

Practical 0

Aim:- To get familiarise with Cisco Packet Tracer and WireShark.

Part A:- What is Cisco Packet Tracer and Wireshark?

Cisco Packet Tracer is a network simulation tool developed by Cisco Systems. It's widely used for teaching and learning networking concepts, Internet of Things (IoT), and cybersecurity skills in a virtual lab environment. Packet Tracer allows users to create network topologies by dragging and dropping virtual devices like routers, switches, and PCs. It's a valuable tool for students and instructors to practice and understand networking without needing physical hardware.

Features:

1. **Network Simulation:** Create and simulate networks with a wide range of Cisco devices, including routers, switches, and PCs.
2. **Interactive Learning:** Provides an interactive platform for learning and understanding network concepts, protocols, and configurations.
3. **Multi-User Functionality:** Allows multiple users to collaborate and interact with the same network topology, enhancing collaborative learning.
4. **Network Modeling:** Supports complex network models with both logical and physical views, enabling users to visualize the entire network setup.
5. **IoT and Cybersecurity:** Includes simulation capabilities for Internet of Things (IoT) devices and cybersecurity scenarios, expanding learning opportunities.

Use Cases:

- **Education:** Widely used in academic institutions to teach networking fundamentals and Cisco certification courses (CCNA, CCNP).
- **Self-Learning:** Enables students and professionals to practice and reinforce their networking skills.
- **Network Design:** Helps network administrators and engineers to prototype and test network designs before deployment.

Wireshark is a free and open-source network protocol analyzer. It's used for network traffic analysis and troubleshooting. Wireshark captures and inspects packets from network connections, allowing users to see the detailed data being transmitted over the network. It's a powerful tool for network administrators, security professionals, and anyone interested in understanding network behavior and diagnosing issues.

Features:

1. **Packet Capture:** Captures live data packets from network interfaces, providing a detailed view of network activity.
2. **Protocol Analysis:** Supports thousands of network protocols, enabling users to analyze specific protocol behaviors and interactions.
3. **Filtering and Search:** Advanced filtering options allow users to focus on specific types of traffic or network events, making it easier to diagnose issues.
4. **Reassembly:** Reassembles and displays the data streams of certain protocols, such as TCP or HTTP, for detailed inspection.
5. **Visualization:** Offers graphical representations of traffic patterns and network statistics, helping users to understand network performance and trends.

Use Cases:

- **Network Troubleshooting:** Helps network administrators to identify and resolve network issues, such as latency, packet loss, and configuration errors.
- **Security Analysis:** Used by cybersecurity professionals to detect and analyze security threats, intrusions, and vulnerabilities.
- **Protocol Development:** Assists protocol developers in testing and debugging new protocols or modifications to existing ones.

Part B:- How to work in Cisco Packet Tracer and Wireshark.

Cisco Packet Tracer is an advanced network simulation tool that allows users to visualize and experiment with network configurations and operations in a virtual environment. Here's a brief guide on how to get started:

1. **Creating a Network:**
 - Open Cisco Packet Tracer.
 - Drag and drop devices (like routers, switches, PCs) from the device palette onto the workspace.
 - Use the connection tool to link devices together with cables (copper straight-through, copper crossover, etc.).
2. **Configuring Devices:**
 - Click on a device to open its configuration window.
 - Configure basic settings like IP addresses, subnet masks, and routing protocols.
 - For routers and switches, use the CLI (Command Line Interface) tab to input commands.

3. Simulating Network Activity:

- Use the simulation mode to visualize packet flows between devices.
- Add applications (like web browsing or file transfer) to endpoints and observe how packets travel through the network.

4. Collaborative Learning:

- Utilize multi-user functionality to collaborate with others on the same network topology, enhancing interactive learning experiences.

5. Saving and Sharing:

- Save your network topology by going to File > Save.
- Share the saved .pkt file with others who can open it in their Cisco Packet Tracer.

Wireshark is a powerful network protocol analyzer that captures and displays data packets traveling through a network. Here's how you can start using it:

1. Capturing Packets:

- Open Wireshark.
- Select the network interface you want to capture traffic from (e.g., Ethernet, Wi-Fi).
- Click on the "Start Capturing Packets" button.

2. Analyzing Packets:

- As packets are captured, they will appear in the main window.
- Click on a packet to view its details. The window will split into three sections: a summary of the capture, detailed packet information, and a hexadecimal representation.

3. Filtering Traffic:

- Use display filters to isolate specific types of traffic. For example, to view only HTTP traffic, type `http` in the filter bar.
- Apply various filters to focus on specific protocols, IP addresses, or port numbers.

4. Packet Reassembly:

- Use reassembly features to analyze complete data streams, such as reassembling TCP streams to view entire communications.

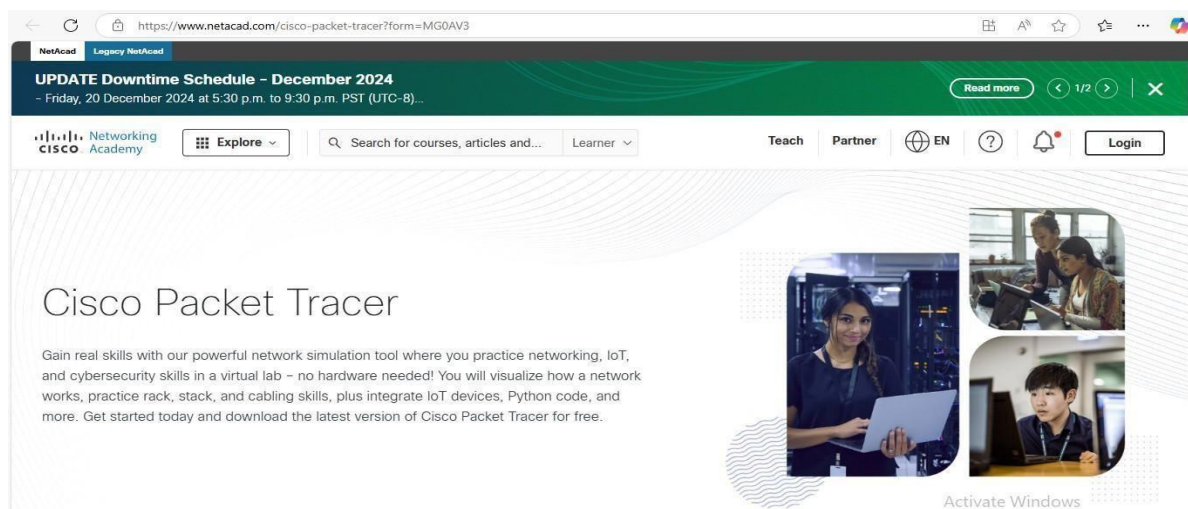
5. Saving and Exporting:

- Save your capture data by going to File > Save As.
- Export specific packets or entire capture sessions for further analysis.

Part C:- How to download the Cisco Packet Tracer and Wireshark.

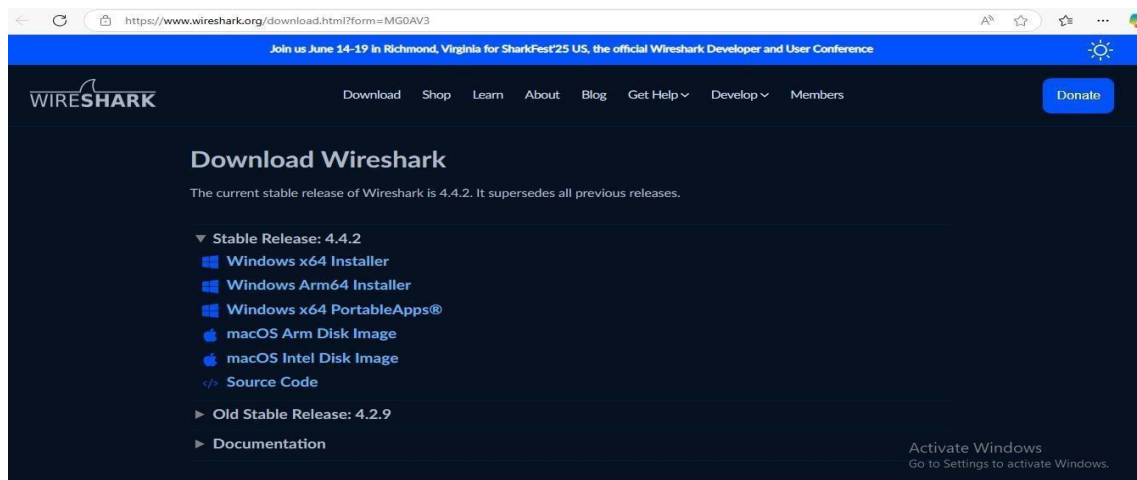
Downloading Cisco Packet Tracer:-

1. **Visit the Cisco Networking Academy website:** Go to the Cisco Packet Tracer download page.
2. **Create an Account:** If you don't have a Cisco Networking Academy account, you'll need to create one.
3. **Download the Software:** Once logged in, you can download Cisco Packet Tracer for your operating system (Windows, macOS, or Linux).



Downloading Wireshark:-

1. **Visit the Wireshark website:** Go to the Wireshark download page.
2. **Choose Your Version:** Select the appropriate installer for your operating system (Windows, macOS, or Linux).
3. **Download and Install:** Click the download link and follow the installation instructions.



Practical 1

Aim:- Experiments on Simulation Tools (Cisco Packet Tracer).

Topologies:-

1. Ring :-

A ring topology is a network configuration where device connections create a circular data path. Each networked device is connected to two others, like points on a circle. Together, devices in a ring topology are referred to as a ring network.

Step1: Select PCs and switches(2950-24) then connect PCs to switches with straight-through(straight wire) and switches to switches with crossover(dashed wired)

Step2: Connect them as shown in the image above. Also give them a proper IP address.

