

FACULTY OF ENGINEERING AND TECHNOLOGY

BACHELOR OF TECHNOLOGY

Computer Network (303105256)

4th SEMESTER (2ND YEAR)

COMPUTER SCIENCE & ENGINEERING DEPARTMENT





**PARUL UNIVERSITY**

FACULTY OF ENGINEERING & TECHNOLOGY PARUL INSTITUTE OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

STUDENT DETAILS

| NAME | : | Kishan Kushwaha |
| --- | --- | --- |
| ENROLLMENT NO | : | 2303031050253 |
| SUBJECT | : | COMPUTER NETWORKS |
| SUBJECT CODE | : | 303105256 |
| SEMESTER | : | 4th |
|  |  |  |



# FACULTY OF ENGINEERING AND TECHNOLOGY BACHELOR OF TECHNOLOGY

**CERTIFICATE**

**This is to certify that Mr. Kishan Kushwaha with**

**enrollment no. 2303031050253 has successfully completed**

**his/her laboratory experiments in the**

**COMPUTER NETWORKS (303105256) from the**

**department of COMPUTER SCIENCE AND ENGINEERING during the**

**academic year 2024-25.**

### Date of Submission: .........................

**Staff In charge: ............................... Head of Department: .....**...............

**INDEX**

| **Sr. No** | **Experiment Title** | **Number of Hours** | **Page No.** | **Date of Performance** | **Date of Assessment** | **Marks (out of 10)** | **Sign** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Experiments on Simulation Tools (CISCO PACKET TRACER). | 2 |  |  |  |  |  |
| 2 | Experiment of Packet Capture Tool: Wireshark. | 2 |  |  |  |  |  |
| 3 | To study behaviour of generic devices used for networking: (cisco packet tracer). | 2 |  |  |  |  |  |
| 4 | To Perform the Data Link layer (Error Detection). | 2 |  |  |  |  |  |
| 5 | Virtual LAN. | 2 |  |  |  |  |  |
| 6 | Wireless LAN. | 2 |  |  |  |  |  |
| 7 | Internetworking with Routers. | 2 |  |  |  |  |  |
| 8 | Implementation of Subnetting | 2 |  |  |  |  |  |
| 9 | Routing at Networking Layer. | 2 |  |  |  |  |  |
| 10 | Experiment on Transport Layer. | 2 |  |  |  |  |  |

