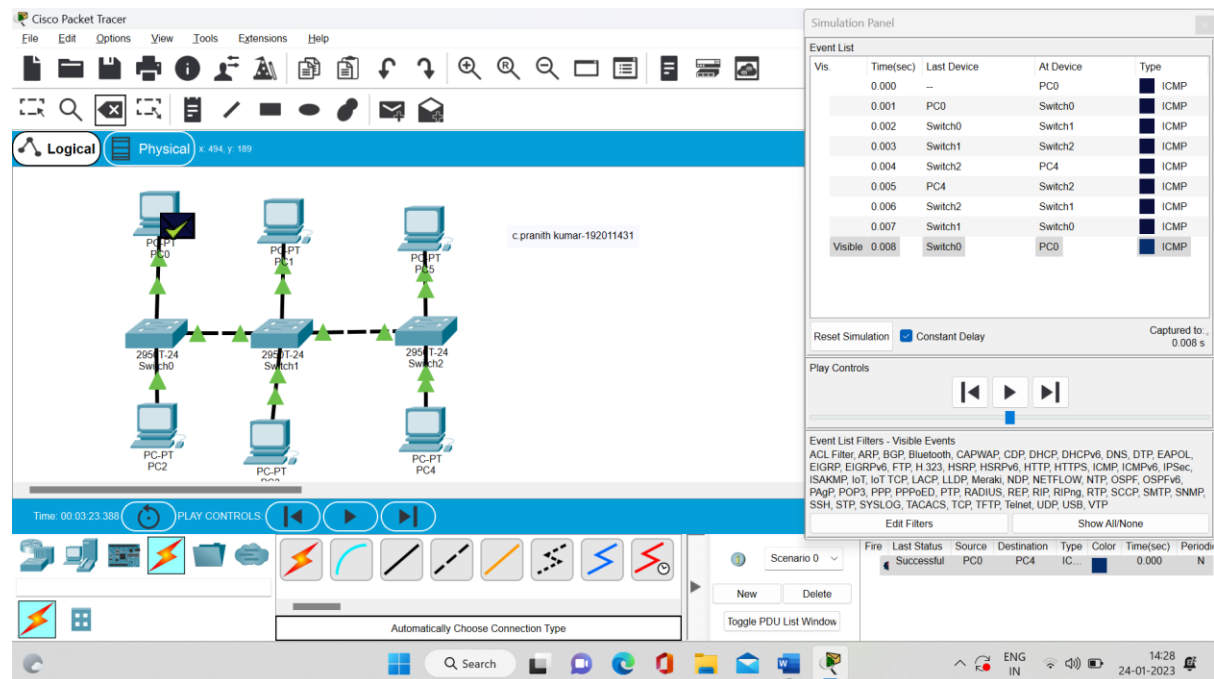


Computer networks

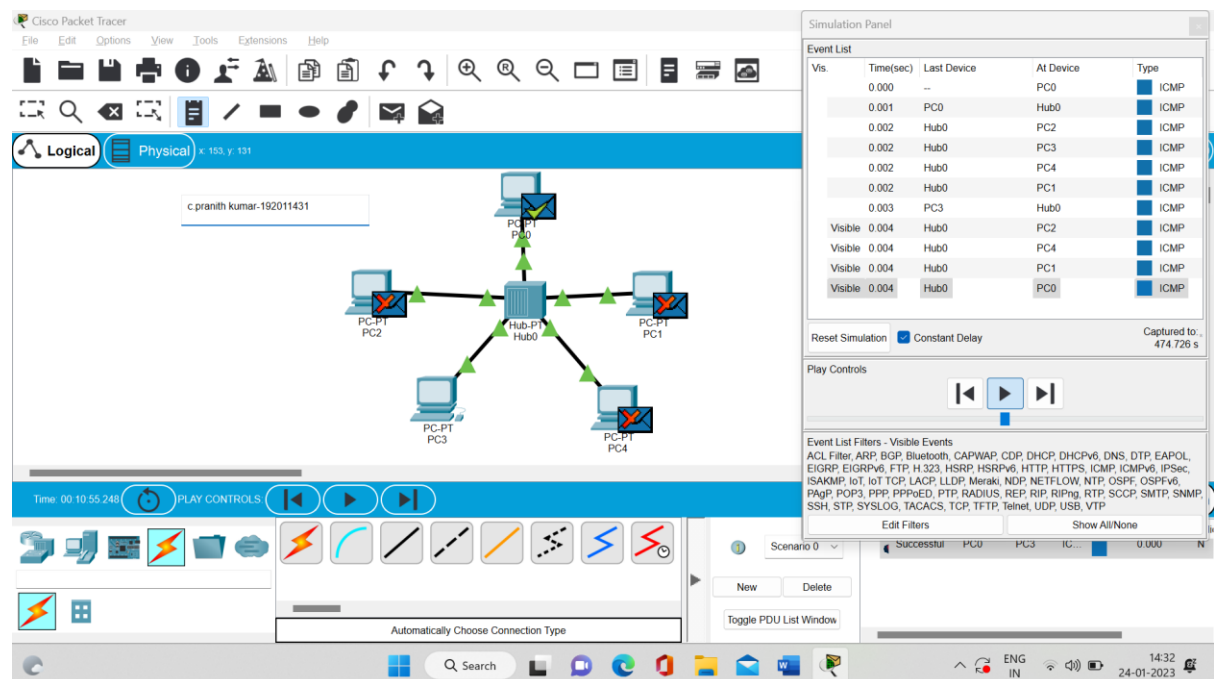
C.PRANITH KUMAR

192011431

1.bus topology



2.star topology



3. ring topology

The screenshot shows the Cisco Packet Tracer interface with a ring topology. The topology consists of four 2950T-24 switches (Switch0, Switch1, Switch2, Switch3) connected in a ring. Four PCs (PC0, PC1, PC2, PC3) are connected to the switches. The Event List panel on the right shows a sequence of ICMP events.