Step3: Pass a message and check the simulation.

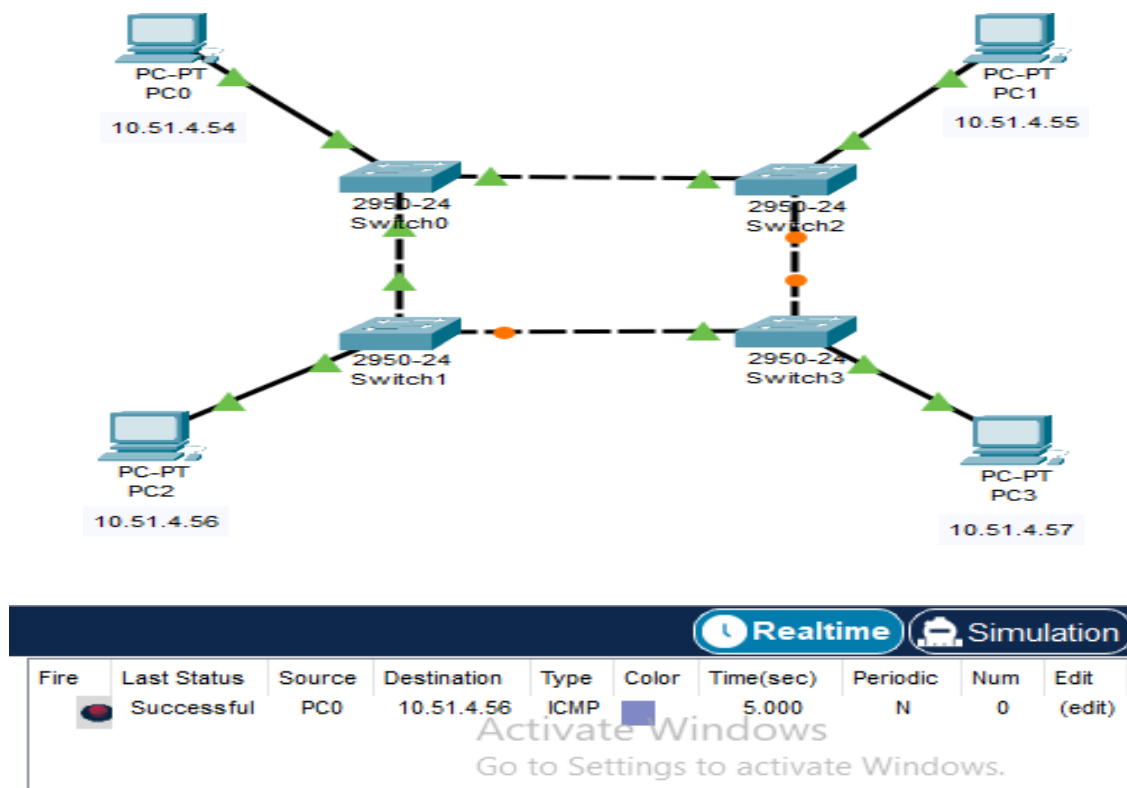


Figure 1.1: Ring Topology

2. MESH

A mesh topology is a network setup where each computer and network device is interconnected with one another. This topology setup allows for most transmissions to be distributed even if one of the connections goes down. It is a topology commonly used for wireless networks.

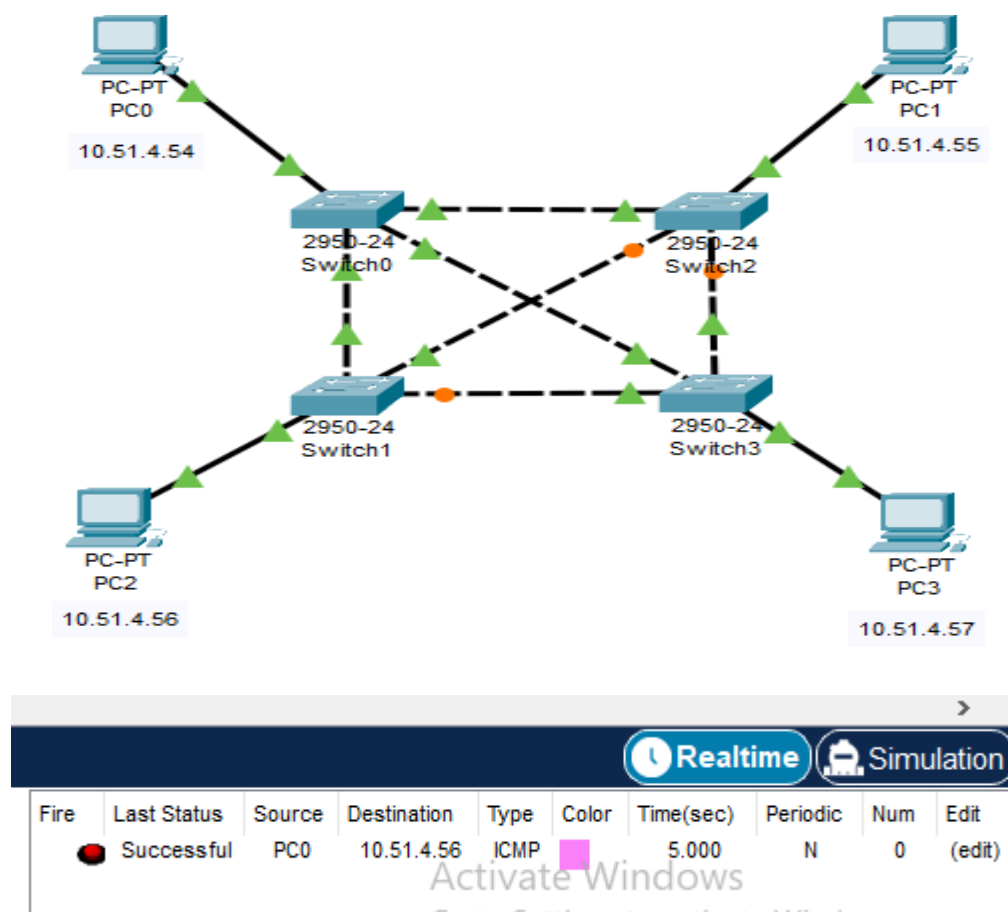


Figure 1.2: Mesh Topology

3. Star

A star topology is a topology for a Local Area Network (LAN) in which all nodes are individually connected to a central connection point, like a hub or a switch. A star takes more cable than e.g. a bus, but the benefit is that if a cable fails, only one node will be brought down.

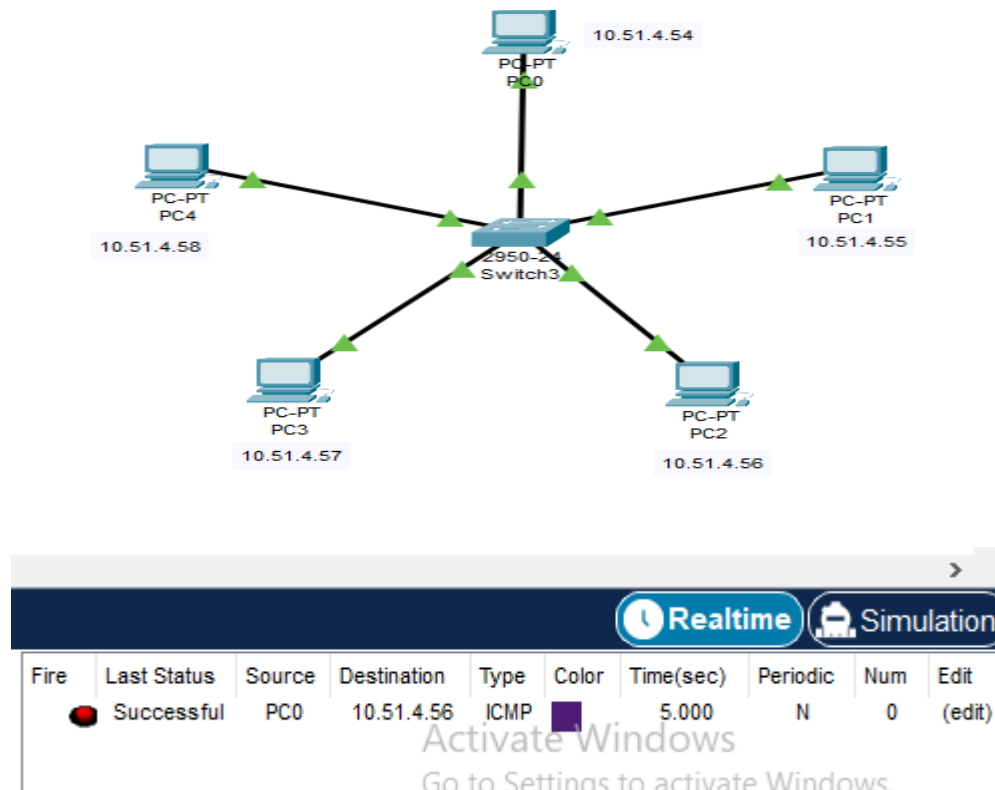
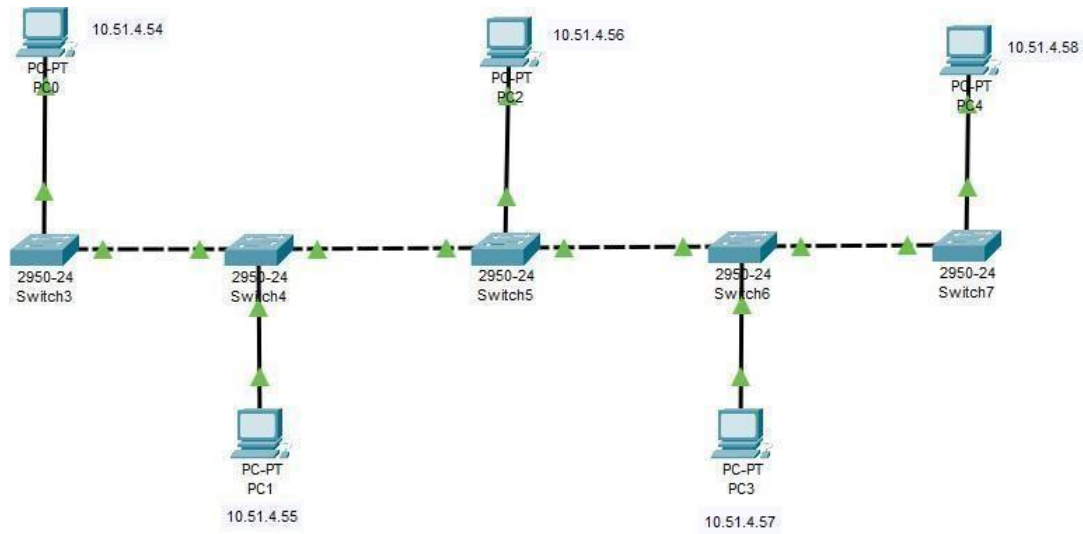


Figure 1.3: Star Topology

4. BUS

A bus topology is a topology for a Local Area Network (LAN) in which all the nodes are connected to a single cable. The cable to which the nodes connect is called a "backbone". If the backbone is broken, the entire segment fails.