**Practical: 1**

**Aim: Experiments on Simulation Tools (CISCO PACKET TRACER).**

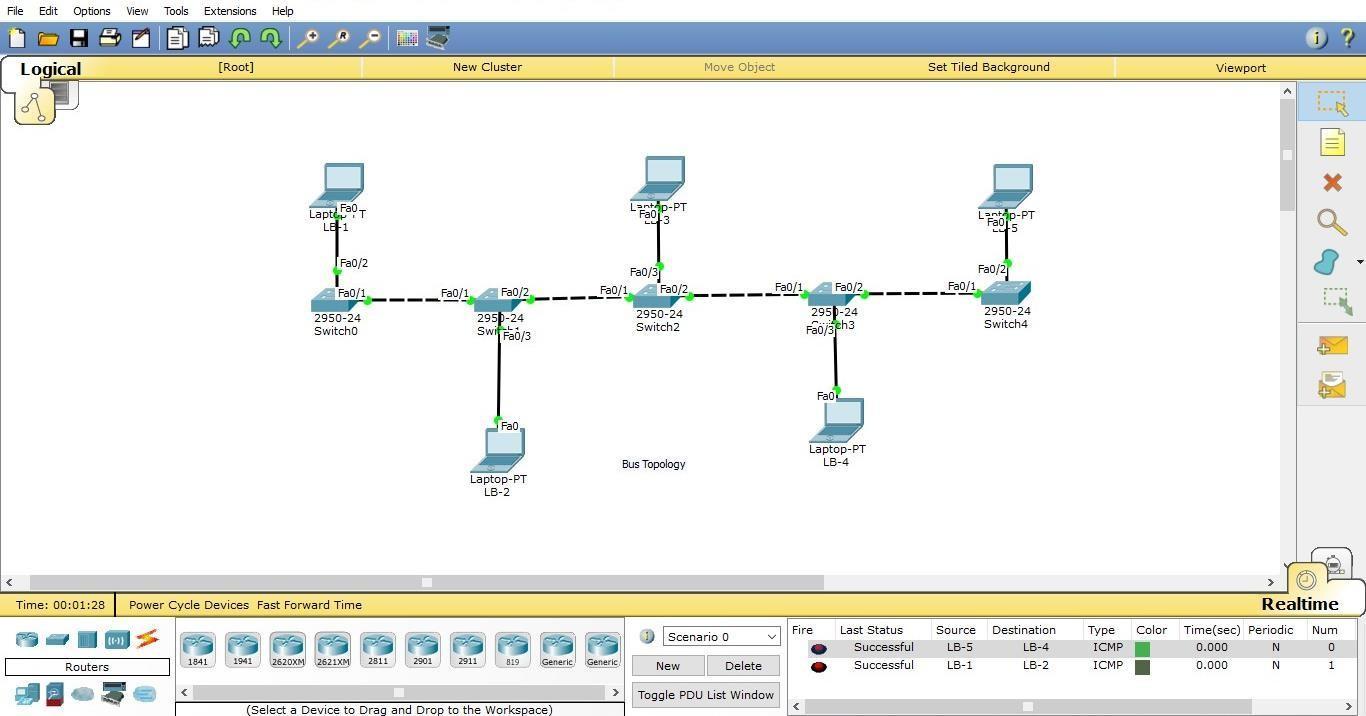
* Packet Tracer is Software or a protocol simulator developed by CISCO.
* Cisco Packet Tracer is a very powerful tool that displays various network and protocol simulation in real-time scenario and simulation mode.
* It gives the ability to design and analyze different types of real-time topologies and configure them as we do in the real world. In CISCO packet Tracer all the layer protocols are enabled or present, for example, Layer II Protocol such as Ethernet and PPP etc., Layer III Protocol such as IP (Internet Protocol), ICMP, (Internet Control Message Protocol), ARP (Address Resolution Protocol) etc., Layer IV Protocol such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
* Packet Tracer supports all the real-time routing protocols such as Static Routing, Default Routing, RIPv1, RIPv2, EIGRP, OSPF, BGP etc. Cisco Packet Tracer provides the real- time network equipment with the packet tracer for working and provides the simulation window for virtual simulation.

### Workspace of Cisco Packet Tracer:

* The workspace is the place where all the components (routers, switches, end devices, firewall, servers etc.) are placed and wired together to send and receive the packets.
* Workspace of Cisco Packet Tracer workspace is very much flexible from the user point of view as it is a drag-and-drop workspace through which they can drag-and-drop the components and starts configuring it beforehand using the built-in bash command window which actually simulates the bash window of the real router.

