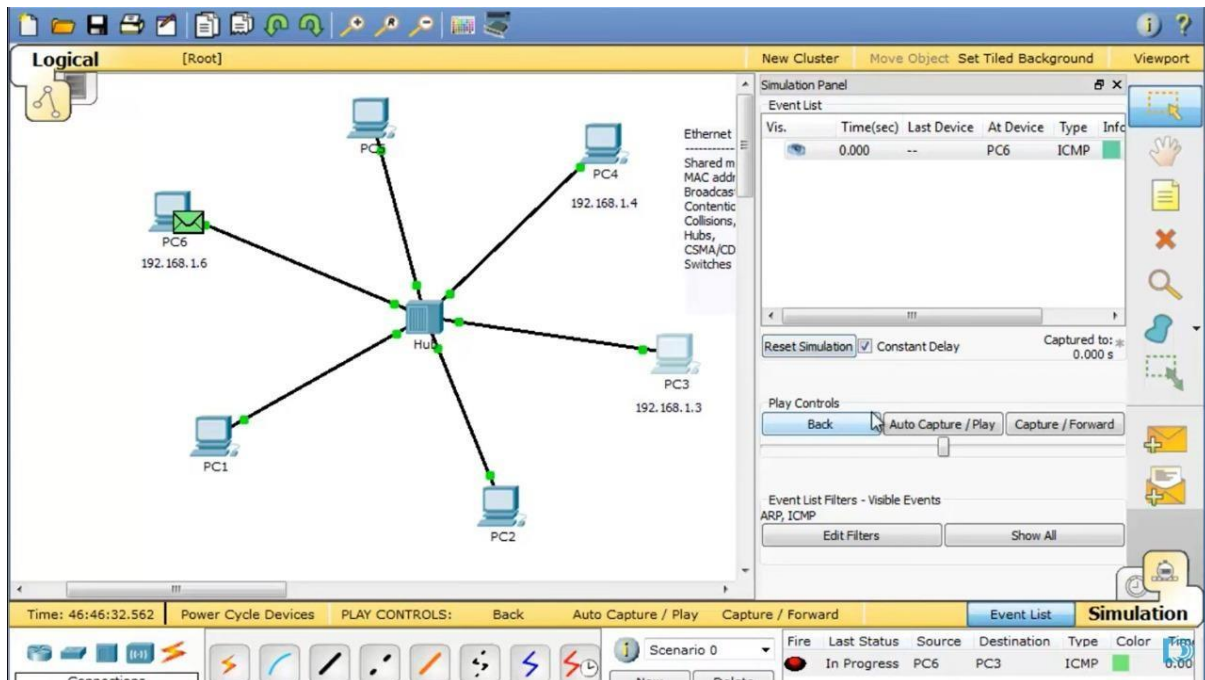


CSA-07

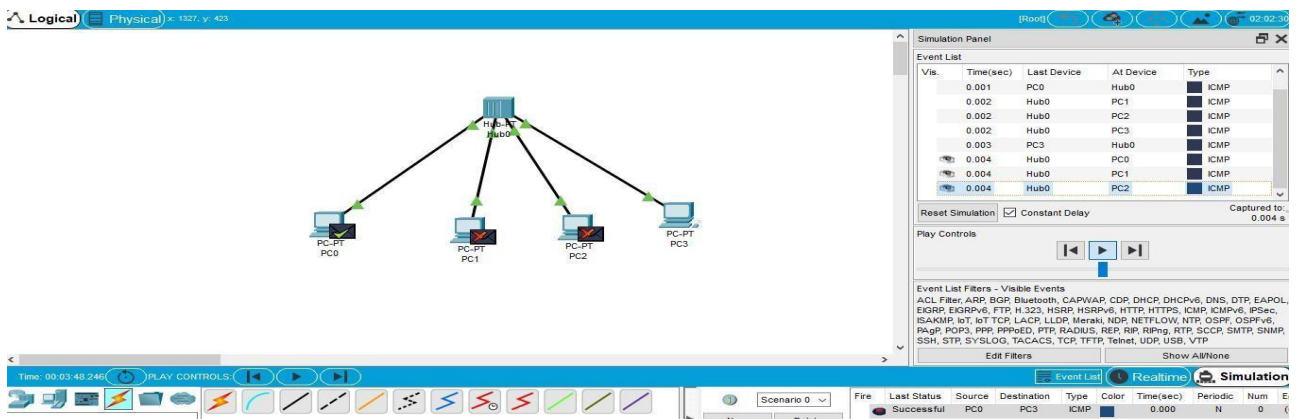
Lab Experiments: 1-5

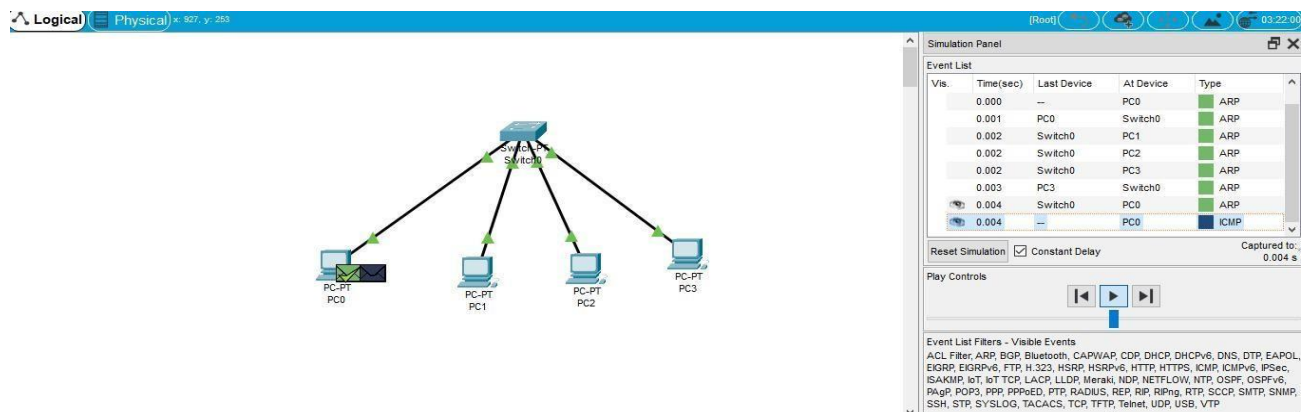
1. Configuration of Network Devices using Packet Tracer tools (Hub, Switch, Ethernet, Broadcast)



2. Design and Configuration of Star Topologies using Packet Tracer

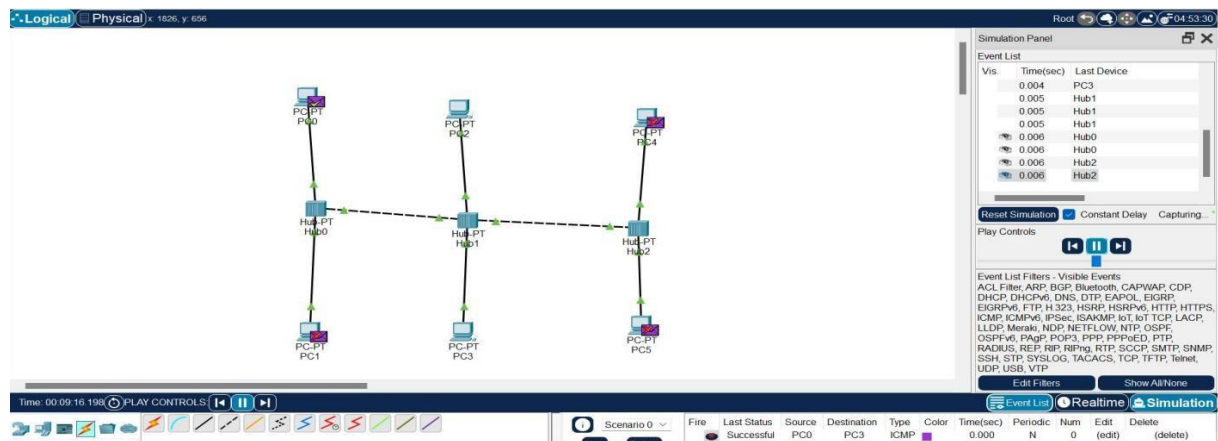
Star Topology using Hub:



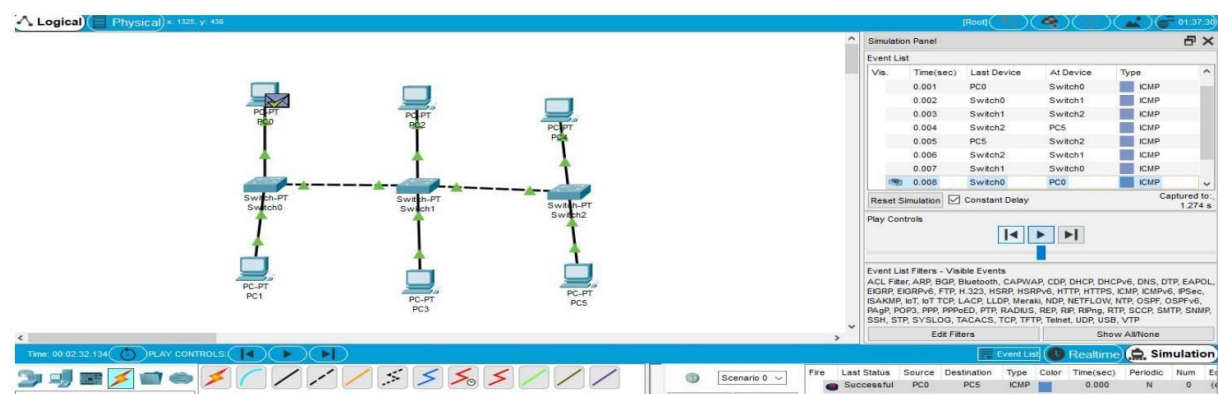


3. Design and Configuration of BUS Topologies using Packet Tracer.

Bus Topology using Hub:

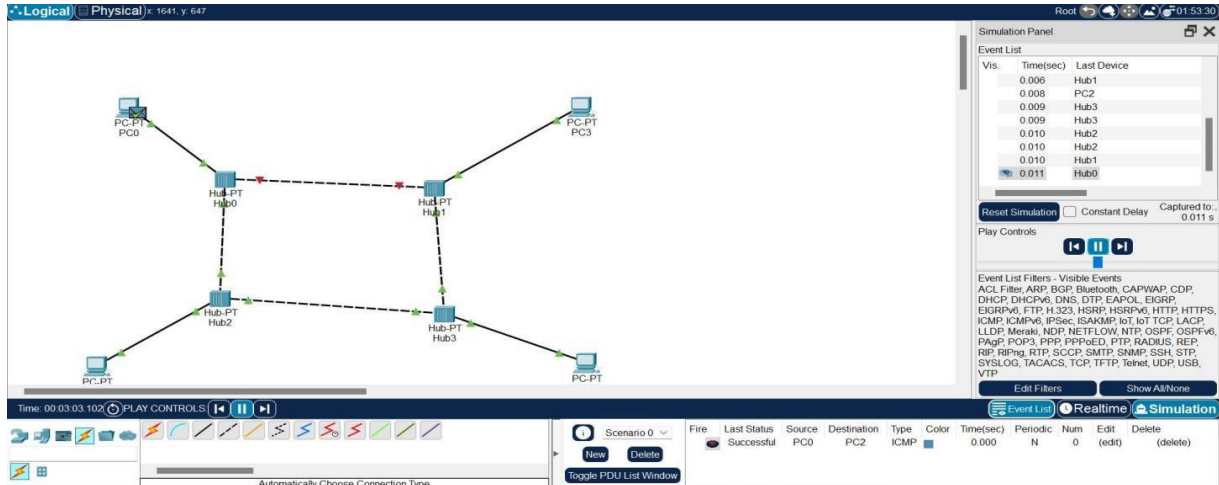


Bus Topology using Switch:

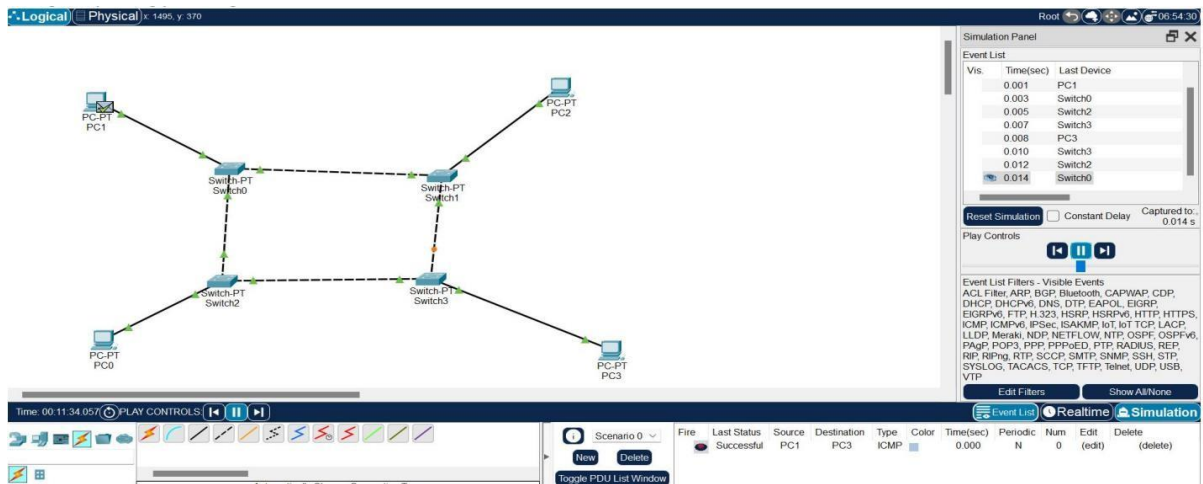


4. Design and Configuration of RING Topologies using Packet Tracer

Ring Topology using Hub:

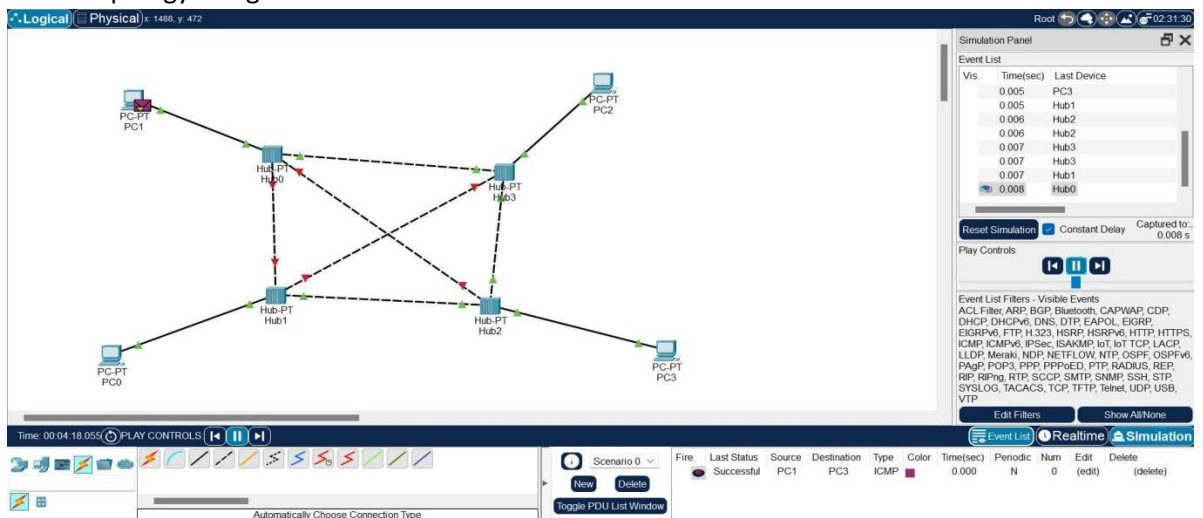


Ring Topology using Switch:

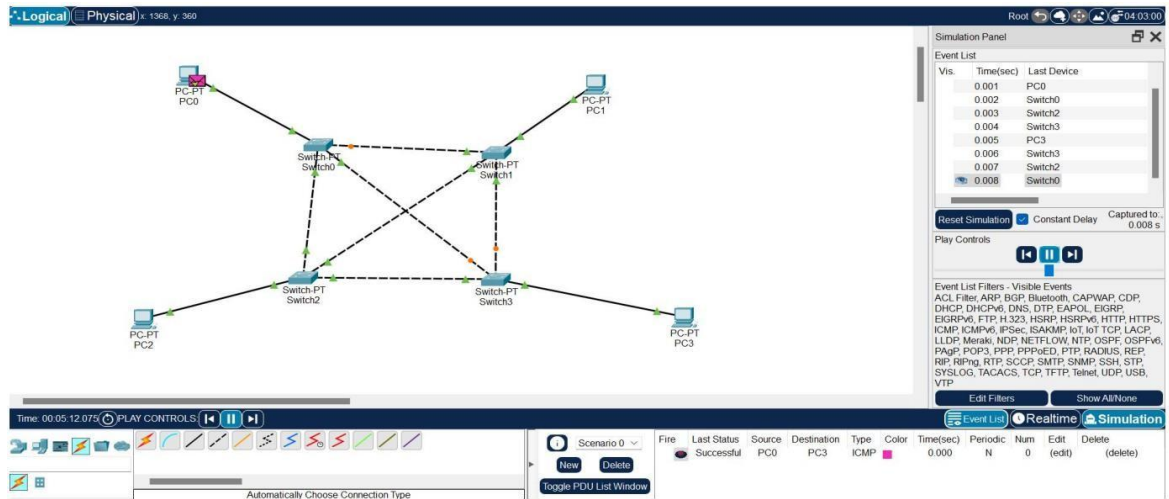


5. Design and Configuration of Mesh Topologies using Packet Tracer

Mesh Topology using Hub:

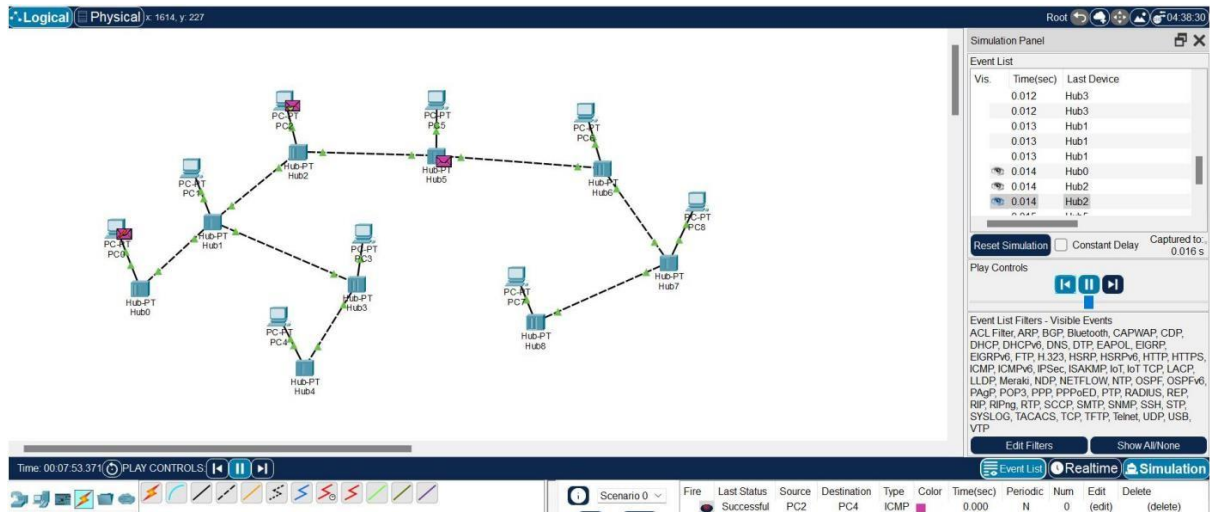


Mesh Topology using Switc

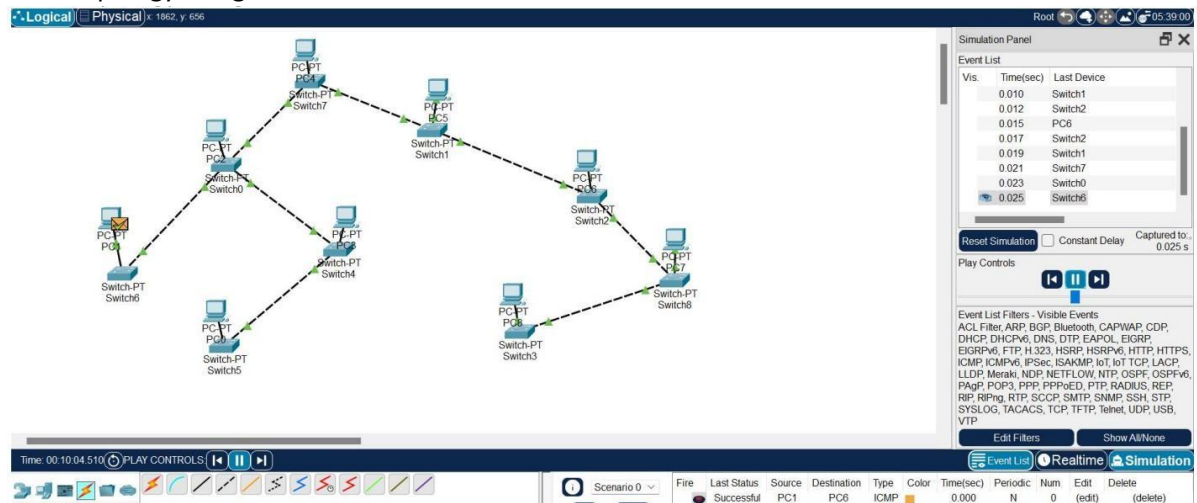


6. Design and Configuration of Tree Topologies using Packet Tracer.

Tree Topology using Hub:

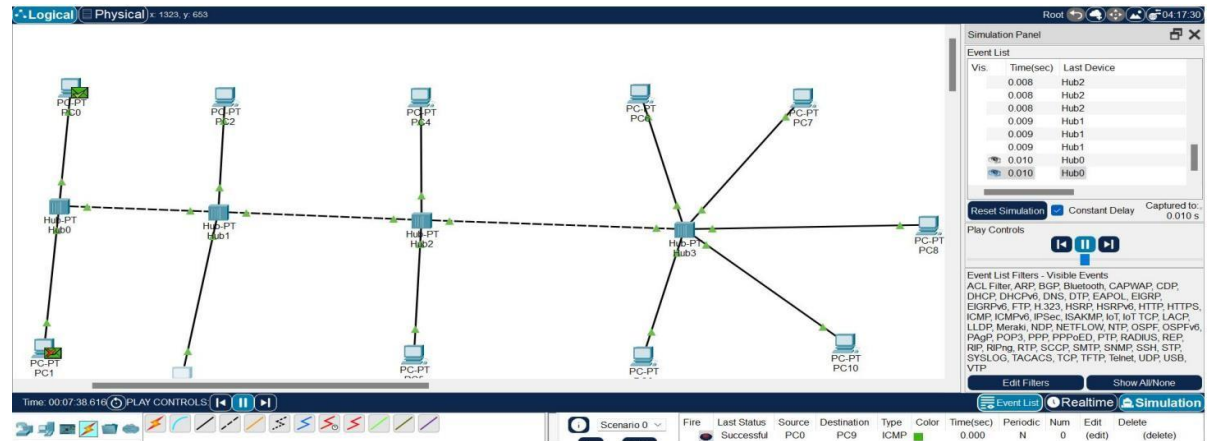


Tree Topology using Switch:

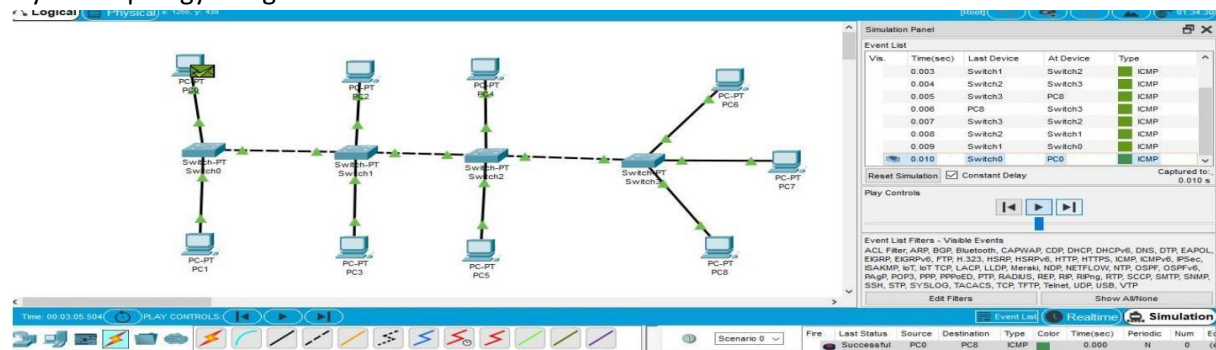


7. Design and Configuration of Hybrid Topologies using Packet Tracer

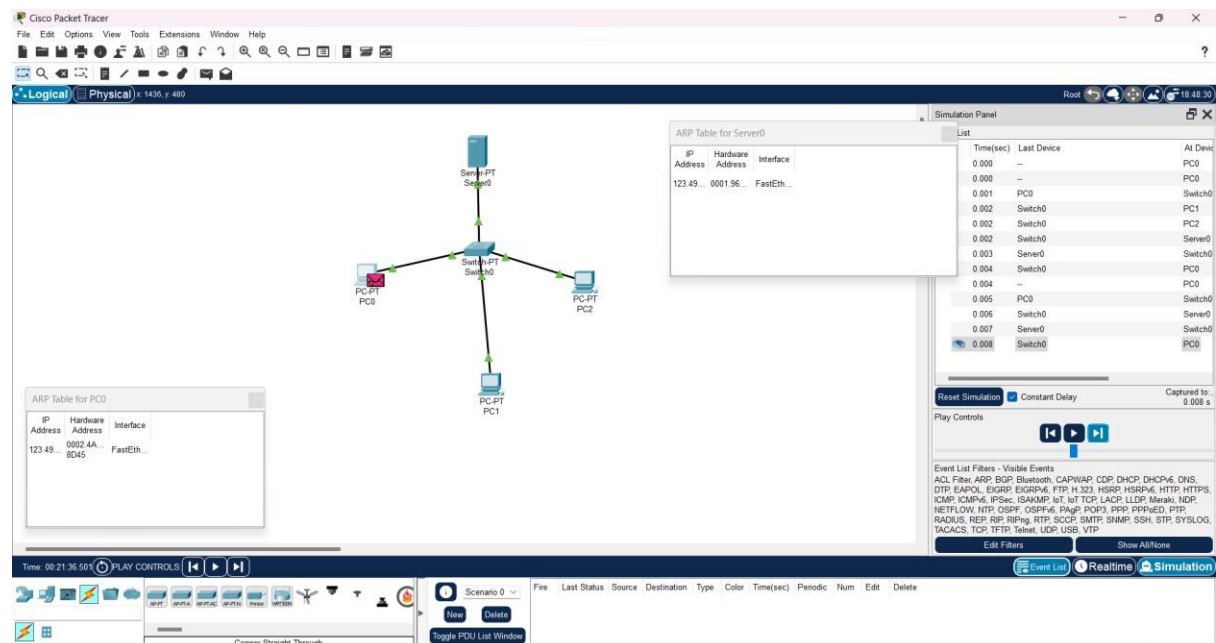
Hybrid Topology using Hub:



Hybrid Topology using Switch:



8. Data Link Layer Traffic Simulation using Packet Tracer Analysis of ARP



9. Data Link Layer Traffic Simulation using Packet Tracer Analysis of CSMA/CD & CSMA/CA

Cisco Packet Tracer - C:\Users\jaya tree dulla\Cisco Packet Tracer 8.2.2\saves\9 CSMA.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x 136% y 69%

CSMA

PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5
PC-PT PC6
Hub0

Simulation Panel

Event List

Vis.	Time(sec)	Last Device
Visible	0.000	

Reset Simulation Constant Delay Captured to: 0.000 s

Play Controls

Event List Filters - Visible Events ICMP

Edit Filters Show All/None

Time: 00:26:22.635K PLAY CONTROLS

Scenario 0

New Delete

Toggle PC/L List Window

File	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC3	PC2	ICMP		294.586	N	4	(edit)	(delete)
	Successful	PC2	PC5	ICMP		598.013	N	5	(edit)	(delete)
	Successful	PC0	PC3	ICMP		1135.283	N	6	(edit)	(delete)