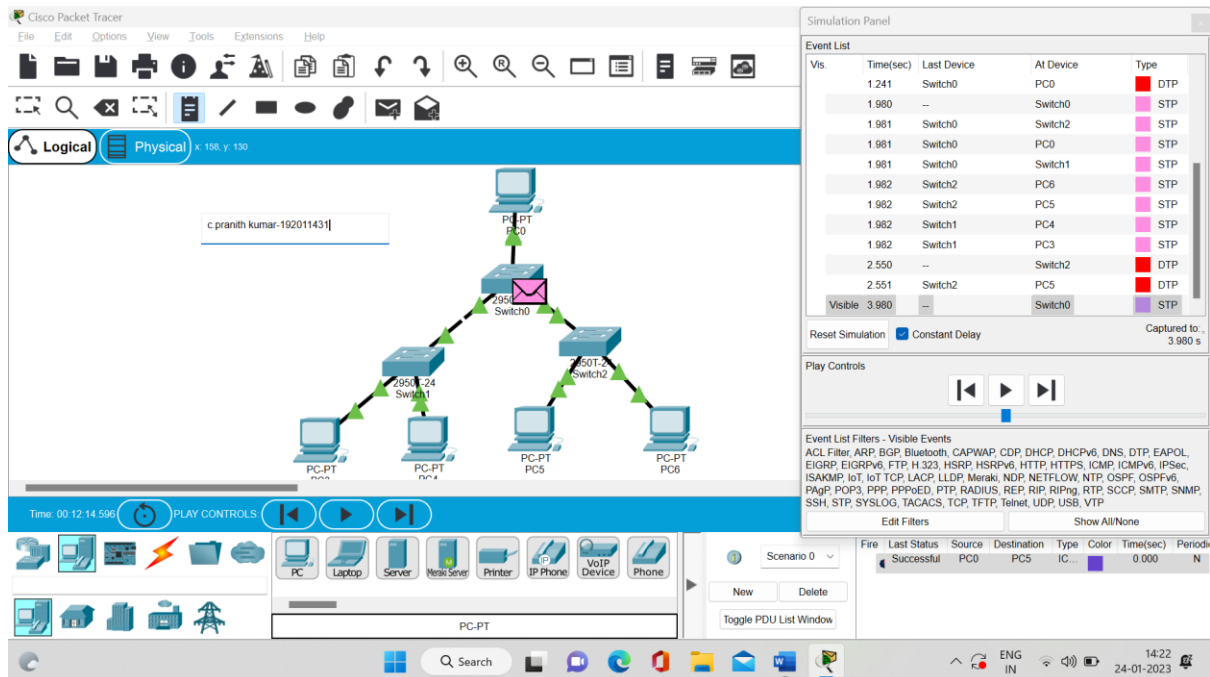
Vis	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.001	PC0	Switch0	ICMP
	0.002	Switch0	Switch3	ICMP
	0.003	Switch3	Switch2	ICMP
	0.004	Switch2	PC2	ICMP
	0.005	PC2	Switch2	ICMP
	0.006	Switch2	Switch3	ICMP
	0.007	Switch3	Switch0	ICMP
	0.008	Switch0	PC0	ICMP
Visible	1.889	--	Switch2	STP

4. mesh topology

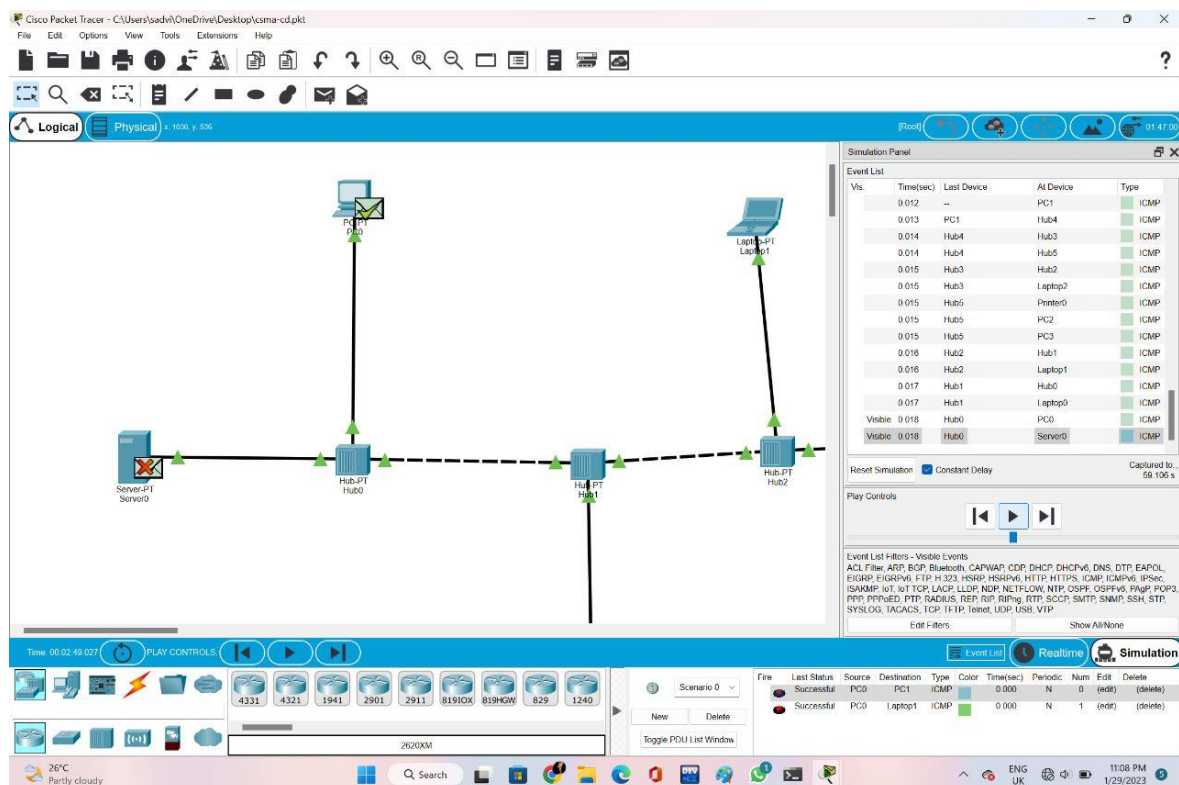
The screenshot shows the Cisco Packet Tracer interface with a mesh topology. The topology consists of four 2950T-24 switches (Switch0, Switch1, Switch2, Switch3) connected in a mesh. Four PCs (PC0, PC1, PC2, PC3) are connected to the switches. The Event List panel on the right shows a sequence of ICMP events.