**Topologies:** Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.

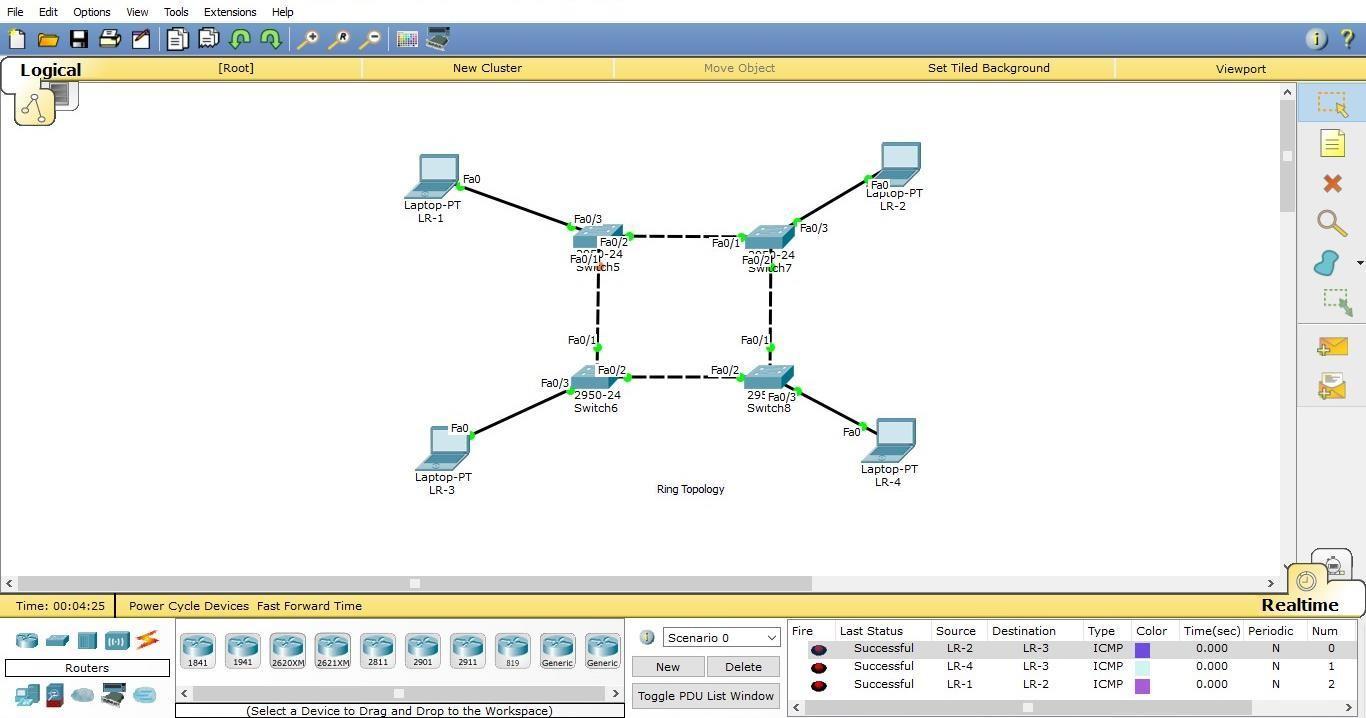
**Bus topology**: The bus topology is also called line topology. All devices in this topology are connected through a single backbone connection. The application of bus topology can be seen in computer labs. When the backbone is damaged or destroyed ,the whole system is destroyed.



**Steps:**

1. Open the CISCO PACKET TRACER software.
2. Drag N different PC’s from end components and place it in the workspace.
3. Assign the different and unique IP address to each PC.
4. Select N switches and connect it to each PC through copper straight through wire to fast ethernet ports.
5. Connect each consecutive switch with each other with copper cross over wire to fast ethernet ports.

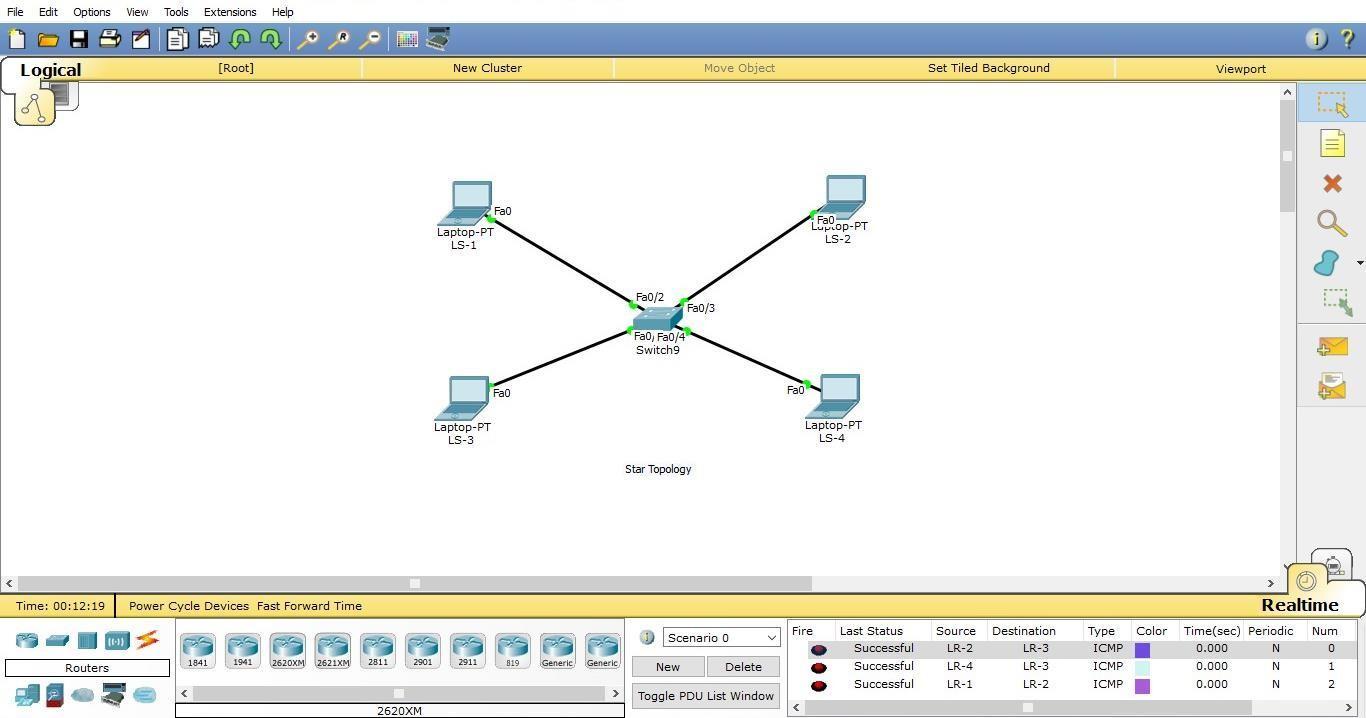
**Ring topology:** The ring topology creates a pattern like a circle. All devices in a network are similar to a point on a circle where each point is connected to two other consecutive points. Similarly, in ring topology the devices are connected in a circular path.