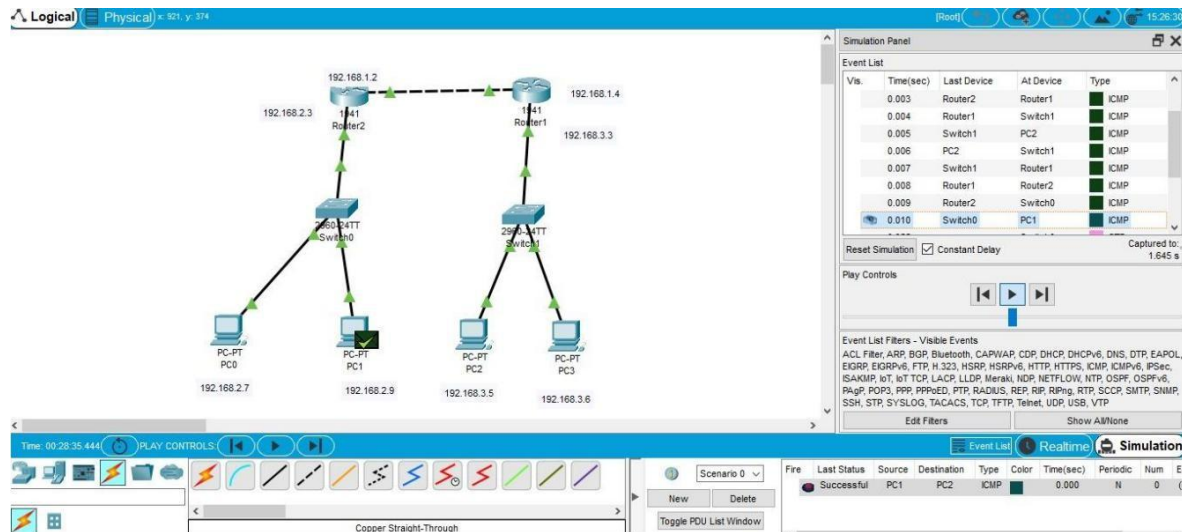
86°F Partly sunny

Search

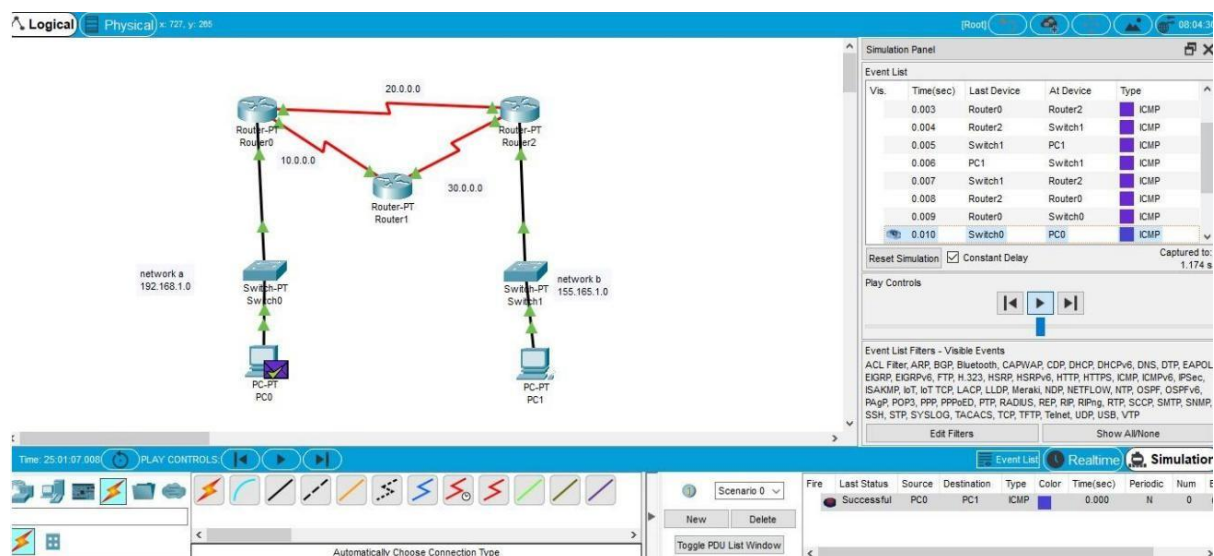
ENG IN

12:20 09-12-2024

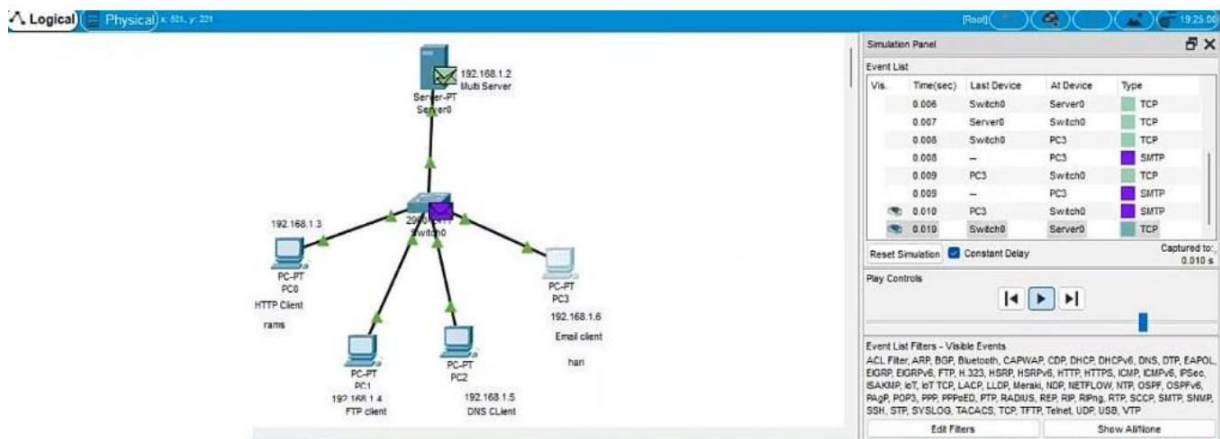
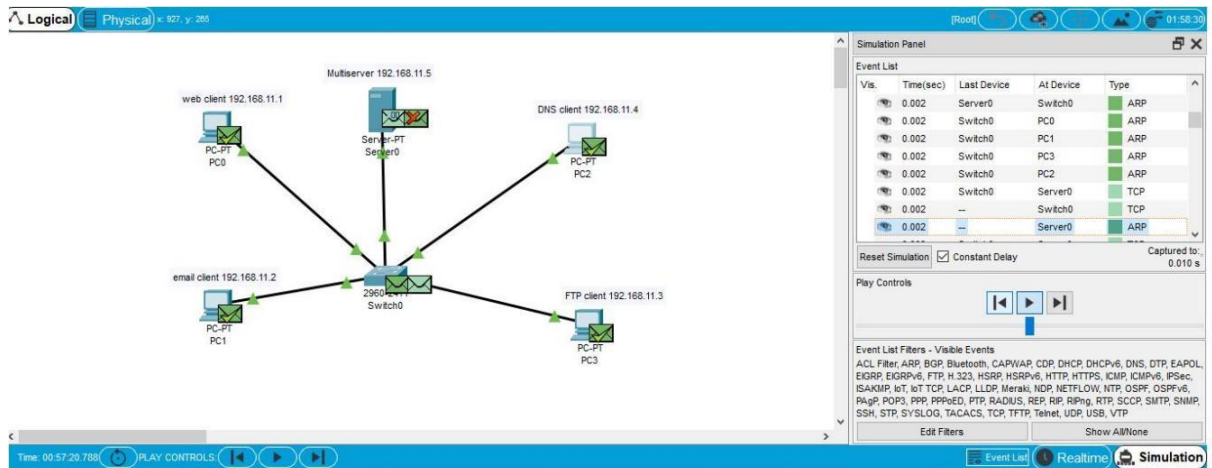
10. Designing two different networks with Static Routing techniques using Packet Tracer



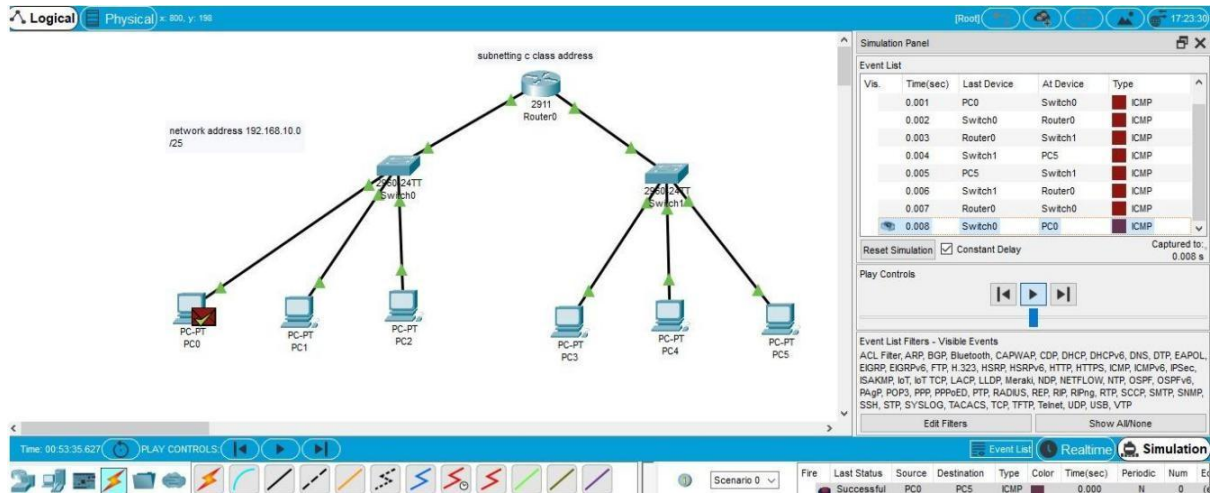
11. Designing two different networks with Dynamic Routing techniques (RIP & OSPF) using Packet Tracer



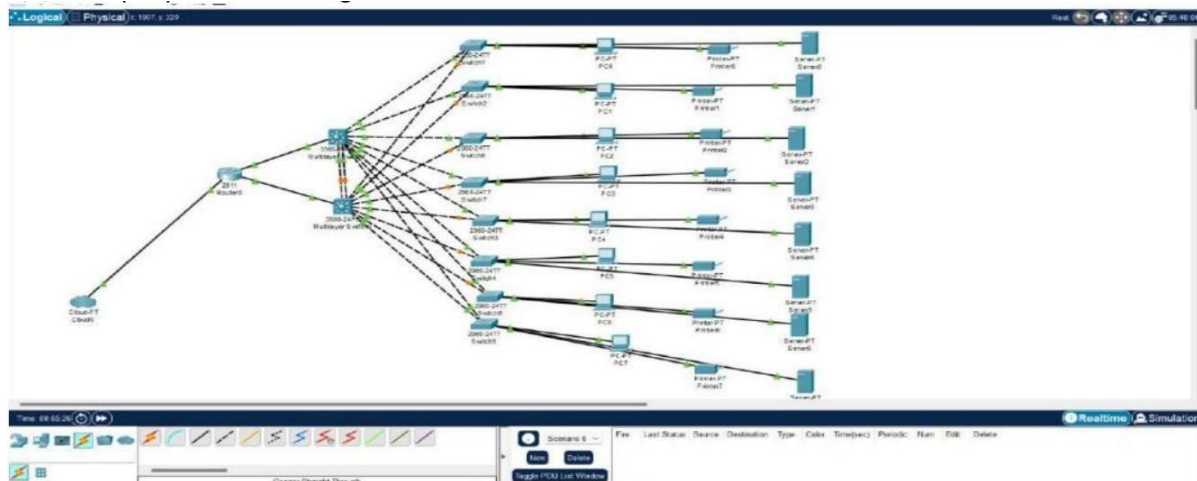
12. Design the Functionalities and Exploration of TCP using Packet Tracer