Vis	Time(sec)	Last Device	At Device	Type
	0.003	Switch0	Switch2	ICMP
	0.003	Switch2	PC2	ICMP
	0.004	Switch2	Switch1	ICMP
	0.004	PC2	Switch2	ICMP
	0.005	Switch1	PC1	ICMP
	0.005	Switch2	Switch0	ICMP
	0.006	PC1	Switch1	ICMP
	0.006	Switch0	PC0	ICMP
	0.007	Switch1	Switch2	ICMP
	0.008	Switch2	Switch0	ICMP
	0.009	Switch0	PC0	ICMP
Visible	0.986	--	Switch2	STP

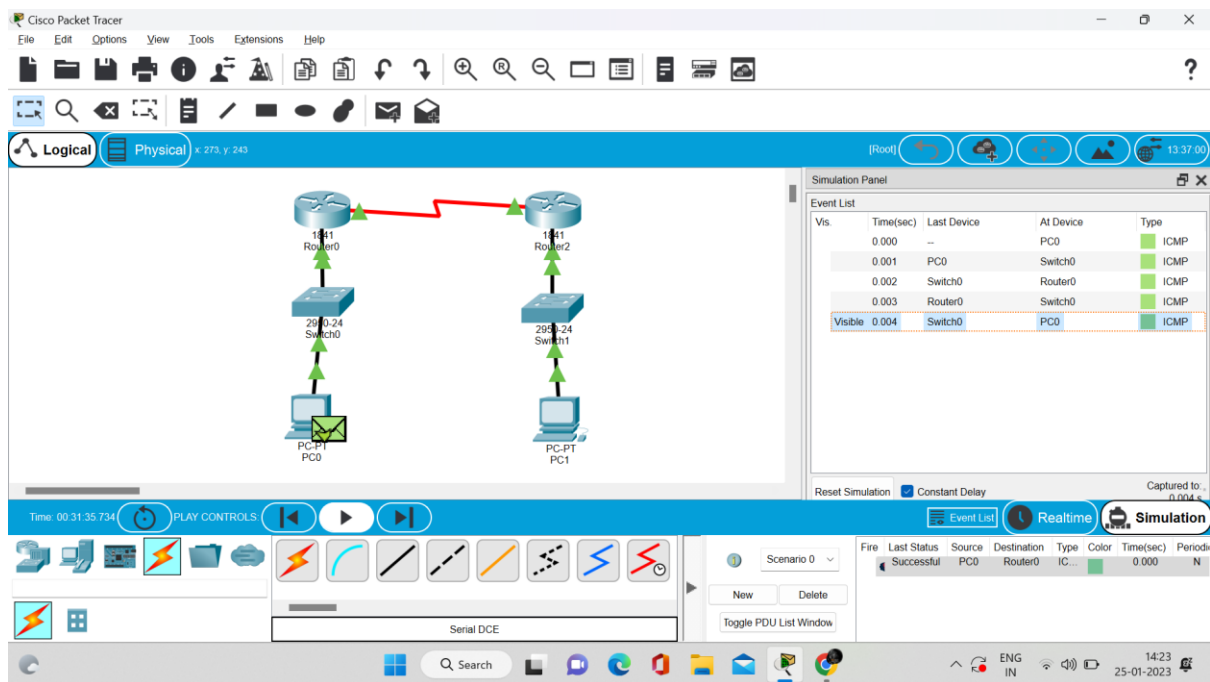
5.Tree Topology



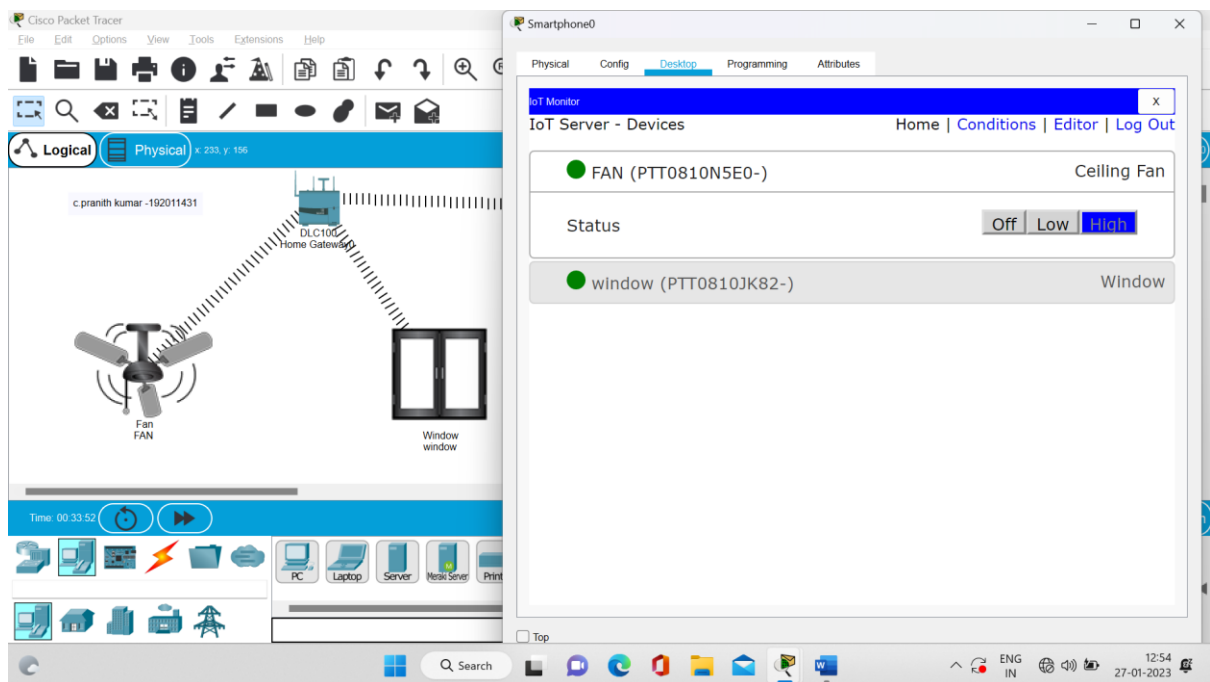
HYBRID TOPOLOGY



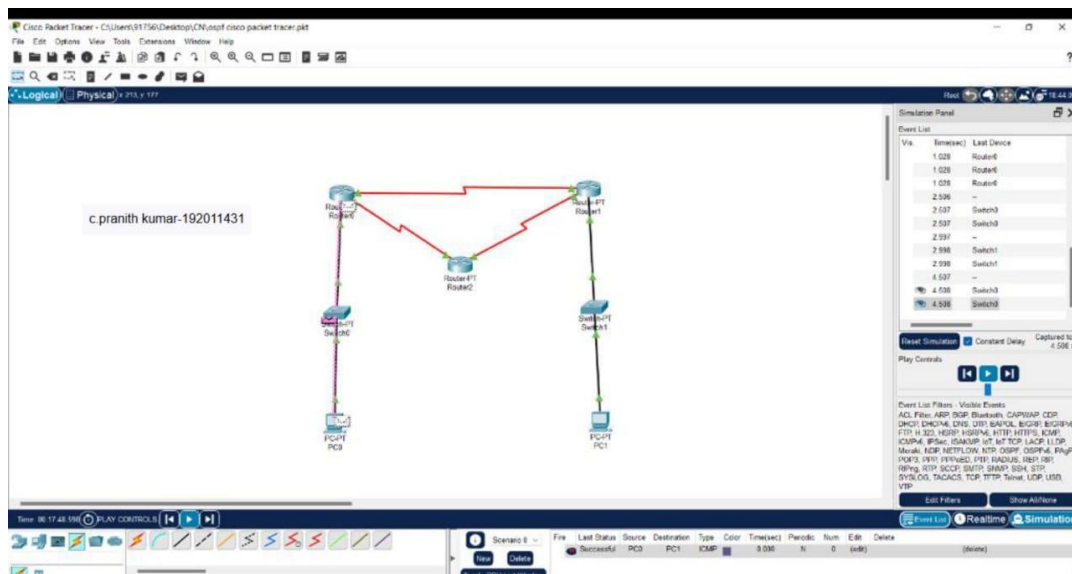
STATIC



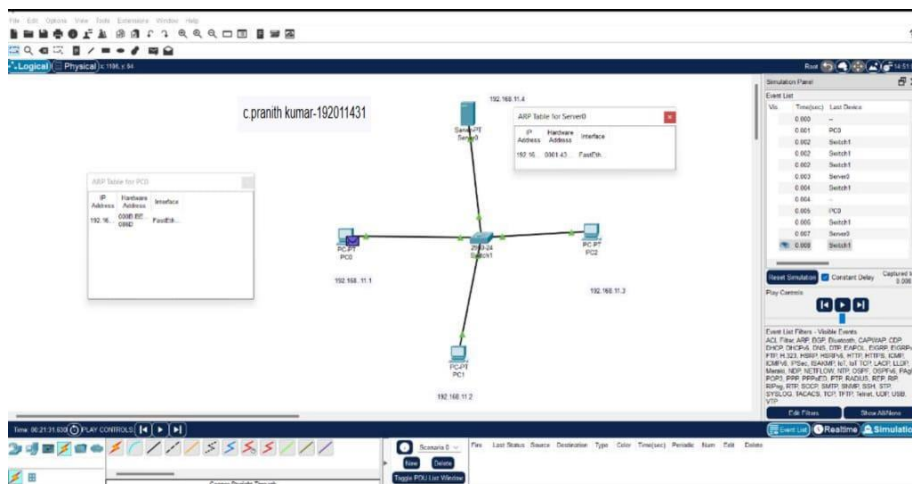
IOT SMART HOME



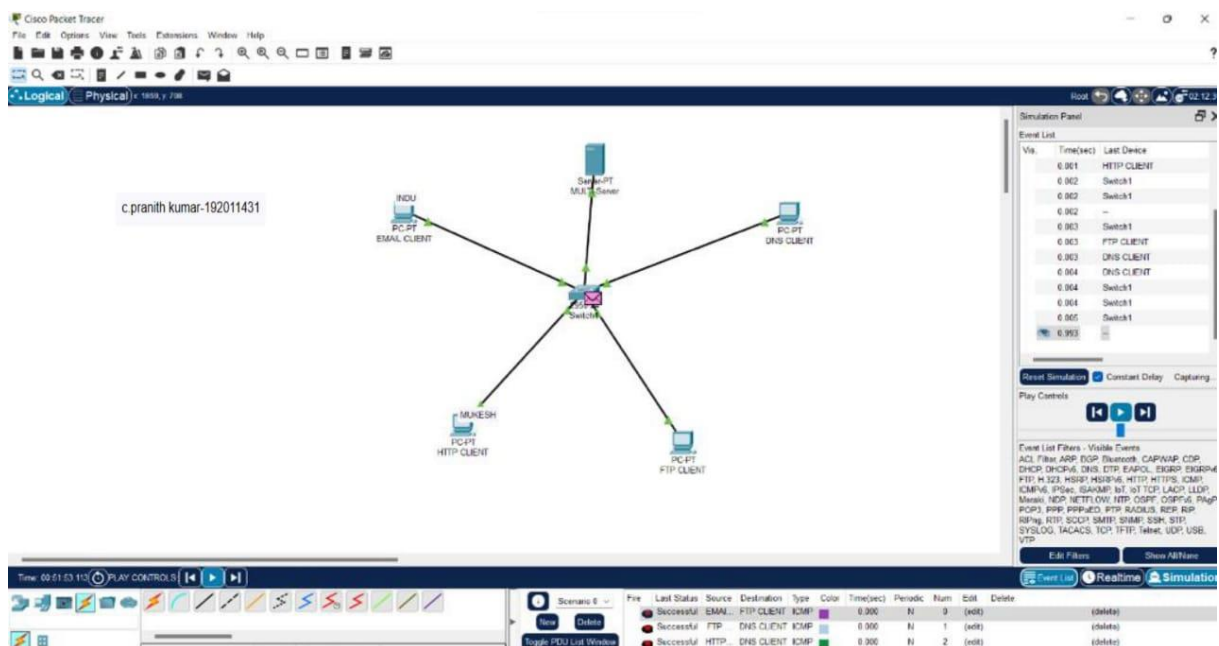
OSPF



DATA LINK LAYER ARP



TCP UDP



BIT STUFFING

```
1 #include<stdio.h>

Enter a String1010010010