### Steps:

1. Open the CISCO PACKET TRACER software.
2. Drag N different PC’s from end components and place it in the workspace.
3. Assign the different and unique IP address to each PC.
4. Drag N switches and connect it with each PC using copper straight through wire to the fast ethernet ports.
5. Connect each switch with its adjacent two switches using copper cross over wire through fast ethernet ports.

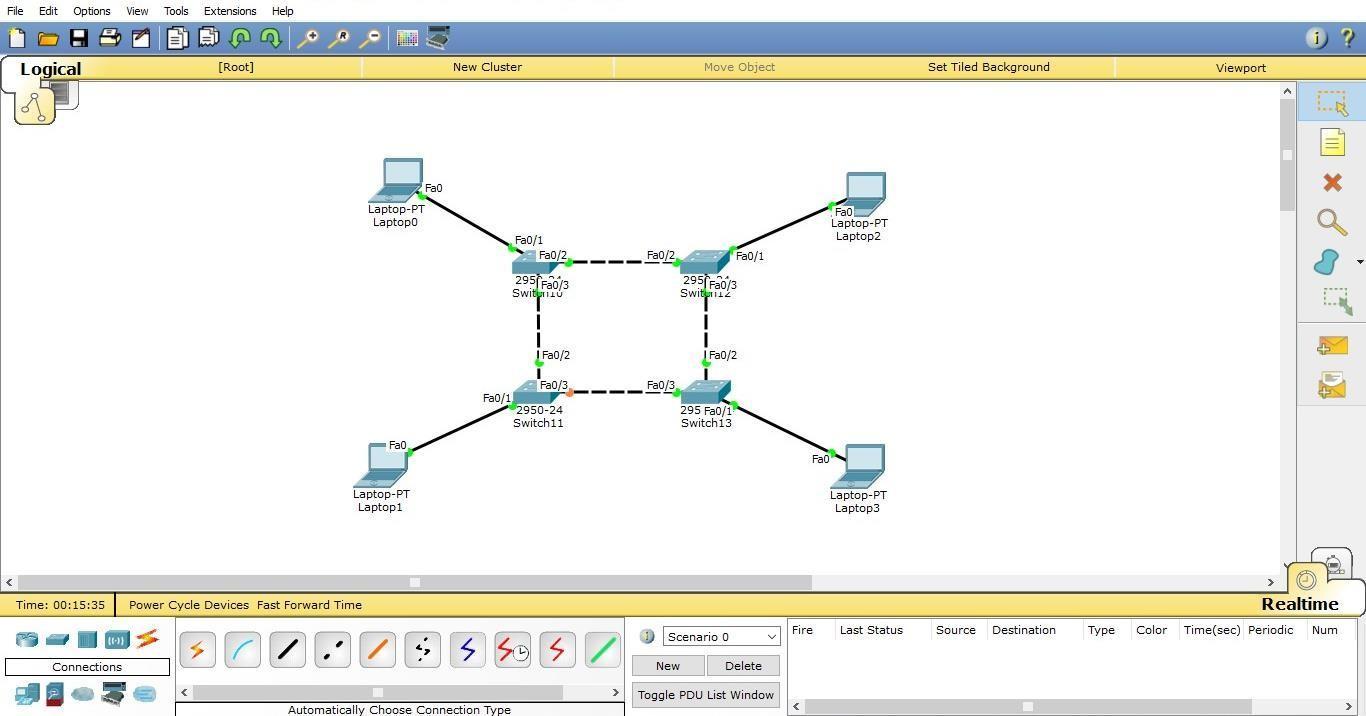
**Star topology:** Star topology is the best example of the LAN network. Where each and every node is connected to only the central switch or hub. There is no direct communication within two devices without using the central node as medium.