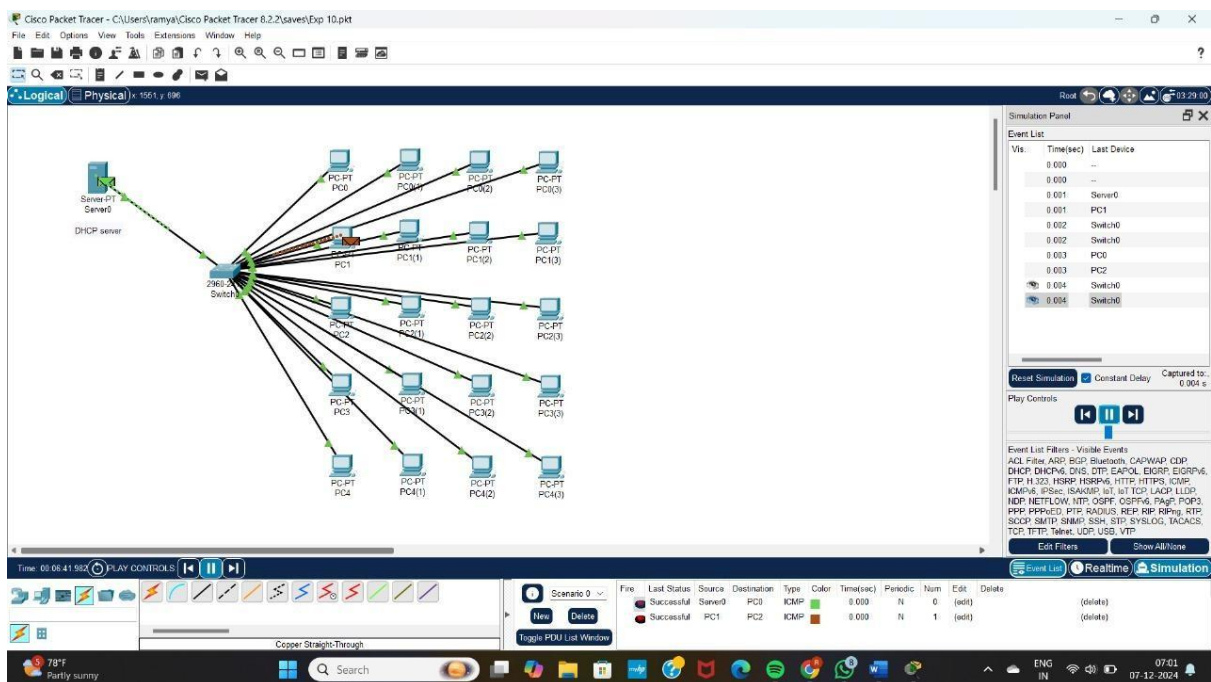
13. Design the network model for Subnetting – Class C Addressing using Packet Tracer.



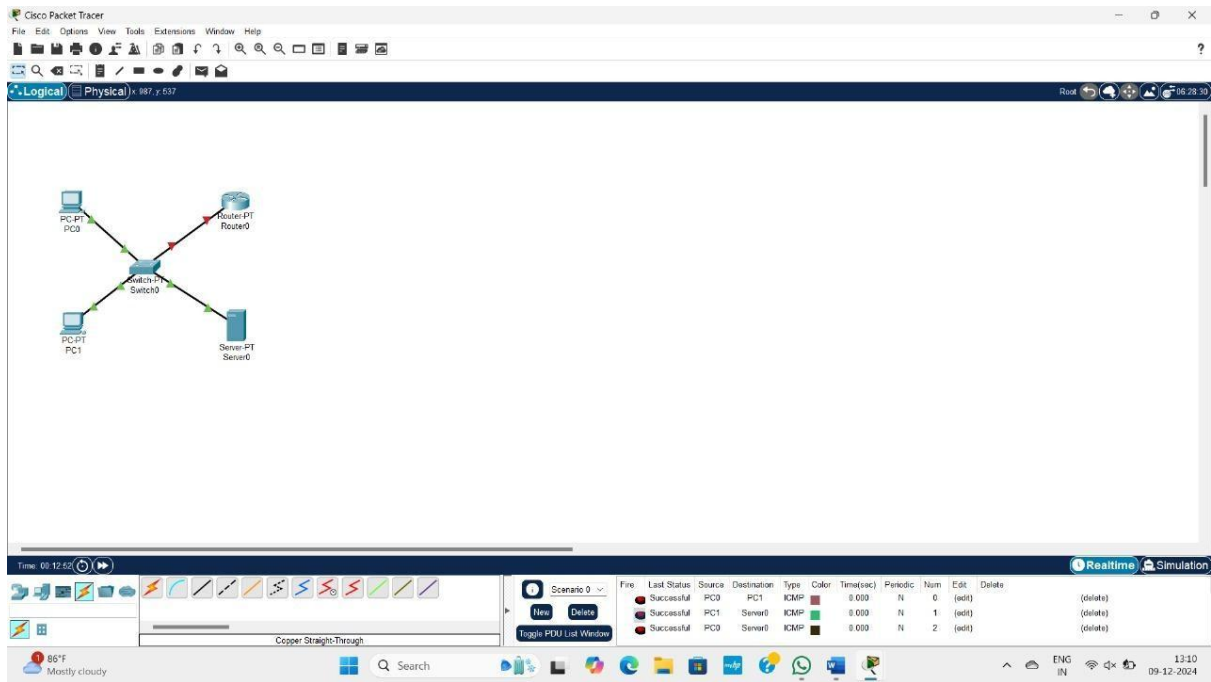
14. Simulating X, Y, Z Company Network Design and simulate using Packet Tracer.



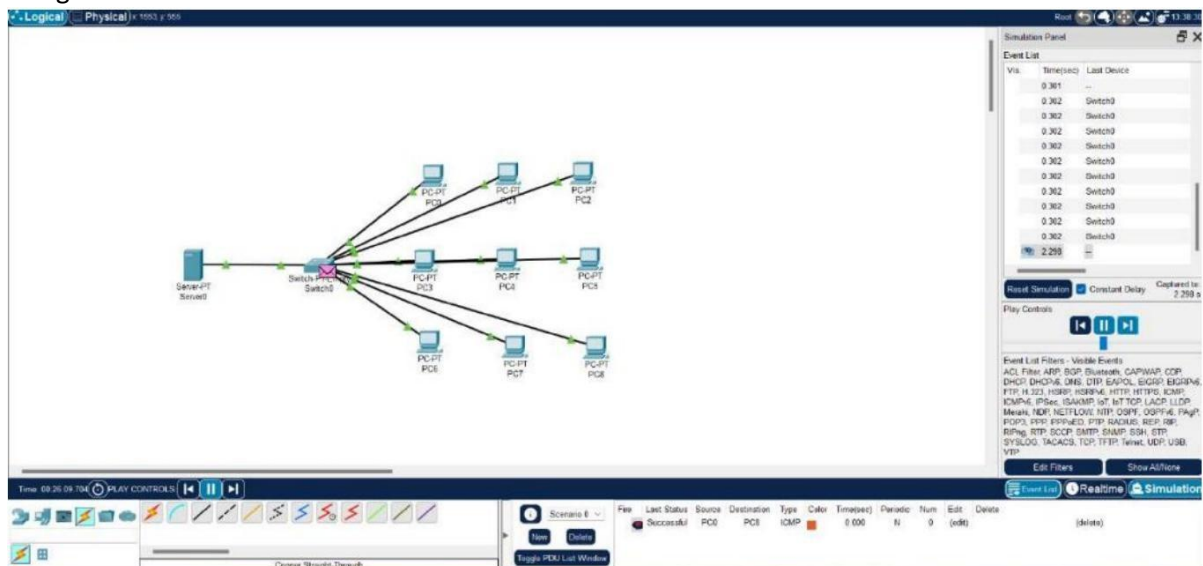
15. Configuration of DHCP (dynamic host configuration protocol) in packet Tracer.



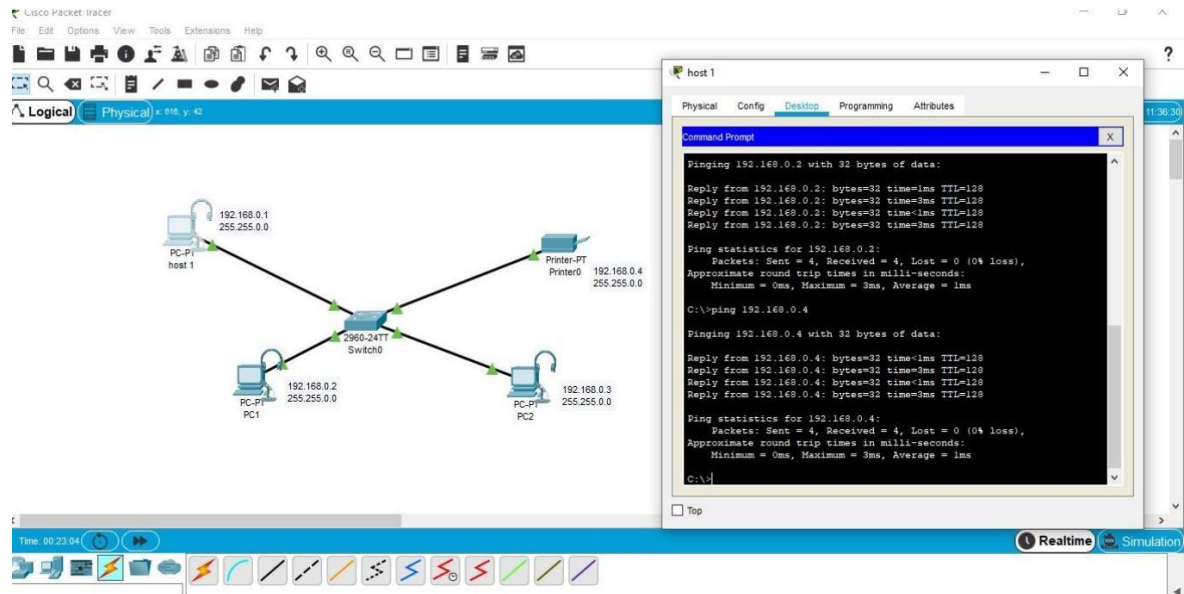
16. Configuration of firewall in packet tracer.