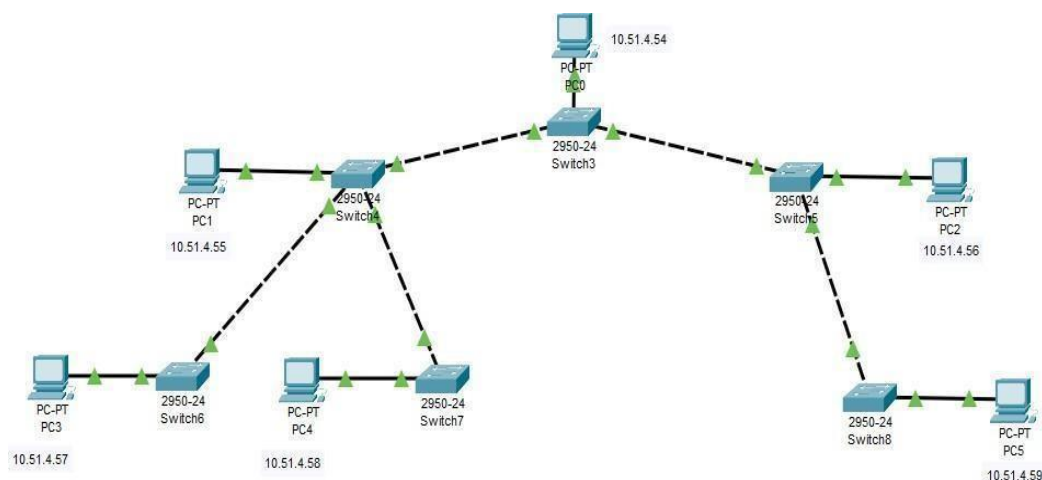
<div> <div>Realtime</div> <div>Simulation</div> </div>									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	10.51.4.57	ICMP		5.000	N	0	(edit)

Figure 1.4: Bus Topology

5. TREE

A tree topology is a special type of structure where many connected elements are arranged like the branches of a tree. For example, tree topologies are frequently used to organize the computers in a corporate network, or the information in a database.





<div> <div>Realtime</div> <div>Simulation</div> </div>									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	10.51.4.58	ICMP		5.000	N	0	(edit)

Figure 1.5: Tree Topology

6. HYBRID

A hybrid topology is a type of network topology that uses two or more different network topologies. These topologies can include a mix of bus topology, mesh topology, ring topology, star topology, and tree topology.