### Steps:

1. Open the CISCO PACKET TRACER software.
2. Drag N different PC’s from end components and place it in the workspace.
3. Assign the different and unique IP address to each PC.
4. Drag a switch and place it in the middle of all devices and connect all devices to the switch using copper straight through wire by the fast ethernet ports.

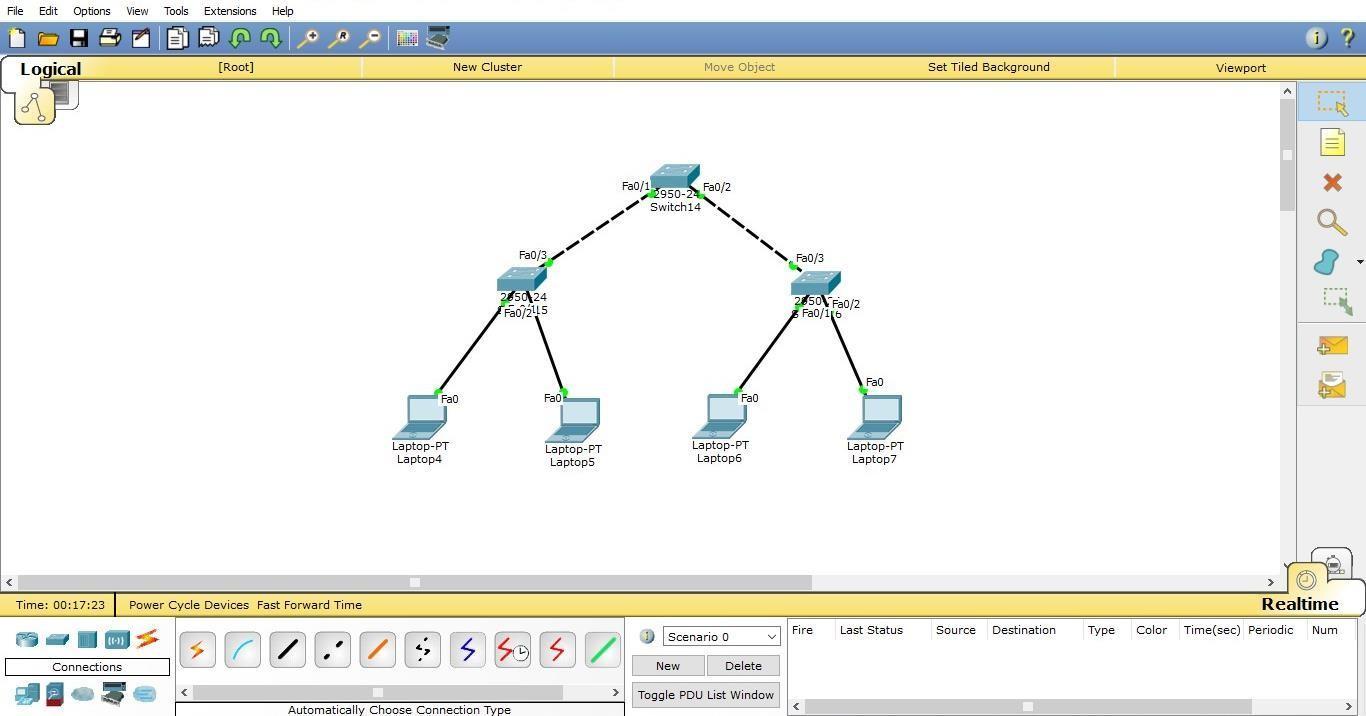
**Mesh topology:** A mesh network doesn’t follow any linear or hierarchical manner because one node is connected to all other nodes in that network. In a mesh network all PC’s communicate with each other through the unique communication path.