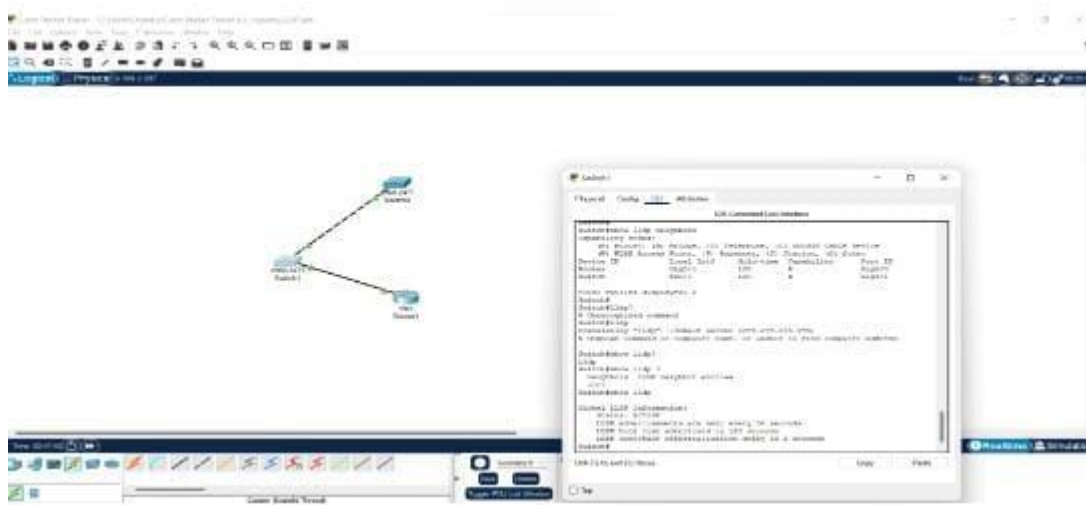
String after Bit Stuffing is performed:
01111110101001001001111110

String after De-Stuffing is performed:
1010010010
```

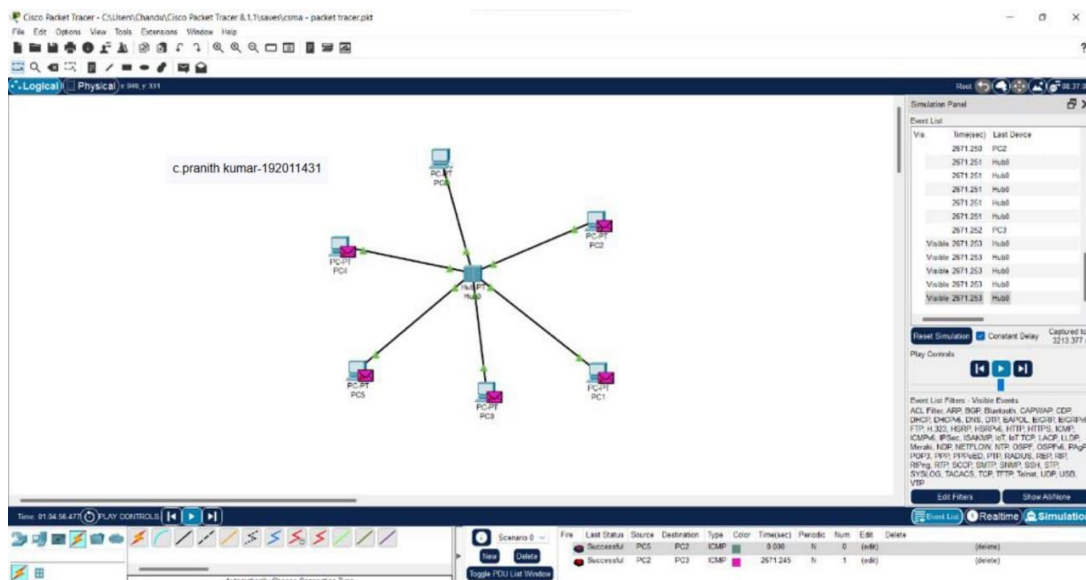
Compiler Output:

```
-----
- Errors: 0
- Warnings: 0
- Output Filename: C:\Users\sadvi\OneDrive\Documents\bit.exe
- Output Size: 129,939463125 KiB
- Compilation Time: 0.47s
```