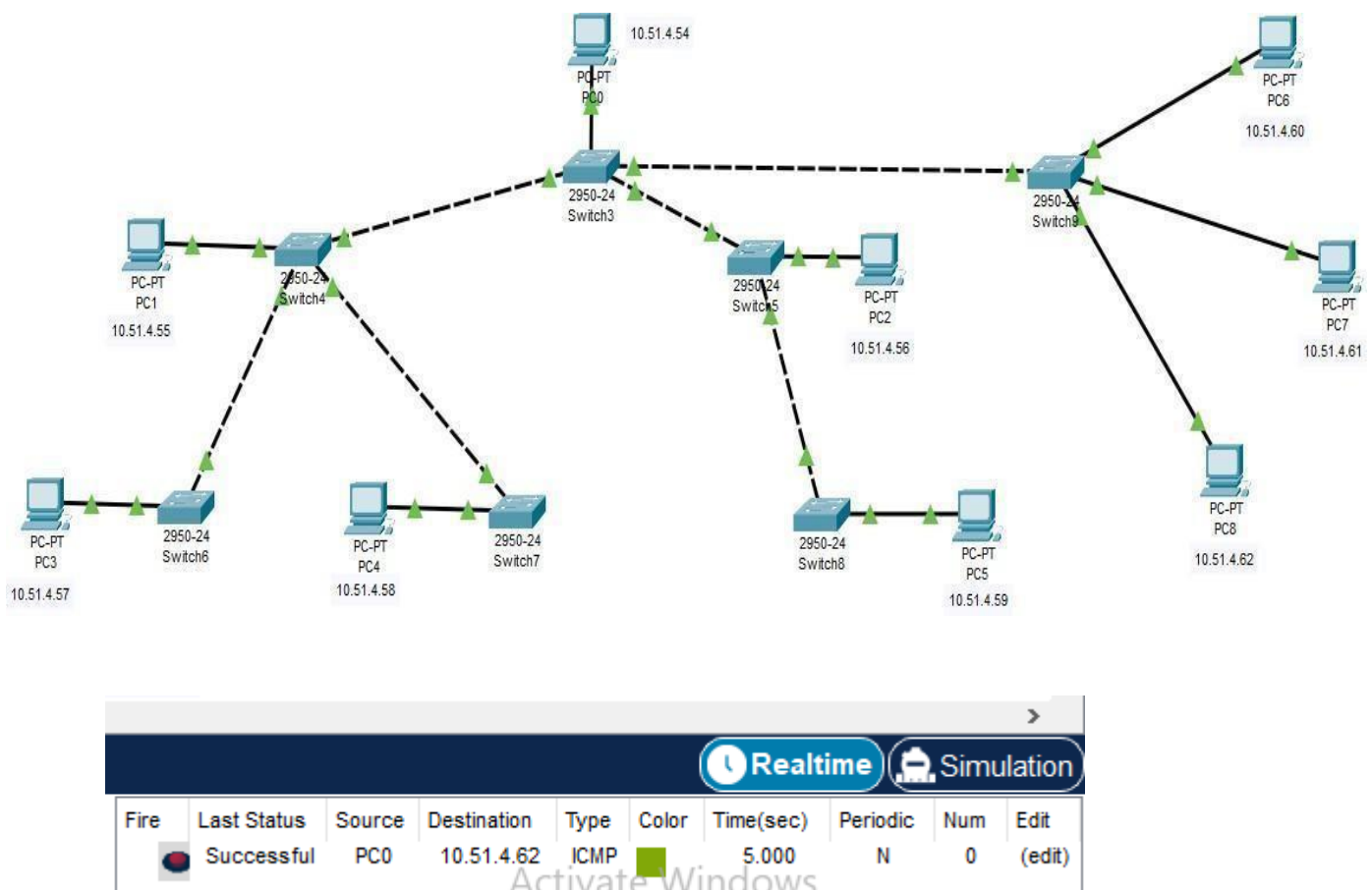


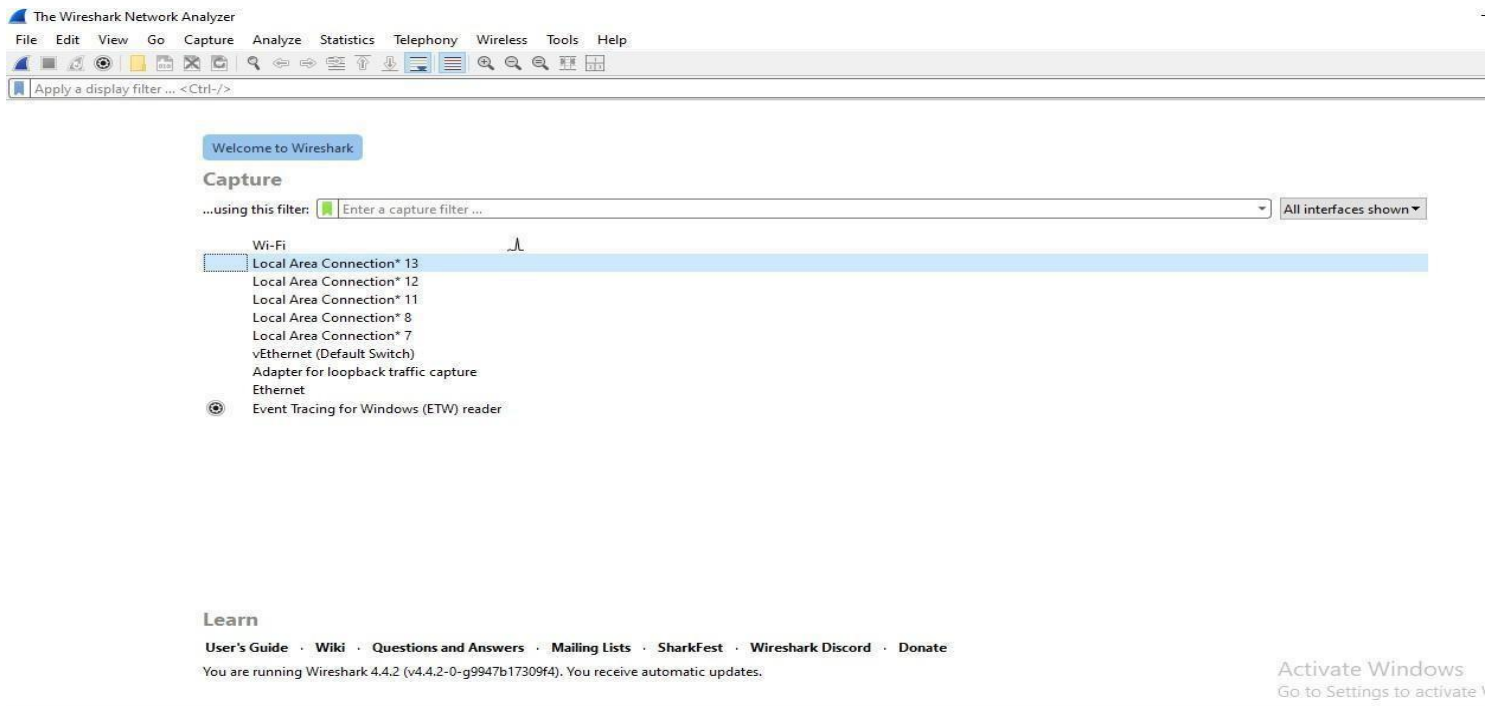
Figure 1.6: Hybrid Topology

Practical 2

Aim:- To understand features of Wireshark as a packet capture tool and understand encapsulation of information. Also study the effect of a few network commands.

Purpose:

The main objective of the proposed experiment is to give exposure of Wireshark tools to students so they can learn to monitor transmission packets being sent in Wi-Fi and LAN environments.



Features:

1. **Live Packet Capture:** Captures live data packets from network interfaces.
2. **File Import:** Can open files containing packet data captured with other programs like tcpdump.
3. **Protocol Dissectors:** Supports thousands of network protocols, providing detailed information about each packet.
4. **Detailed Display:** Displays packets with detailed protocol information, including headers and payloads.
5. **Filtering:** Allows users to filter packets based on various criteria, such as protocol type, IP address, or port number.

Encapsulation of Information :-

Encapsulation is the process of wrapping data with protocol-specific headers and trailers as it moves down the OSI model layers. Each layer adds its own header (and sometimes trailer) to the data from the upper layer, creating a new data unit. For example, an HTTP message is encapsulated within a TCP segment, which is then encapsulated within an IP packet, and finally, the IP packet is encapsulated within an Ethernet frame.

Capturing from Wi-Fi

No.	Time	Source	Destination	Protocol	Length	Info
2566	157.091272	192.168.0.114	20.189.173.8	TCP	54	54849 → 443 [ACK] Seq=198 Ack=6321 Win=262144 Len=0
2567	157.147003	192.168.0.114	20.189.173.8	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2568	157.182285	TPLink_db:fe:dc	Broadcast	ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
2569	157.377771	20.189.173.8	192.168.0.114	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
2570	157.377975	192.168.0.114	20.189.173.8	TCP	54	54849 → 443 [ACK] Seq=356 Ack=6372 Win=261888 Len=0
2571	157.382766	192.168.0.114	20.189.173.8	TLSv1.2	968	Application Data
2572	157.591892	TPLink_db:fe:dc	Broadcast	ARP	42	Who has 192.168.0.106? Tell 192.168.0.1
2573	157.623552	20.189.173.8	192.168.0.114	TLSv1.2	581	Application Data
2574	157.623765	192.168.0.114	20.189.173.8	TCP	54	54849 → 443 [ACK] Seq=1270 Ack=6899 Win=261376 Len=0
2575	157.854726	23.54.83.211	192.168.0.114	TLSv1.2	78	Application Data
2576	157.901713	192.168.0.114	23.54.83.211	TCP	54	54779 → 443 [ACK] Seq=502 Ack=73 Win=508 Len=0
2577	158.103945	TPLink_db:fe:dc	Broadcast	ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
2578	159.845843	TPLink_db:fe:dc	Broadcast	ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
2579	160.049741	TPLink_db:fe:dc	Broadcast	ARP	42	Who has 192.168.0.109? Tell 192.168.0.1
2580	160.357113	TPLink_db:fe:dc	Broadcast	ARP	42	Who has 192.168.0.106? Tell 192.168.0.1
2581	160.873353	TPLink_db:fe:dc	Broadcast	ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
2582	160.971643	TPLink_db:fe:dc	Broadcast	ARP	42	Who has 192.168.0.109? Tell 192.168.0.1
2583	161.380871	TPLink_db:fe:dc	Broadcast	ARP	42	Who has 192.168.0.106? Tell 192.168.0.1

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF...
Ethernet II, Src: TPLink_db:fe:dc (54:af:97:db:fe:dc), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 54 af 97 db fe dc 08 06 00 01T.....
0010 08 00 06 04 00 01 54 af 97 db fe dc c0 a8 00 01T.....
0020 00 00 00 00 00 00 c0 a8 00 6aj.....

HTTP (Hypertext Transfer Protocol) :-

HTTP is the foundation of data communication on the web. It's the protocol used to load web pages using hypertext links. It defines how messages are formatted and transmitted, and how web servers and browsers should respond to various commands. When you enter a URL in your web browser, an HTTP request is sent to the web server, which then returns the requested webpage.

Capturing from Wi-Fi

No.	Time	Source	Destination	Protocol	Length	Info
456	98.394518	10.226.10.43	34.104.35.123	HTTP	314	HEAD /edgedl/diffgen-puffin/hfnkpihlhgieaddgfemjhofmblmnib/8c072a630910a6a89a32f254b5ee8ba7d074b8d31aa78346dcf..
459	98.425042	34.104.35.123	10.226.10.43	HTTP	642	HTTP/1.1 200 OK
460	98.460832	10.226.10.43	34.104.35.123	HTTP	386	GET /edgedl/diffgen-puffin/hfnkpihlhgieaddgfemjhofmblmnib/8c072a630910a6a89a32f254b5ee8ba7d074b8d31aa78346dcf..
462	98.494569	34.104.35.123	10.226.10.43	HTTP	161	HTTP/1.1 416 Requested Range Not Satisfiable
470	98.514329	10.226.10.43	34.104.35.123	HTTP	314	HEAD /edgedl/diffgen-puffin/hfnkpihlhgieaddgfemjhofmblmnib/8c072a630910a6a89a32f254b5ee8ba7d074b8d31aa78346dcf..
472	98.544689	34.104.35.123	10.226.10.43	HTTP	642	HTTP/1.1 200 OK
473	98.581598	10.226.10.43	34.104.35.123	HTTP	386	GET /edgedl/diffgen-puffin/hfnkpihlhgieaddgfemjhofmblmnib/8c072a630910a6a89a32f254b5ee8ba7d074b8d31aa78346dcf..
488	98.632871	10.226.10.43	34.104.35.123	HTTP	314	HEAD /edgedl/diffgen-puffin/hfnkpihlhgieaddgfemjhofmblmnib/8c072a630910a6a89a32f254b5ee8ba7d074b8d31aa78346dcf..
490	98.654164	34.104.35.123	10.226.10.43	HTTP	642	HTTP/1.1 200 OK
491	98.689732	10.226.10.43	34.104.35.123	HTTP	386	GET /edgedl/diffgen-puffin/hfnkpihlhgieaddgfemjhofmblmnib/8c072a630910a6a89a32f254b5ee8ba7d074b8d31aa78346dcf..
493	98.716067	34.104.35.123	10.226.10.43	HTTP	161	HTTP/1.1 416 Requested Range Not Satisfiable
576	105.782119	10.226.10.43	34.104.35.123	HTTP	314	HEAD /edgedl/diffgen-puffin/hfnkpihlhgieaddgfemjhofmblmnib/8c072a630910a6a89a32f254b5ee8ba7d074b8d31aa78346dcf..
578	105.800677	34.104.35.123	10.226.10.43	HTTP	603	HTTP/1.1 200 OK
579	105.845183	10.226.10.43	34.104.35.123	HTTP	386	GET /edgedl/diffgen-puffin/hfnkpihlhgieaddgfemjhofmblmnib/8c072a630910a6a89a32f254b5ee8ba7d074b8d31aa78346dcf..
595	105.892921	10.226.10.43	34.104.35.123	HTTP	314	HEAD /edgedl/diffgen-puffin/hfnkpihlhgieaddgfemjhofmblmnib/8c072a630910a6a89a32f254b5ee8ba7d074b8d31aa78346dcf..
598	105.916059	34.104.35.123	10.226.10.43	HTTP	642	HTTP/1.1 200 OK

Frame 55: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits) on interface \Device\NPF...
Ethernet II, Src: NonHsiPrecis_a6:d3:45 (40:49:0f:a6:d3:45), Dst: PaloAltoNetw_e2:80:58 (b4:0e:06:27:80:58)
Internet Protocol Version 4, Src: 10.226.10.43, Dst: 34.104.35.123
Transmission Control Protocol, Src Port: 52363, Dst Port: 80, Seq: 1, Ack: 1, Len: 260
Hypertext Transfer Protocol