### Steps:

1. Open the CISCO PACKET TRACER software.
2. Drag N different PC’s from end components and place it in the workspace.
3. Assign the different and unique IP address to each PC.
4. Drag N switches and connect it to each PC using copper straight through wire by fast ethernet ports.
5. Connect each switch with every other switch of the network using copper cross over wire by the fast ethernet ports.

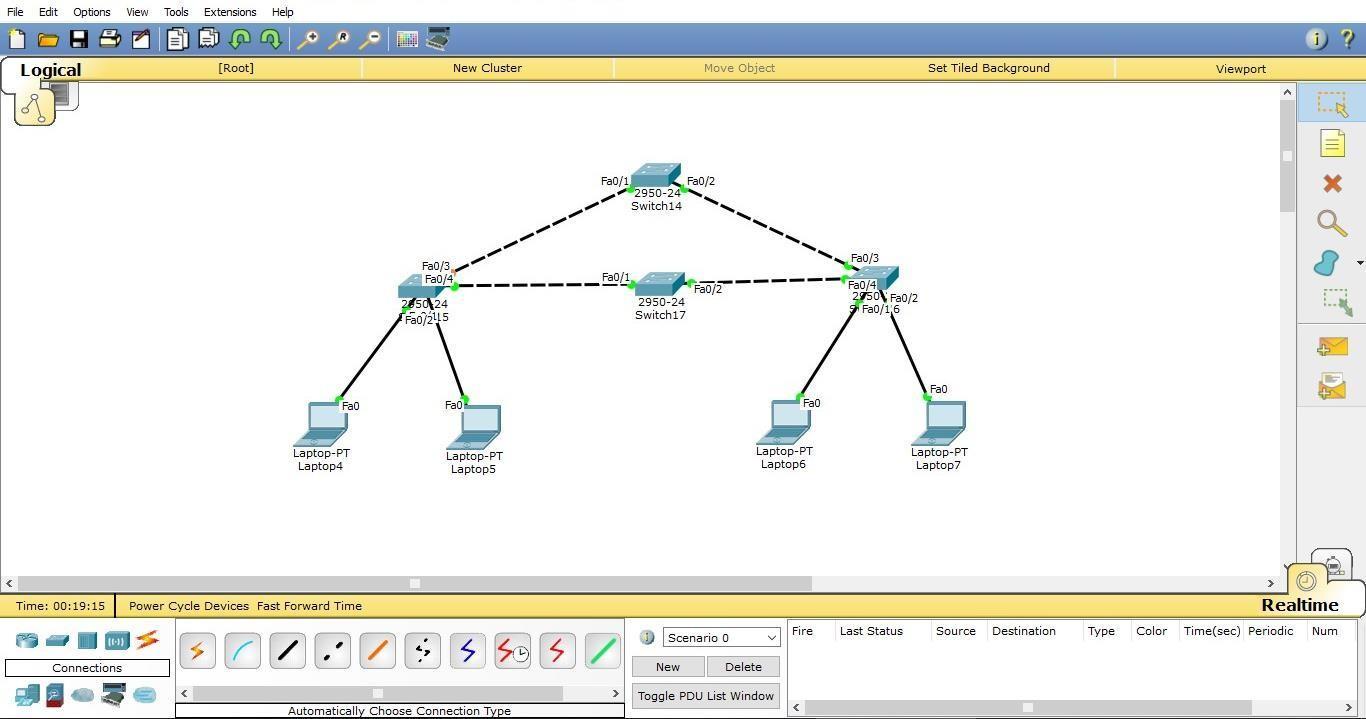
**Tree topology:** Tree topology is a different concept from other topologies like bus, tree, star, etc. It works in the hierarchical manner instead of linear manner. The tree topology network seems to be a tree and its different branches.