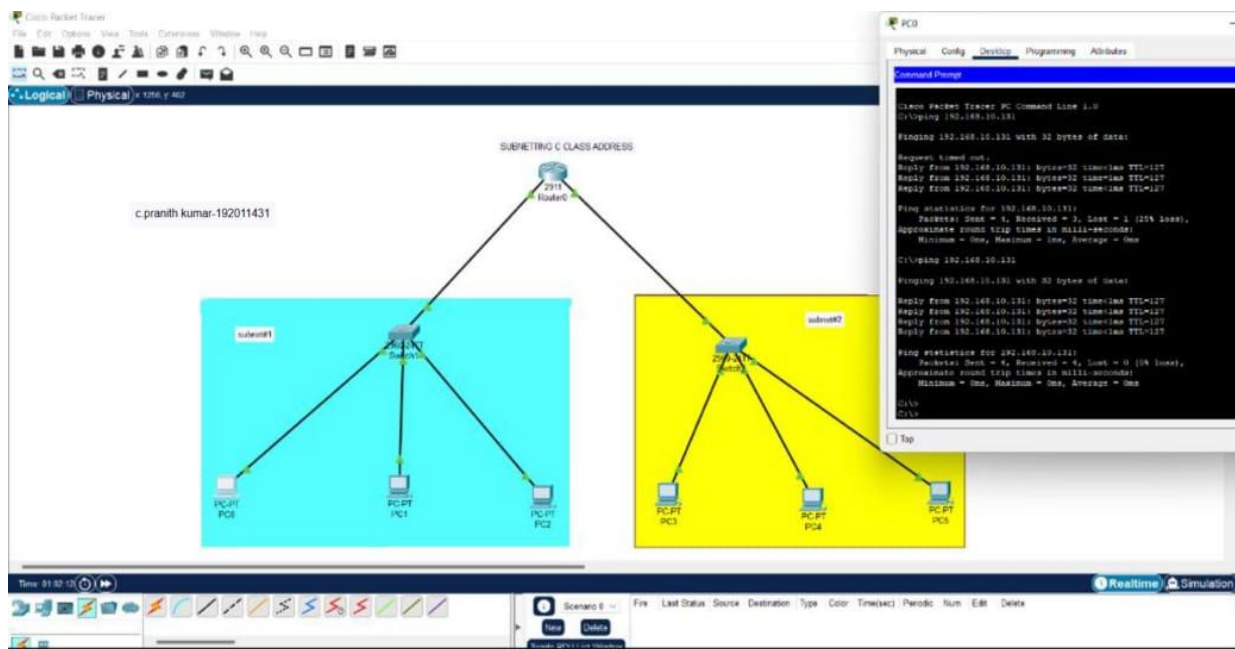
LLDP



CSMA CD/CA



SUB NETTING



ARP USING WIRESHARK

Wireshark packet capture showing ARP requests. The capture is on the 'arp' filter. The table shows 13 packets, all of which are ARP requests from source IP 192.168.139.201 to destination IP 192.168.139.253. The packet details show the Ethernet II frame and the ARP request.

No.	Time	Source	Destination	Protocol	Length	Info
7	11.068004	de:0e:24:1f:bf:4c	Broadcast	ARP	42	Who has 192.168.139.201? Tell 192.168.139.253
11	20.070348	de:0e:24:1f:bf:4c	Broadcast	ARP	42	Who has 192.168.139.201? Tell 192.168.139.253
13	21.088732	de:0e:24:1f:bf:4c	Broadcast	ARP	42	Who has 192.168.139.201? Tell 192.168.139.253
15	29.285069	de:0e:24:1f:bf:4c	Broadcast	ARP	42	Who has 192.168.139.201? Tell 192.168.139.253
16	30.308644	de:0e:24:1f:bf:4c	Broadcast	ARP	42	Who has 192.168.139.201? Tell 192.168.139.253
17	31.336216	de:0e:24:1f:bf:4c	Broadcast	ARP	42	Who has 192.168.139.201? Tell 192.168.139.253
19	39.325181	de:0e:24:1f:bf:4c	Broadcast	ARP	42	Who has 192.168.139.201? Tell 192.168.139.253
20	40.347048	de:0e:24:1f:bf:4c	Broadcast	ARP	42	Who has 192.168.139.201? Tell 192.168.139.253
21	41.373946	de:0e:24:1f:bf:4c	Broadcast	ARP	42	Who has 192.168.139.201? Tell 192.168.139.253

Frame 13: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{3657754C-7678-45EA-B548-ACD694A6EACA}, id 0
Ethernet II, Src: de:0e:24:1f:bf:4c (de:0e:24:1f:bf:4c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

0000 ff ff ff ff ff de 0e 24 1f bf 4c 08 06 00 01 \$-L-...
0010 08 00 06 04 00 01 de 0e 24 1f bf 4c 08 06 00 01 \$-L-...
0020 00 00 00 00 00 00 c0 a8 8b c9

HTTP USING WIRESHARK

The screenshot shows a Wireshark capture of HTTP traffic on interface \Device\NPF_{3657754C-7678-45EA-B548-ACD694A6EACA}. The packet list shows a GET request (No. 806) and a 206 Partial Content response (No. 808). The packet details pane shows the structure of the HTTP response, including the status bar (206 Partial Content) and the Content-Type (application/x-chrome-extension). The packet bytes pane shows the raw data of the response, including the status bar and the content body.