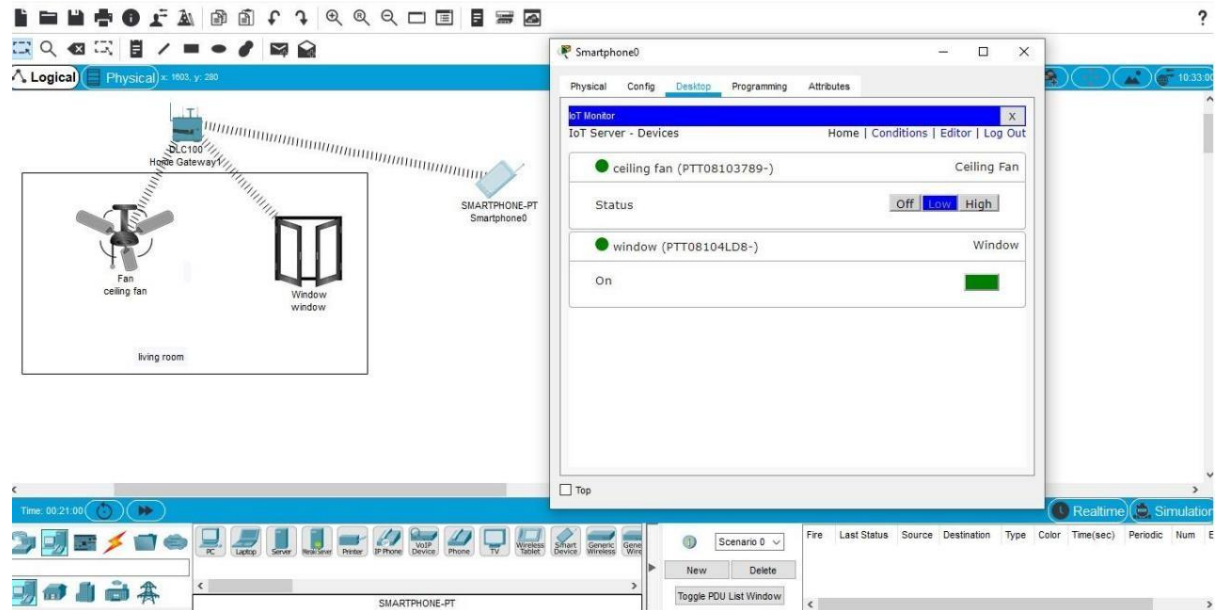
17. Make a Computer Lab to transfer a message from one node to another to design and simulate using Cisco Packet Tracer.



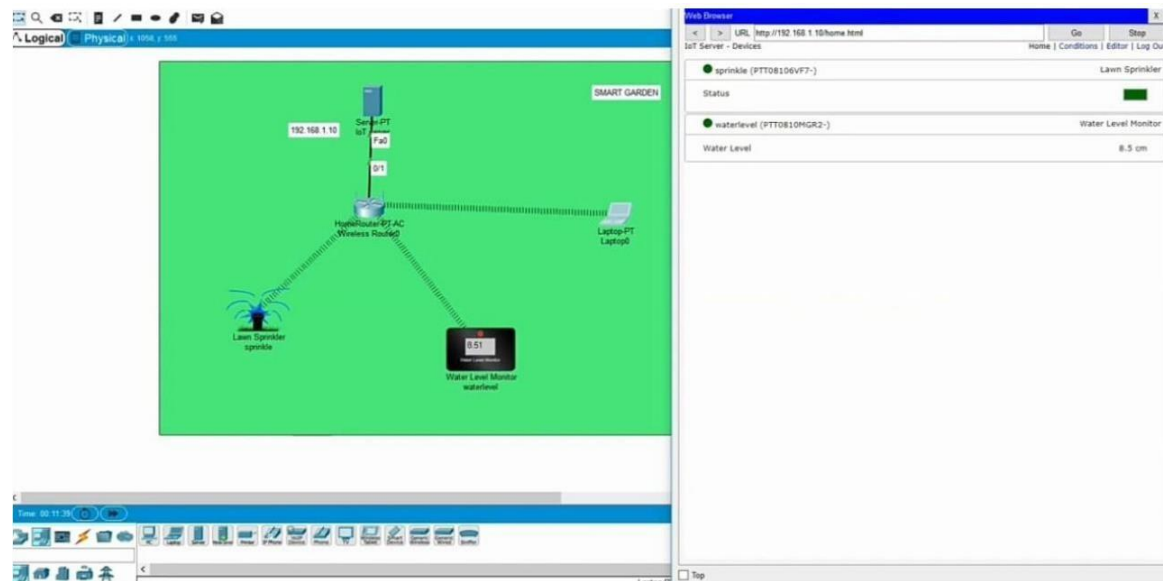
18. Simulate a Multimedia Network in Cisco Packet Tracer.



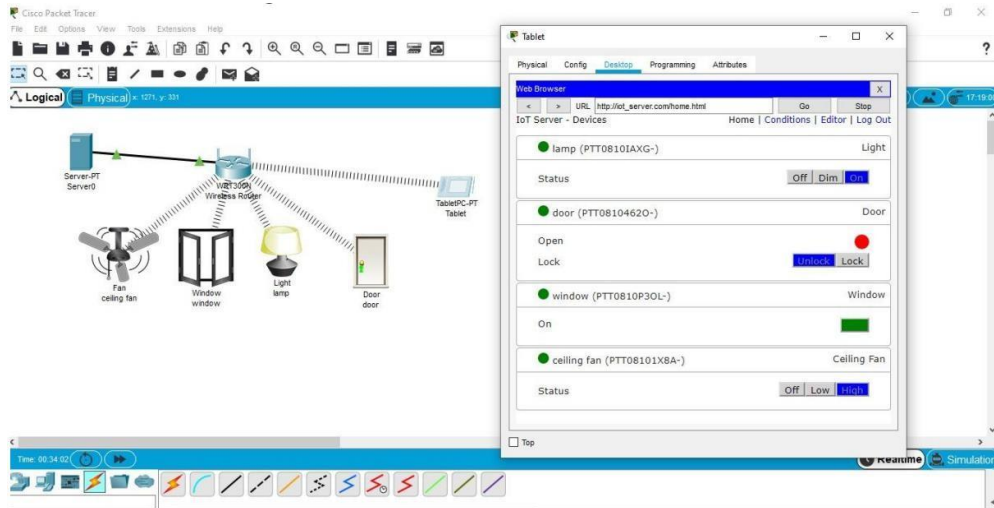
19. IoT based smart home applications.



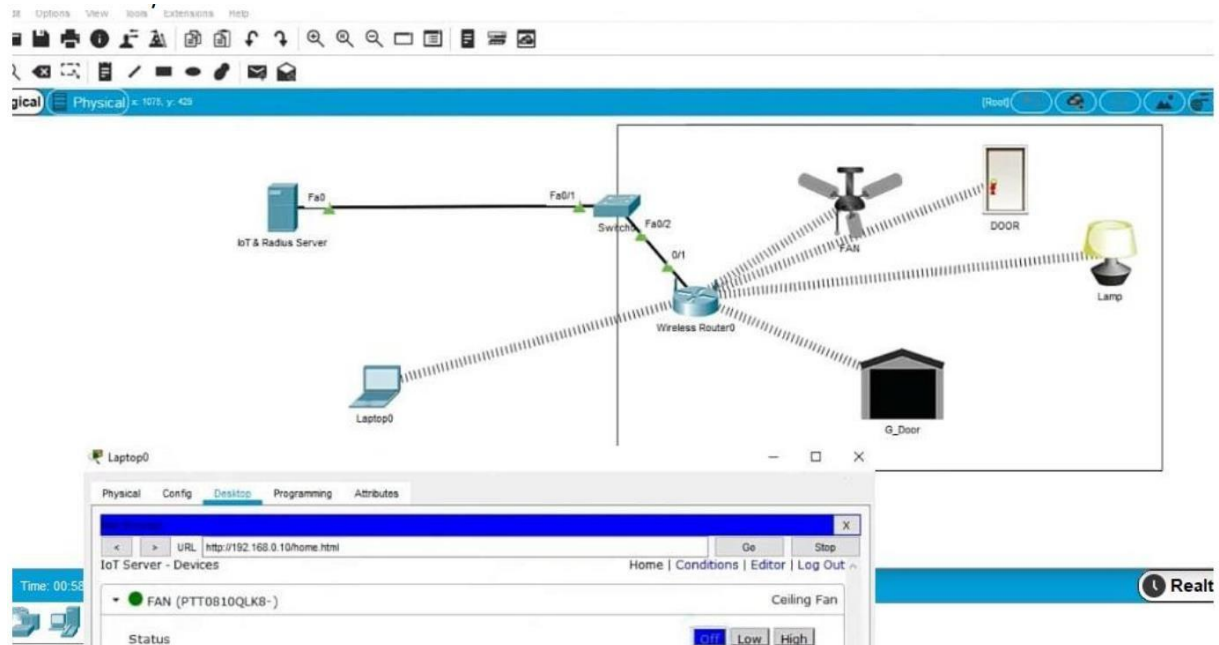
20. Implementation of IoT based smart gardening.