0000 b4 0e 25 e2 80 58 40 0f a6 d3 45 08 00 45 00 %..X@I...E..
0010 01 2c cc 90 40 00 80 06 d2 4b 0a e2 0a 2b 22 68 .,.-@...K...+h
0020 23 7b cc 80 00 50 bf 64 69 f8 5d f9 fe df 50 18 #[...P.d 1 j...P
0030 82 05 2e 0f 00 00 48 45 41 44 20 2f 65 64 67 65HE AD /edge
0040 64 6c 2f 64 69 66 66 67 65 6e 2d 70 75 66 66 69 d1/diffg en-puffi
0050 6e 2f 68 66 6e 6b 70 69 6d 6c 68 68 67 69 65 61 n/hfnkpi mlhg1ea
0060 64 64 67 65 65 6d 6a 68 6f 66 6d 66 62 6c 6d 6e ddgfemjhf ofmblm
0070 69 62 2f 38 63 30 37 32 61 36 33 30 39 31 30 61 tb/0c072 a630910a
0080 36 61 38 39 61 33 32 66 32 35 34 62 35 65 65 38 6a89a32f 254b5ee8
0090 62 61 37 64 30 37 34 62 38 64 33 31 61 61 37 38 ba7d074b 8d31aa78
00a0 33 34 36 64 63 66 31 37 63 36 37 30 63 37 36 62 346dcf17 c670c76b
00b0 66 39 65 20 40 54 54 50 2f 31 2a 31 0d 0a 43 6f f9e HTTP /1.1 Co
00c0 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 nnection : Keep-A
00d0 6c 69 76 65 0d 0a 41 63 65 70 74 3a 20 2a 2f live-Ac cept: /*
00e0 2a 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 *. Accep t-encodi
00f0 6e 67 3a 20 69 64 65 6e 74 69 74 79 0d 0e 55 73 ng: Iden tity-Us
0100 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 er-Agent : Micros
0110 6f 66 74 20 42 49 54 53 2f 37 2e 38 0d 0a 48 6f oft B1RS /7.8 HoVS
0120 73 74 3a 20 65 64 67 65 64 6c 2e 6d 65 2e 6f 76 Go to: edge.dl.me.gov
0130 74 31 2e 63 6f 6d 0d 0a 0d 0a

DNS (Domain Name System) :-

DNS is like the phonebook of the internet. It translates domain names (like www.example.com) into IP addresses that computers use to identify each other on the network. When you type a domain name into your browser, a DNS server translates that name into the corresponding IP address, allowing your browser to locate the web server and access the website.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
117	28.967983	10.226.10.43	218.248.114.1	DNS	86	Standard query 0x878c A android.clients.google.com
118	28.969747	10.226.10.43	218.248.114.1	DNS	86	Standard query 0xd0c9 HTTPS android.clients.google.com
119	28.990821	218.248.114.1	10.226.10.43	DNS	160	Standard query response 0xd0c9 HTTPS android.clients.google.com CNAME android.l.google.com SOA ns1.google.com
120	28.992009	218.248.114.1	10.226.10.43	DNS	366	Standard query response 0x878c A android.clients.google.com CNAME android.l.google.com A 142.250.193.46 A 142.250.193.46
674	118.846043	10.226.10.43	49.45.0.4	DNS	89	Standard query 0x14cb A t-ring-fallback-s2.msedge.net
675	118.854937	49.45.0.4	10.226.10.43	DNS	167	Standard query response 0x14cb A t-ring-fallback-s2.msedge.net CNAME t-ring.s-part2-t-9999.fb-t-msedge.net CNAME ...
697	119.060252	10.226.10.43	49.45.0.4	DNS	87	Standard query 0x90c9 A fp-vp-nocache.azureedge.net
698	119.104757	10.226.10.43	218.248.114.1	DNS	87	Standard query 0x90c9 A fp-vp-nocache.azureedge.net
699	119.129402	218.248.114.1	10.226.10.43	DNS	162	Standard query response 0x90c9 A fp-vp-nocache.azureedge.net CNAME fp-vp-nocache.ec.azureedge.net CNAME cs9.wpc.v...
745	119.766051	10.226.10.43	49.45.0.4	DNS	77	Standard query 0x48b4 A fp-afd.azurefd.us
746	119.772568	49.45.0.4	10.226.10.43	DNS	248	Standard query response 0x48b4 A fp-afd.azurefd.us CNAME t-0001.msedge.azure.us CNAME eafd-3p-profile.usgovtraffi...
799	120.965090	10.226.10.43	49.45.0.4	DNS	90	Standard query 0xf18a A self.events.data.microsoft.com
800	120.975492	49.45.0.4	10.226.10.43	DNS	208	Standard query response 0xf18a A self.events.data.microsoft.com CNAME self-events-data.trafficmanager.net CNAME o...

> Frame 117: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF...
 > Ethernet II, Src: HonHaiPrecis_a6:d3:45 (40:49:0f:a6:d3:45), Dst: PaloAltoNetw_e2:80:58 (b4:0c:06:27:00:58)
 > Internet Protocol Version 4, Src: 10.226.10.43, Dst: 218.248.114.1
 > User Datagram Protocol, Src Port: 60264, Dst Port: 53
 > Domain Name System (query)

0000 b4 0c 25 e2 80 58 40 49 0f a6 d3 45 08 00 45 00 ...X@I...E..E..
 0010 00 48 51 c5 00 00 80 11 86 d9 0a e2 0a 2b da f8 ...HQ.....+..
 0020 72 01 eb 68 00 35 00 34 77 54 87 8c 01 00 00 01 ...h54WT.....
 0030 00 00 00 00 00 00 07 61 6e 64 72 6f 69 64 07 63a android-c
 0040 6c 69 65 6e 74 73 06 67 6f 6f 67 6c 65 03 63 6f ...lients:g oogle-co
 0050 6d 00 00 01 00 01 m.....

TCP (Transmission Control Protocol) :-

TCP is one of the main protocols in the Internet Protocol (IP) suite. It provides reliable, ordered, and error-checked delivery of data between applications communicating over a network. TCP ensures that data sent from one end of a connection arrives correctly at the other end, by establishing a connection, managing data transfer, and handling errors or lost packets.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
2646	300.068766	10.226.10.43	117.18.232.200	TCP	54	52380 → 443 [ACK] Seq=890 Ack=7579 Win=260864 Len=0
2653	303.721176	10.226.10.43	204.79.197.203	TCP	54	52409 → 443 [RST, ACK] Seq=4369 Ack=27624 Win=0 Len=0
2658	306.494101	10.226.10.43	148.113.9.138	TCP	55	[TCP Keep-Alive] 51853 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1
2659	306.510599	148.113.9.138	10.226.10.43	TCP	66	[TCP Keep-Alive ACK] 443 → 51853 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
2662	306.989286	10.226.10.43	172.253.118.188	TCP	55	[TCP Keep-Alive] 52113 → 5228 [ACK] Seq=1 Ack=1 Win=508 Len=1
2663	307.075230	172.253.118.188	10.226.10.43	TCP	66	[TCP Keep-Alive ACK] 5228 → 52113 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
2696	316.520738	10.226.10.43	148.113.9.138	TCP	55	[TCP Keep-Alive] 51853 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1
2697	316.538722	148.113.9.138	10.226.10.43	TCP	66	[TCP Keep-Alive ACK] 443 → 51853 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
2708	326.543341	10.226.10.43	148.113.9.138	TCP	55	[TCP Keep-Alive] 51853 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1
2710	326.559444	148.113.9.138	10.226.10.43	TCP	66	[TCP Keep-Alive ACK] 443 → 51853 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
2719	331.814945	10.226.10.43	34.104.35.123	TCP	54	52416 → 80 [FIN, ACK] Seq=282 Ack=552 Win=131584 Len=0
2720	331.816016	10.226.10.43	34.104.35.123	TCP	66	52417 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2721	331.838568	34.104.35.123	10.226.10.43	TCP	60	80 → 52416 [FIN, ACK] Seq=552 Ack=283 Win=66816 Len=0
2722	331.838692	10.226.10.43	34.104.35.123	TCP	54	52416 → 80 [ACK] Seq=283 Ack=553 Win=131584 Len=0
2728	332.821214	10.226.10.43	34.104.35.123	TCP	66	[TCP Retransmission] 52417 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2729	332.837370	34.104.35.123	10.226.10.43	TCP	60	80 → 52417 [RST] Seq=1 Win=0 Len=0

> Frame 2505: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF...
 > Ethernet II, Src: HonHaiPrecis_a6:d3:45 (40:49:0f:a6:d3:45), Dst: PaloAltoNetw_e2:80:58 (b4:0c:06:27:00:58)
 > Internet Protocol Version 4, Src: 10.226.10.43, Dst: 34.104.35.123
 > Transmission Control Protocol, Src Port: 52415, Dst Port: 80, Seq: 635, Ack: 660, Len: 0

0000 b4 0c 25 e2 80 58 40 49 0f a6 d3 45 08 00 45 00 ...X@I...E..E..
 0010 00 28 cd a8 40 00 00 06 d2 37 0a e2 0a 2b 22 68 ...(-@...7...+h
 0020 23 7b cc bf 00 50 48 99 57 32 84 f3 b6 04 50 10 ...#{...PH.W2....P
 0030 02 02 ab 0f 00 00

Practical 3

Aim :- To study behavior of generic devices used for networking: (Cisco Packet Tracer)

Summary of devices we use:

Switch 2950-54:

The Cisco Catalyst 2950C 24 and Catalyst 2950T 24 Switches belong to the Cisco Catalyst 2950 series of high-performance, standalone, 10/100 auto sensing Fast Ethernet and Gigabit Ethernet switches. Both products bring intelligent services to the network edge to accommodate the needs of growing workgroups and server connectivity.

Router 4321:

The Cisco 4000 Series Integrated Services Routers (ISR) revolutionize WAN communications in the enterprise branch. With new levels of built-in intelligent network capabilities and convergence, the routers specifically address the growing need for application-aware networking in distributed enterprise sites.

Hub-pt:

Hub is a very simple network device that is used in LANs. It is basically a multiport repeater. Hubs do not decide anything and forwards any traffic to all of the ports. So, they are not smart devices.

Server:

Servers are an entirely different breed when compared to other end devices. They have various functionalities and also have space for two network interfaces. The modules available for servers are the same as PC modules, except that the servers do not have the PC-HOST-NM-1AM module.