No.	Time	Source	Destination	Protocol	Length	Info
806	4.811788	2409:4072:693:64db:...	2606:2800:147:120f:...	HTTP	431	HEAD /filestreamingservice/files/01236773-1436-4b98-8dd4-67c470fcb917?P1=16...
808	4.868350	2606:2800:147:120f:...	2409:4072:693:64db:...	HTTP	901	HTTP/1.1 206 OK
813	4.952439	2409:4072:693:64db:...	2606:2800:147:120f:...	HTTP	503	GET /filestreamingservice/files/01236773-1436-4b98-8dd4-67c470fcb917?P1=16...
818	5.573902	2606:2800:147:120f:...	2409:4072:693:64db:...	HTTP	848	HTTP/1.1 206 Partial Content (application/x-chrome-extension)
825	8.071936	2409:4072:693:64db:...	2606:2800:147:120f:...	HTTP	506	GET /filestreamingservice/files/01236773-1436-4b98-8dd4-67c470fcb917?P1=16...
828	8.126361	2606:2800:147:120f:...	2409:4072:693:64db:...	HTTP	698	HTTP/1.1 206 Partial Content (application/x-chrome-extension)
830	9.301378	2409:4072:693:64db:...	2606:2800:147:120f:...	HTTP	506	GET /filestreamingservice/files/01236773-1436-4b98-8dd4-67c470fcb917?P1=16...
835	9.640565	2606:2800:147:120f:...	2409:4072:693:64db:...	HTTP	330	HTTP/1.1 206 Partial Content (application/x-chrome-extension)
837	10.359376	2409:4072:693:64db:...	2606:2800:147:120f:...	HTTP	506	GET /filestreamingservice/files/01236773-1436-4b98-8dd4-67c470fcb917?P1=16...
840	10.405077	2606:2800:147:120f:...	2409:4072:693:64db:...	HTTP	81	HTTP/1.1 206 Partial Content (application/x-chrome-extension)

Frame 806: 431 bytes on wire (3448 bits), 431 bytes captured (3448 bits) on interface \Device\NPF_{3657754C-7678-45EA-B548-ACD694A6EACA}, id 0

Ethernet II, Src: IntelCor_29:6e:13 (ec:63:d7:29:6e:13), Dst: de:0e:24:1f:bf:4c (de:0e:24:1f:bf:4c)

Internet Protocol Version 6, Src: 2409:4072:693:64db:c8f6:fbf0:fb:ae:1, Dst: 2606:2800:147:120f:30c:1ba0:fc6:265a

Transmission Control Protocol, Src Port: 51759, Dst Port: 80, Seq: 1, Ack: 1, Len: 357

Hypertext Transfer Protocol

de 0e 24 1f bf 4c ec 63 d7 29 6e 13 86 dd 60 0c ..\$.L.c.)n...
91 57 01 79 06 fe 24 09 40 72 06 93 64 db c8 f6 .W.y..\$.@n..d...
0020 fb f0 0f bb ae d1 26 06 28 00 01 47 12 0f 03 0c&- (.G....
0030 1b a0 0f c6 26 5a ca 2f 00 50 94 c5 14 27 eb ae&Z/ .P....
0040 99 0a 50 18 02 02 0b 06 00 00 48 45 41 44 20 2f ..P.....HEAD /
0050 66 69 6c 65 73 74 72 65 61 6d 69 6e 67 73 65 72 filestre amingser
0060 76 69 63 65 2f 66 69 6c 65 73 2f 30 31 32 33 36 vice/fil es/01236
0070 37 37 33 2d 31 34 33 36 2d 34 62 39 38 2d 38 64 773-1436 -4b98-8d
0080 64 34 2d 36 37 63 34 37 30 66 63 62 39 31 37 3f d4-67c47 0fcb917?
0090 50 31 3d 31 36 37 35 34 34 34 34 35 38 26 50 32 P1=16754 44458&P2
00a0 3d 34 30 34 26 50 33 3d 32 26 50 34 3d 66 38 25 =404&P3= 2&P4=f8%
00b0 32 66 50 39 7a 49 25 32 66 79 33 38 38 63 51 32 2fP9zI%2 fy388cQ2
00c0 61 25 32 66 64 4c 68 61 4c 4a 48 30 79 30 69 43 a%2fdLh LJH0y0iC

Hypertext Transfer Protocol: Protocol

Packets: 3244 · Displayed: 26 (0.8%)

Profile: Default

28°C Mostly sunny

10:35 AM 1/28/2023

TCP USING WIRESHARK

The screenshot shows a Wireshark capture of TCP traffic on interface \Device\NPF_{3657754C-7678-45EA-B548-ACD694A6EACA}. The packet list shows a RST packet (No. 3141) and subsequent ACKs (Nos. 3142, 3143, 3144, 3145, 3146, 3147, 3148, 3149). The packet details pane shows the structure of the TCP RST packet, including the sequence number (Seq=1) and the acknowledgment number (Ack=1). The packet bytes pane shows the raw data of the RST packet, including the sequence number and the acknowledgment number.