21. Implementation of IoT devices in networking.



22. IOT Based Smart building using WPA Security & Radius Server.



23. TCP

No.	Time	Source	Destination	Protocol	Length	Info
138	26.218260	34.208.110.97	192.168.1.52	TLSv1.2	370	Application Data
139	26.218260	34.208.110.97	192.168.1.52	TLSv1.2	92	Application Data
140	26.218368	192.168.1.52	34.208.110.97	TCP	54	62986 → 443 [ACK] Seq=419 Ack=801 Win=508 Len=0
141	26.220395	192.168.1.52	34.208.110.97	TLSv1.2	96	Application Data
150	26.575741	192.168.1.52	34.208.110.97	TCP	96	[TCP Retransmission] 62986 → 443 [PSH, ACK] Seq=419

> Frame 3: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{BEDE0CDF-D84F-4436-818D-5D1E780DBFF5}
> Ethernet II, Src: IntelCor_ea:4a:5c (34:f3:9a:ea:4a:5c), Dst: TaicangT_2b:71:e0 (24:0b:88:2b:71:e0)
> Internet Protocol Version 4, Src: 192.168.1.52, Dst: 185.184.8.90
> Transmission Control Protocol, Src Port: 51636, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

0000	00100100	00001011	10001000	00101011	01110001	11100000	00110100	11110011	\$-+q 4-
0008	10011010	11101010	01001010	01011100	00001000	01000000	01000101	00000000	-J\ -E-
0016	00000000	00101001	10111100	00100100	01000000	00000000	10000000	00000110	-) \$e -
0024	10111010	10111011	11000000	10101000	00000001	00110100	10111001	10111000	-:- 4 -
0032	00001000	01011010	11001001	10110100	00000001	10111011	01100010	10000011	-Z - - b-
0040	01011000	11010111	01111000	01011101	11011100	00010010	01010000	00010000	X-x] -P-
0048	00000001	11111101	01001110	10101101	00000000	00000000	00000000	00000000	-N -x-

24. ICMP

The screenshot shows a Wireshark capture of ICMP Echo (ping) requests and replies. The packet list pane displays 11 packets, all of which are Echo (ping) requests or replies. The packet details pane shows the structure of an ICMP Echo request, including the Echo (ping) request type, ID, and sequence number. The packet bytes pane shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol header.

No.	Time	Source	Destination	Protocol	Length	Info
33	29.633524	192.168.43.241	142.104.75.58	ICMP	74	Echo (ping) request id=0x0001, seq=289/8449, ttl=128 (reply ...)
34	30.249428	142.104.75.58	192.168.43.241	ICMP	74	Echo (ping) reply id=0x0001, seq=289/8449, ttl=41 (request ...)
40	30.641976	192.168.43.241	142.104.75.58	ICMP	74	Echo (ping) request id=0x0001, seq=290/8705, ttl=128 (reply ...)
46	31.209199	142.104.75.58	192.168.43.241	ICMP	74	Echo (ping) reply id=0x0001, seq=290/8705, ttl=41 (request ...)
47	31.649021	192.168.43.241	142.104.75.58	ICMP	74	Echo (ping) request id=0x0001, seq=291/8961, ttl=128 (reply ...)
49	32.169936	142.104.75.58	192.168.43.241	ICMP	74	Echo (ping) reply id=0x0001, seq=291/8961, ttl=41 (request ...)
50	32.654228	192.168.43.241	142.104.75.58	ICMP	74	Echo (ping) request id=0x0001, seq=292/9217, ttl=128 (reply ...)
51	33.129417	142.104.75.58	192.168.43.241	ICMP	74	Echo (ping) reply id=0x0001, seq=292/9217, ttl=41 (request ...)
52	33.682669	192.168.43.241	142.104.75.58	ICMP	74	Echo (ping) request id=0x0001, seq=293/9473, ttl=128 (reply ...)
53	34.090728	142.104.75.58	192.168.43.241	ICMP	74	Echo (ping) reply id=0x0001, seq=293/9473, ttl=41 (request ...)
54	34.695329	192.168.43.241	142.104.75.58	ICMP	74	Echo (ping) request id=0x0001, seq=294/9729, ttl=128 (reply ...)
55	35.054650	142.104.75.58	192.168.43.241	ICMP	74	Echo (ping) reply id=0x0001, seq=294/9729, ttl=41 (request ...)

Frame 33: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{AAF6E947-B49B-45AE-9916-FE3C80C32315}, id 0
Ethernet II, Src: AzureNav_3c:97:91 (d0:c5:d3:3c:97:91), Dst: Motorola_d8:fc:58 (64:db:43:d8:fc:58)
Internet Protocol Version 4, Src: 192.168.43.241, Dst: 142.104.75.58
Internet Control Message Protocol

Activate Windows
Go to Settings to activate Windows.

Internet Control Message Protocol: Protocol

Packets: 73 · Displayed: 20 (27.4%) · Dropped: 0 (0.0%)

Profile: Default

Type here to search

01:41 AM
28/04/2020

25. ARP

The screenshot shows a Wireshark capture of ARP requests and replies. The packet list pane displays 11 packets, including ARP requests, ARP replies, and a DHCP request. The packet details pane shows the structure of an ARP request, including the Hardware type, Protocol type, Hardware size, Protocol size, Opcode, Sender MAC address, Sender IP address, and Target MAC address. The packet bytes pane shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol header.

No.	Time	Source	Destination	Protocol	Length	Info
319	5.706447	HonHaiPr_94:5f:ff	Broadcast	ARP	42	Who has 192.168.42.152? Tell 192.168.42.45
320	5.707749	Dell_a0:dc:1c	HonHaiPr_94:5f:ff	ARP	60	192.168.42.152 is at a0:29:19:a0:dc:1c
353	7.620105	7e:c2:6d:1a:da:da	Broadcast	ARP	60	ARP Announcement for 192.168.42.154
354	7.620961	7e:c2:6d:1a:da:da	Broadcast	ARP	60	Who has 192.168.42.1? Tell 192.168.42.154
373	8.847173	7e:c2:6d:1a:da:da	Broadcast	ARP	60	Who has 192.168.42.1? Tell 192.168.42.154
374	8.949676	7e:c2:6d:1a:da:da	Broadcast	ARP	60	ARP Announcement for 192.168.42.154
421	12.328697	TexasIns_04:5c:d0	Broadcast	ARP	60	ARP Announcement for 192.168.42.85
434	13.005849	Ubiquiti_b3:d9:a6	HonHaiPr_94:5f:ff	ARP	60	Who has 192.168.42.45? Tell 192.168.42.39
435	13.005887	HonHaiPr_94:5f:ff	Ubiquiti_b3:d9:a6	ARP	42	192.168.42.45 is at 54:13:79:94:5f:ff
352	7.619492	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xa0cd764b

Frame 319: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{6A50B021-BECC-489E-B8B1-5FB4C2D45E41}, id 0
Ethernet II, Src: HonHaiPr_94:5f:ff (54:13:79:94:5f:ff), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: HonHaiPr_94:5f:ff (54:13:79:94:5f:ff)
Sender IP address: 192.168.42.45
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.42.152

0000 ff ff ff ff ff 54 13 79 94 5f ff 08 06 00 01T. y
0010 08 00 06 04 00 01 54 13 79 94 5f ff c0 a8 2a 2dT. y
0020 00 00 00 00 00 00 c0 a8 2a 98*