Meraki server:

The Meraki cloud solution is a centralized management service that allows users to manage all of their Meraki network devices via a single simple and secure platform. Users are able to deploy, monitor and configure their Meraki devices via the Meraki dashboard web interface or via APIs.

Ip phone:

IP telephony refers to any phone system that uses an internet connection to send and receive voice data. Unlike a regular telephone that uses landlines to transmit analog signals, IP phones connect to the internet via a router and modem.

Voip device:

A VoIP phone or IP phone uses voice over IP technologies for placing and transmitting telephone calls over an IP network, such as the Internet, instead of the traditional public switched telephone network (PSTN).

Copper straight through wire:

This is a standard Ethernet cable that is used to connect two devices that operate in different layers of the OSI model (such as hub to router and switch to PC). It can be used with Ethernet, Fast Ethernet and Gigabit Ethernet port types.

Copper cross over wire:

This Ethernet cable connects devices operating in the same OSI layer (such as hub to hub, PC to PC, PC to router, and PC to printer). This cable can also be used with Ethernet, Fast Ethernet and Gigabit Ethernet ports .

Phone:-

The mobile phone network enables wireless communication using mobile devices, such as mobile phones, smartphones or tablets. Mobile phone networks provide the necessary infrastructure and are operated by mobile phone providers.

Automatically choose connection wire:

Connections can be made automatically by choosing the connection type shown below. Router links will be red or not active until you correctly configure the interfaces.

Coaxial wire:

The coaxial cable used to connect the Cisco uBR7200 series universal broadband routers at the headend should be very high-quality cable because imperfections that do not visibly affect video transmissions can significantly affect digital data transmissions.

Sniffer:

I have assignment that i need to create full "Network", using all device like switch, hub, server ..etc.The problem that i force that i need to use "Sniffer" its first time to me using that device. I need help on how to configure or connect the Sniffer with my network.

Smart device:

A smart device is an electronic device, generally connected to other devices or networks via different wireless protocols such as Bluetooth, Zigbee, NFC, Wi-Fi, LiFi, 5G, etc., that can operate to some extent interactively and autonomously.

Mcu-pt board:

Components are physical objects that connect to microcontrollers (MCU-PT) or single boarded computers (SBC-PT). They typically do not have a network interface and rely on the MCU-PT or SBC-PT for network access. These are simple devices that only communicate through their analog or digital slots.

Web server in Cisco packet trace :-

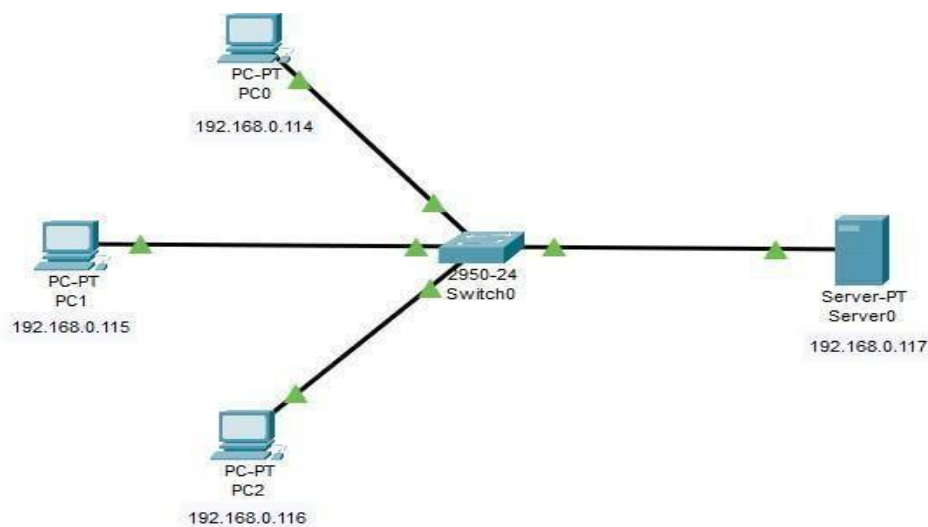


Figure 3.1

- In this lesson we will learn about how to create the first web server on cisco packet tracer that can be applied on a real time web server.
- So we are taking a few PCs and one web server and one switch for connecting all devices. Make sure all devices should be connected by straight through cable because for connecting different devices, straight through cable is required. Assign IPs to each end device (server and PCs) of a single network with subnet mask It can different as per your choice.
- Then go to server>services>http in that enable http and https modes.In that go to index.html and edit. In that write the message you want... At the end click on save.and close it .

- Then we go to PC1 and in that we select the desktop and we write the IP address of the server and click on enter. You can see the message which you wrote in the server message.

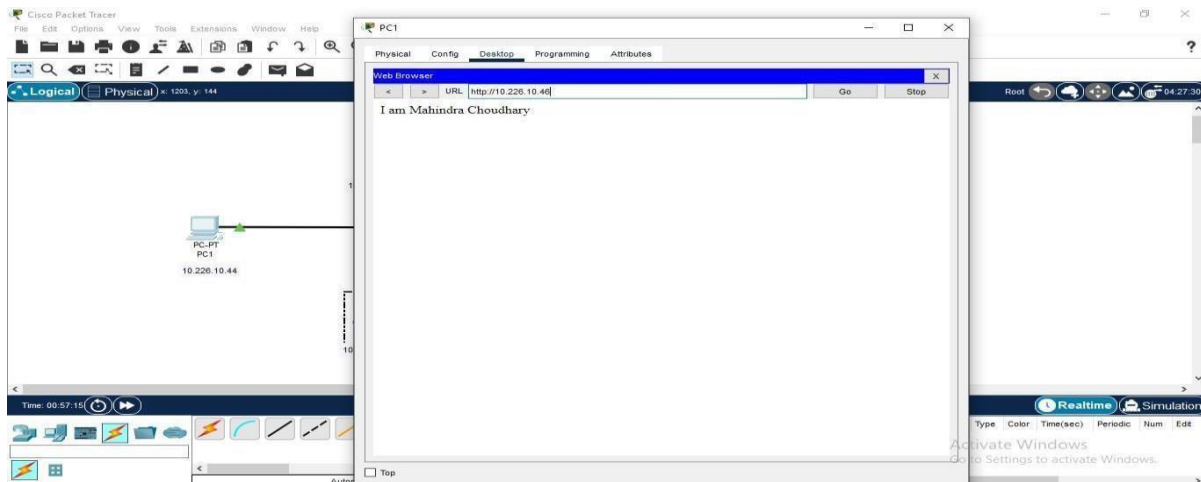


Figure 3.2

- If you want to see that your connection is proper or not then you want to click on your pc then desktop>command prompt and in that you need to write ping 190.0.0.1(IT_address). And enter.

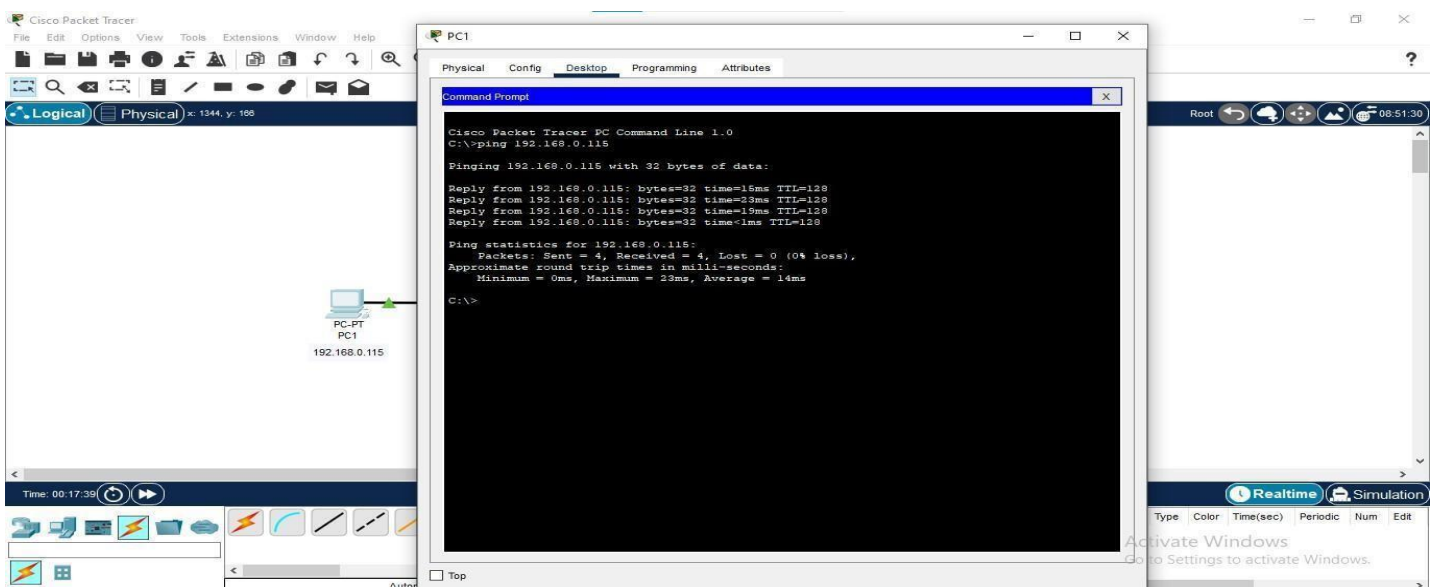


Figure 3.3

Use of switch :-

A switch is used in a wired network to connect to other devices using Ethernet cables. The switch allows each connected device to talk to the others. Wireless-only networks do not use switches because devices such as wireless routers and adapters communicate directly with one another.