No.	Time	Source	Destination	Protocol	Length	Info
3141	116.889805	2620:1ec:4e:1::58	2409:4072:693:64db:...	TCP	74	443 → 51731 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3142	119.978167	192.168.139.208	13.76.45.26	TCP	55	[TCP Keep-Alive] 51673 → 443 [ACK] Seq=571 Ack=263 Win=510 Len=1
3143	120.049755	13.76.45.26	192.168.139.208	TCP	66	[TCP Keep-Alive ACK] 443 → 51673 [ACK] Seq=263 Ack=572 Win=16383 Len=0 SLE...
3144	123.036191	2409:4072:693:64db:...	2606:2800:147:120f:...	TCP	74	51761 → 80 [FIN, ACK] Seq=356 Ack=713 Win=130816 Len=0
3145	123.082643	2606:2800:147:120f:...	2409:4072:693:64db:...	TCP	74	80 → 51761 [FIN, ACK] Seq=713 Ack=357 Win=67072 Len=0
3146	123.082767	2409:4072:693:64db:...	2606:2800:147:120f:...	TCP	74	51761 → 80 [ACK] Seq=357 Ack=714 Win=130816 Len=0
3147	123.169020	2409:4072:693:64db:...	2606:2800:147:120f:...	TCP	74	51762 → 80 [FIN, ACK] Seq=2599 Ack=1678229 Win=263424 Len=0
3148	123.218468	2606:2800:147:120f:...	2409:4072:693:64db:...	TCP	74	80 → 51762 [FIN, ACK] Seq=1678229 Ack=2600 Win=72192 Len=0
3149	123.218585	2409:4072:693:64db:...	2606:2800:147:120f:...	TCP	74	51762 → 80 [ACK] Seq=2600 Ack=1678230 Win=263424 Len=0

Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{3657754C-7678-45EA-B548-ACD694A6EACA}, id 0

Ethernet II, Src: de:0e:24:1f:bf:4c (de:0e:24:1f:bf:4c), Dst: IntelCor_29:6e:13 (ec:63:d7:29:6e:13)

Internet Protocol Version 6, Src: 2620:1ec:c11:239, Dst: 2409:4072:693:64db:c8f6:fbf0:fb:ae:1

Transmission Control Protocol, Src Port: 443, Dst Port: 51738, Seq: 1, Ack: 1, Len: 0

ec 63 d7 29 6e 13 de 0e 24 1f bf 4c 86 dd 62 8e .c.)n... \$.L..b.
c6 7e 00 14 06 34 26 20 01 ec 0c 11 00 00 00 0048.....
0020 00 00 00 00 02 39 24 09 40 72 06 93 64 db c8 f69\$.@n..d...
0030 fb f0 0f bb ae d1 01 bb ca 1a ad d4 75 b9 12 dfu....
0040 ab 4a 50 10 40 02 38 91 00 00 .JP.@-8-...

Transmission Control Protocol: Protocol

Packets: 3149 · Displayed: 3052 (96.9%)

Profile: Default

28°C Mostly sunny

10:33 AM 1/28/2023

UDP USING WIRESHARK

The image shows a Wireshark capture of network traffic on a Wi-Fi interface. The packet list pane displays several packets, with packet 1048 selected. The packet details pane shows the structure of the selected packet, and the packet bytes pane shows the raw data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
801	4.753083	192.168.139.253	192.168.139.208	DNS	267	Standard query response 0x3250 AAAA msedge.b.tlu.dl.delivery.mp.microsoft.com
802	4.755903	192.168.139.253	192.168.139.208	DNS	255	Standard query response 0xc844 A msedge.b.tlu.dl.delivery.mp.microsoft.com
820	6.259806	192.168.139.208	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
821	7.009498	192.168.139.208	192.168.139.253	DNS	181	Standard query 0x4cf9 A msedge.b.tlu.dl.delivery.mp.microsoft.com
822	7.009737	192.168.139.208	192.168.139.253	DNS	181	Standard query 0x4cf9 A msedge.b.tlu.dl.delivery.mp.microsoft.com
823	7.062787	192.168.139.253	192.168.139.208	DNS	255	Standard query response 0x4cf9 A msedge.b.tlu.dl.delivery.mp.microsoft.com
824	7.062787	192.168.139.253	192.168.139.208	DNS	267	Standard query response 0x4cf9 A msedge.b.tlu.dl.delivery.mp.microsoft.com
1047	16.384150	192.168.139.253	224.0.0.251	MDNS	681	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local
1048	16.384150	fe80::dc0e:24ff:fe1... ff02::fb		MDNS	701	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local

Packet Details (Frame 1):

- Frame 1: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits) on interface \Device\NPF_{3657754C-7678-45EA-B548-ACD694A6EACA}, id 0
- Ethernet II, Src: de:0e:24:1f:bf:4c (de:0e:24:1f:bf:4c), Dst: IntelCor_29:6e:13 (ec:63:d7:29:6e:13)
- Internet Protocol Version 4, Src: 192.168.139.253, Dst: 192.168.139.208
- User Datagram Protocol, Src Port: 53, Dst Port: 55873
- Domain Name System (response)

Packet Bytes:

```
0000  ec 63 d7 29 6e 13 de 0e 24 1f bf 4c 08 00 45 00 .c.)n...$.L..E.
0010  00 b6 25 2c 40 00 40 11 7b ec c0 a8 8b fd c0 a8 ...%.@- {...
0020  8b d0 00 35 da 41 00 a2 c0 42 f6 3f 81 80 00 01 ...S-A...B?...
0030  00 02 00 01 00 00 04 65 64 67 65 09 6d 69 63 72 .....e dge-micr
0040  6f 73 6f 66 74 03 63 6f 6d 00 00 41 00 01 c0 0c osoft co m-A...
0050  00 05 00 01 00 00 0c a7 00 2d 12 65 64 67 65 2d .....edge-
0060  6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 0b 64 75 microsof t-com-du
0070  61 6c 2d 61 2d 30 30 33 36 08 61 2d 6d 73 65 64 al-a-003 6-a-msd
0080  67 65 03 6e 65 74 00 c0 30 00 05 00 01 00 00 00 ge.net... ..
0090  1d 00 02 c0 43 c0 4f 00 06 00 01 00 00 00 c6 00 ...C.O. ....
00a0  23 03 6e 73 31 c0 4f 06 6d 73 6e 68 73 74 c0 11 #ns1.O: msnhst...
00b0  78 2b 22 e5 00 00 07 08 00 00 03 84 00 24 ea 00 x+.....$.
00c0  00 00 00 f0 .....
```