64	53685 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
84	16.345131	192.168.19.15	13.187.42.32	TCP	64	53685 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
85	16.377328	13.187.42.32	192.168.19.15	TCP	64	443 → 53685 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
86	16.377646	192.168.19.15	13.187.42.32	TCP	64	53685 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
87	16.379198	2405:200:1687:1731::	2409:40f4:39:8405:2::	UDP	86	443 → 62483 Len=34

Frame 81: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF\_{6A4006-...}

Ethernet II, Src: F2:32:91:a0:38:57 (F2:32:91:a0:38:57), Dst: AzureWaveTec\_F0:5a:83 (F0:5a:f6:f0:5a:83)

Internet Protocol Version 4, Src: 2405:200:1687:1731::132c:5f9b, Dst: 2409:40f4:39:8405:2:a0:11fb:06

User Datagram Protocol, Src Port: 443, Dst Port: 62483

Data (31 bytes)

Data: 593b7267a92b0d52b0d4f9840ba29afca07352a6f04aa2353fca4bfa [length: 31]

0000 59 3b 72 67 a9 2b 0d 52 b0 d4 f9 84 0b a2 9a fc a0 73 52 a6 f0 4a a2 35 3f ca 4b fa

0010 00

0020 00

0030 11 f8 99 a4 f4 2d 01 00 f3 c3 00 22 9c 21 19 3b

0040 77 a7 a9 2b 0d 05 2b a0 4f a9 04 00 a2 9a fa 1a

0050 00 73 52 14 3d 34 0a a1 35 3f ac 0b fa

0060