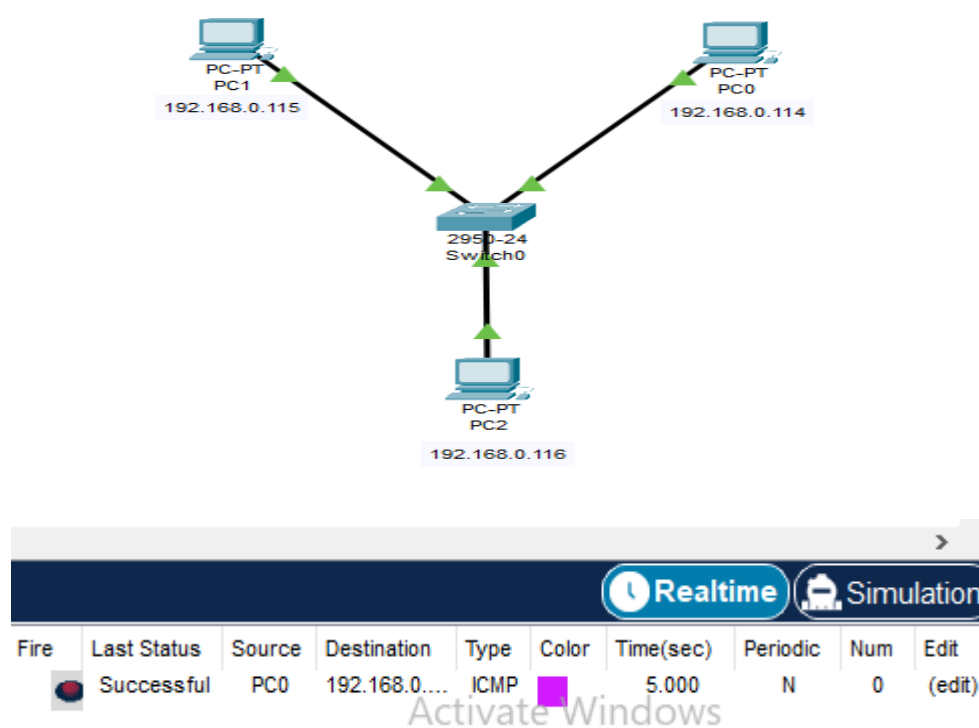


Figure 3.4

- Connect multiple hosts: Normally, a switch provides a large number of ports for cable connections, allowing for star topology routing. It is usually used to connect multiple PCs to the network.
- Forwards a message to a specific host: Like a bridge, a switch uses the same forwarding or filtering logic on each port. When any host on the network or a switch sends a message to another host on the same network or the
- Same switch, the switch receives and decodes the frames to read the physical (MAC) address portion of the message.
- Manage traffic: A switch in networking can manage traffic either coming into or exiting the network and can connect devices like computers and access points with ease.

- Keep electrical signal undistorted: When a switch forwards a frame, it regenerates an undistorted square electrical signal.
- Increase LAN bandwidth: A switch divides a LAN into multiple collision domains with independent broadband, thus greatly increasing the bandwidth of the LAN.

Use of hub :-

A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN.

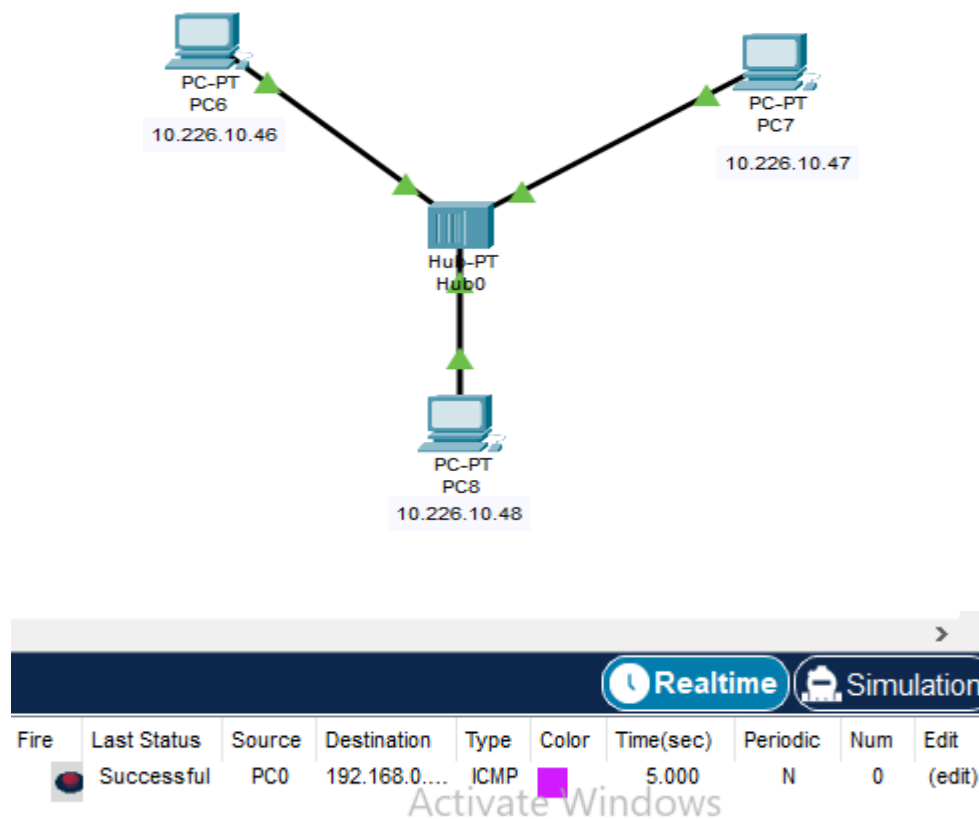


Figure 3.5

A hub has many ports in it. A computer which intends to be connected to the network is plugged into one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.

When a Hub receives data from one of the connected devices, it passes data to all the other ports without checking for the destination device except the port through which it receives the data. Below figure, shows the working of a HUB.



Figure 3.6

Consider, Device A wants to send data to device D. When device A sends data, the hub receives it through one port and transfers the data to all the other connected devices instead of passing it to only device D. This feature of the hub leads to congestion and extends the collision domain. So, it is considered as an inefficient device and needs more bandwidth for working.

Difference between switch and hub :-

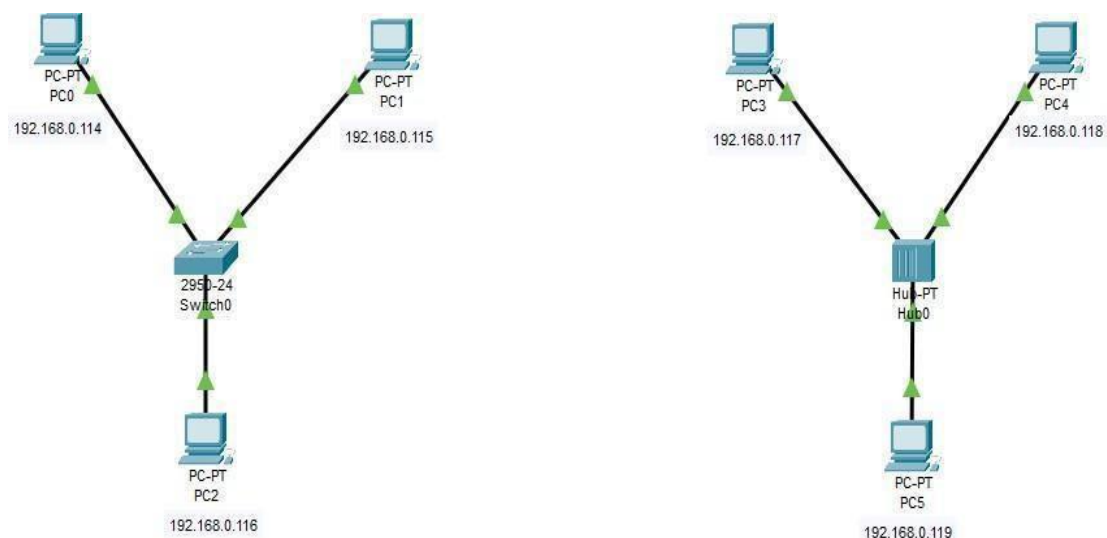


Figure 3.7

HUB	SWITCH
<ul style="list-style-type: none"> ● A hub operates on the physical layer. 	<ul style="list-style-type: none"> ● A switch operates on the data link layer.
<ul style="list-style-type: none"> ● Hubs perform frame flooding that can be unicast, multicast, or broadcast. 	<ul style="list-style-type: none"> ● It performs broadcast, then the unicast and multicast as needed.
<ul style="list-style-type: none"> ● Just a singular domain of collision is present in a hub. 	<ul style="list-style-type: none"> ● Varied ports have separate collision domains.
<ul style="list-style-type: none"> ● Transmission mode is Half-duplex. 	<ul style="list-style-type: none"> ● Transmission mode is Full duplex.
<ul style="list-style-type: none"> ● Hubs operates as a Layer 1 device per the OSI model. 	<ul style="list-style-type: none"> ● Network switches help you to operate at Layer 2 of the OSI model.
<ul style="list-style-type: none"> ● To connect a network of personal computers should be joined through a central hub. 	<ul style="list-style-type: none"> ● Allow connecting multiple devices and ports.
<ul style="list-style-type: none"> ● Uses electrical signal orbits. 	<ul style="list-style-type: none"> ● Uses frame & packet
<ul style="list-style-type: none"> ● Does not offer Spanning-Tree. 	<ul style="list-style-type: none"> ● Multiple Spanning-Tree is possible
<ul style="list-style-type: none"> ● Collisions occur mostly in setups using hubs. 	<ul style="list-style-type: none"> ● No collisions occur in a full-duplex switch.
<ul style="list-style-type: none"> ● Hub is a passive device. 	<ul style="list-style-type: none"> ● A switch is an active device
<ul style="list-style-type: none"> ● A network hub can't store MAC addresses. 	<ul style="list-style-type: none"> ● Switches use CAM (Content Accessible Memory) that can be accessed by ASIC (Application Specific Integrated Chips).
<ul style="list-style-type: none"> ● Not an intelligent device. 	<ul style="list-style-type: none"> ● Intelligent device.
<ul style="list-style-type: none"> ● Its speed is up to 10 Mbps. 	<ul style="list-style-type: none"> ● 10/100 Mbps, 1 Gbps, 10 Gbps
<ul style="list-style-type: none"> ● Does not use software. 	<ul style="list-style-type: none"> ● Has software for administration.

Practical 4

Aim :- Data Link Layer (Error Detection).

The **Data Link Layer** is the second layer in the OSI (Open Systems Interconnection) model, positioned just above the Physical Layer. Its primary purpose is to provide reliable data transfer across a physical link by organizing data into frames, detecting and correcting errors, and controlling the flow of data.

Key Functions of the Data Link Layer :-

1. Framing :-

- Divides data from the Network Layer into manageable units called *frames* for transmission.
- Adds a header and a trailer to the frame to provide necessary information for error detection and control.

2. Error Detection and Correction :-

- Ensures that errors introduced during transmission (e.g., due to noise, interference) are identified and, if possible, corrected.
- Common techniques include :-
 - **Parity Checking:** Adds a parity bit to detect single-bit errors.
 - **Cyclic Redundancy Check (CRC):** Adds a checksum value derived from the data, which is verified at the receiver.
 - **Checksums:** A simpler error-checking method based on the summation of data segments.

3. Flow Control :-

- Manages the rate of data transfer to ensure the receiver is not overwhelmed by data.

4. Error Handling :-

- Retransmits corrupted frames when errors are detected, using techniques like Automatic Repeat Request (ARQ).

5. Addressing :-

- Incorporates physical addresses (MAC addresses) to identify devices on the same local network.

6. Medium Access Control (MAC) :-

- Coordinates access to the physical transmission medium to avoid collisions.

Error Detection:

Error detection is a crucial aspect of the Data Link Layer. It ensures the integrity of data during transmission. When data is sent over a network, it is susceptible to corruption caused by electrical noise, interference, or hardware issues. Error detection techniques help identify these corruptions.

Errors in data transmission can occur in various forms, depending on how bits are altered during transit. The main types are **single-bit error** and **burst-bit error**:

1. Single-Bit Error :-

- **Definition:** Only one bit in a data unit (e.g., a frame or packet) is altered during transmission.
- **Causes:** Typically occurs due to a brief noise spike or electrical interference.

Detection and Correction :-

- Simple error detection methods like **parity checks** are sufficient to detect single-bit errors. Correction may require retransmission.

2. Burst-Bit Error:

- **Definition:** Two or more consecutive bits in a data unit are altered during transmission.
- **Causes:** Commonly caused by interference lasting over multiple clock cycles, such as electrical surges or cross-talk.

Detection and Correction:

- Techniques like **CRC** or **interleaving** are effective in detecting burst errors.
- Correcting burst errors can be challenging without retransmission.

Common Techniques for Error Detection:

1. Parity Bit:

- Adds an extra bit to the data to make the number of 1s either even (even parity) or odd (odd parity).
- Simple and fast but can detect only single-bit errors.

2. Checksum:

- Divides data into segments, sums them, and appends the sum (checksum) to the data.
- The receiver recalculates the sum to detect mismatches.

3. Cyclic Redundancy Check (CRC):

- Uses polynomial division to calculate a checksum based on the data.
- Extremely robust and widely used in network protocols like Ethernet.

4. Hamming Code:

- Adds redundancy bits to data, allowing the detection and correction of single-bit errors and detection of double-bit errors.

5. Frame Check Sequence (FCS):

- A field in the frame's trailer containing a value calculated from the frame's contents (e.g., using CRC).

Source Code :-

```
#include<stdio.h>

void main(){

int data[10];

int dataatrec[10],c,c1,c2,c3,i;

printf("Enter 4 bits of data one by one\n");

scanf("%d",&data[0]);

scanf("%d",&data[1]);

scanf("%d",&data[2]);

scanf("%d",&data[4]);

//Calculation of even parity

data[6]=data[0]^data[2]^data[4];

data[5]=data[0]^data[1]^data[4];

data[3]=data[0]^data[1]^data[2];
```

```
printf("\nEncoded data is\n");

for(i=0;i<7;i++)

printf("%d",data[i]);

printf("\n\nEnter received data bits one by one\n");

for(i=0;i<7;i++)

scanf("%d",&dataatrec[i]);

c1=dataatrec[6]^dataatrec[4]^dataatrec[2]^dataatrec[0]

;

c2=dataatrec[5]^dataatrec[4]^dataatrec[1]^dataatrec[0]

;

c3=dataatrec[3]^dataatrec[2]^dataatrec[1]^dataatrec[0]

;c=c3*4+c2*2+c1 ;

if(c==0) {

printf("\nNo error while transmission of data\n");

}

else {

printf("\nError on position

%d",c); printf("\nDatsent :");

for(i=0;i<7;i++)

printf("%d",data[i]);

printf("\nData received : ");

for(i=0;i<7;i++)

printf("%d",dataatrec[i]);

printf("\nCorrect message is\n");

//if errorneous bit is 0 we complement it else vice versa

if(dataatrec[7-c]==0)
```

```
dataatrec[7-c]=1;

else

dataatrec[7-c]=0;

for (i=0;i<7;i++) {

printf("%d",dataatrec[i]);

}

}

}
```

Output :-

```
PS C:\Programs\C++ (Phase 3)> cd "c:\Programs\C++
Enter 4 bits of data one by one
1
1
0
1

Encoded data is
1100110

Enter received data bits one by one
1
1
0
1
1
1
0

Error on position 4
Datasant :1100110
Data received : 1101110
Correct message is
1100110
PS C:\Programs\C++ (Phase 3)> █
```

Practical 5

Aim :- Virtual LAN : Simulate Virtual LAN

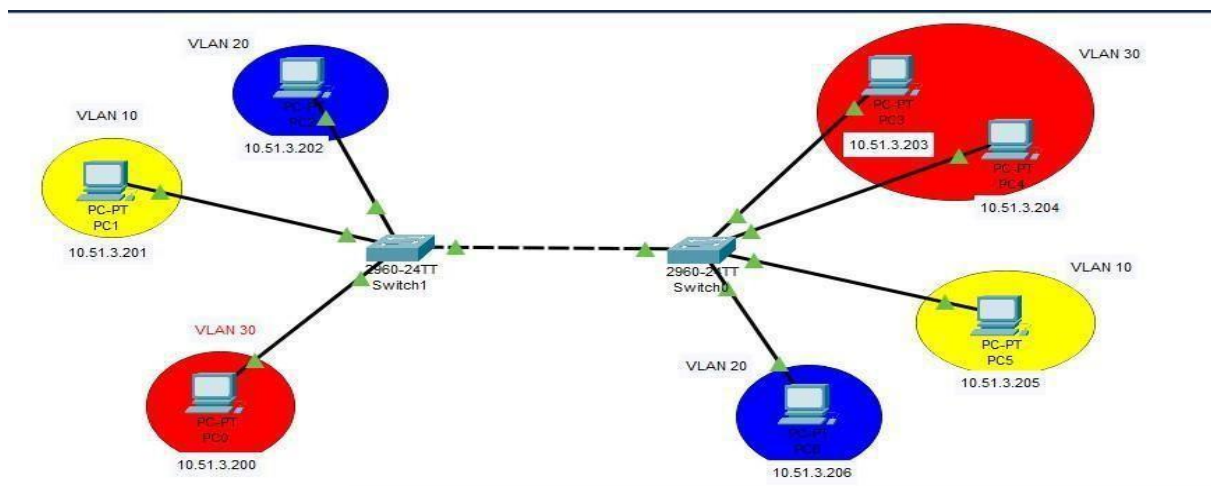
Configuration using cisco packet tracer

Tracer Simulation

DESCRIPTION -

STEP 1: Make a network

- Connect the pcs and switches shown in the below figure. Give IP address.
- Connect pcs to switches with copper straight through and connect switches to one another with copper cross over.



STEP 2: Configure VLAN on all switches.

- Go to switch0 CLI, enter ENA command to enable switch.

```
Physical  Config  CLI  Attributes  IOS

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
Switch>en
Translating "Switch>en"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name blue
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name yellow
Switch(config-vlan)#exit
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief
```

Write the following. commands conf t>vlan 10> name yellow>exit as shown below.

- Do the same for second Vlan 20 and name it orange.
- Repeat the process for switch1.

To see the vlan the command used is >show vlan brief. The output of the command is below,

```
Switch#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   blue                    active
20   yellow                  active
1002 fddi-default            active
1003 token-ring-default     active
1004 fddinet-default         active
1005 trnet-default           active
Switch#
Switch#
```

STEP 3: Configure TRUNK MODE.

- To enable trunk mode the first go to switch CLI
- The command ena>conf t>interface fa0/7>switchport mode trunk.
- This is to be done for every switches ports.
- The below figure shows the command.

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fa0/6
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface fa0/5
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#
```


STEP 4: Configure ACCESS MODE.

- ACCESS MODE is configured for all the pcs who are connect to the switch
- To configure access mode for pc command `ena>conf t>interface fa0/1>switchport mode access>switchport access vlan10>exit.`

```
Switch#  
%SYS-5-CONFIG_I: Configured from console by console  
  
Switch#ena  
Switch#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#interface fa0/1  
Switch(config-if)#switchport mode access  
Switch(config-if)#switchport access vlan 10  
Switch(config-if)#exit  
Switch(config)#exit  
Switch#  
%SYS-5-CONFIG_I: Configured from console by console
```

This is to be done with each pc connected to the switch.

Communication in same and different vlans with two switches.