### Steps:

1. Open the CISCO PACKET TRACER software.
2. Drag N different PC’s from end components and place it in the workspace.
3. Assign the different and unique IP address to each PC.
4. Drag N switches connect each switch with a pc and connect it to two or more switches in a hierarchical manner.

**Hybrid topology:** A hybrid topology refers to the network which uses two or more than two topologies together in a single network



### Steps:

1. Open the CISCO PACKET TRACER software.
2. Drag N different PC’s from end components and place it in the workspace.
3. Assign the different and unique IP address to each PC.
4. Make two or more topologies and then connect them together into a single network by connecting switches of different topologies using copper cross over wire.

**CONCLUSION: In conclusion, Cisco Packet Tracer is an invaluable simulation tool for learning and experimenting with networking concepts. It allows users to design, configure, and troubleshoot various network setups without needing physical hardware. By offering a wide range of devices and protocols, it enables hands-on practice with essential networking tasks such as VLANs, routing, NAT, DHCP, and security configurations. Overall, it serves as an effective, cost-efficient learning platform for both beginners and professionals to develop their networking skills.**

**Practical: 2**

**Aim: Experiment of Packet Capture Tool: Wireshark.**

## WHAT IS WIRESHARK?

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

## USES OF WIRESHARK:

### Wireshark can be used in the following ways:

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

## HISTORY OF WIRESHARK:

In the late 1990's Gerald Combs, a computer science graduate of the University of Missouri-Kansas City was working for the small ISP (Internet Service Provider). The protocol at that time did not complete the primary requirements. So, he started writing ethereal and released the first version around 1998. The Network integration services owned the Ethernet trademark.

## FUNCTIONALITY OF WIRESHARK:

Wireshark is similar to TCP dump in networking. Tcpdump is a common packet analyzer which allows the user to display other packets and TCP/IP packets, being transmitted and received over a network attached to the computer. It has a graphic end and some sorting and filtering functions. Wireshark users can see all the traffic passing through the network. Wireshark can also monitor the unicast traffic which is not sent to the network's MAC address interface. But the switch does not pass all the traffic to the port. Hence, the promiscuous mode is not sufficient to see all the traffic. The various network taps or port mirroring is used to extend capture at any point. Port mirroring is a method to monitor network traffic. When it is enabled, the switch sends the copies of all the network packets present at one port to another port.

## WHAT IS COLOR CODING IN WIRESHARK?

The packets in the Wireshark are highlighted with blue, black, and green colour These colours help users to identify the types of traffic. It is also called packet colorization. The kinds of colouring rules in the Wireshark are temporary rules and permanent rules.

The temporary rules are there until the program is in active mode or until we quit the program. The permanent color rules are available until the Wireshark is in use or the next time you run the Wireshark. The steps to apply color filters will be discussed later in this topic.

## FEATURES OF WIRESHARK:

* + It is multi-platform software, i.e., it can run on Linux, Windows, OS X, FreeBSD, NetBSD, etc.
  + It is a standard three-pane packet browser.
  + It performs deep inspection of hundreds of protocols.
  + It often involves live analysis, i.e., from the different types of the network like the Ethernet, loopback, etc., we can read live data.
  + It has sort and filter options which makes it easy for the user to view the data. It is also useful in VoIP analysis.
  + It can also capture raw USB traffic.

Various settings, like timers and filters, can be used to filter the output.

* + It can only capture packets on the PCAP (an application programming interface used to capture the network) supported networks.
  + Wireshark supports a variety of well-documented capture file formats such as the PcapNg and Libpcap. These formats are used for storing the captured data.
  + It is the no.1 piece of software for its purpose. It has countless applications ranging from the tracing down, unauthorized traffic, firewall settings, etc.

### INSTALLATION OF WIRESHARK SOFTWARE:

Below are the steps to install the Wireshark software on the computer: Open the web browser. Search for 'Download Wireshark.'

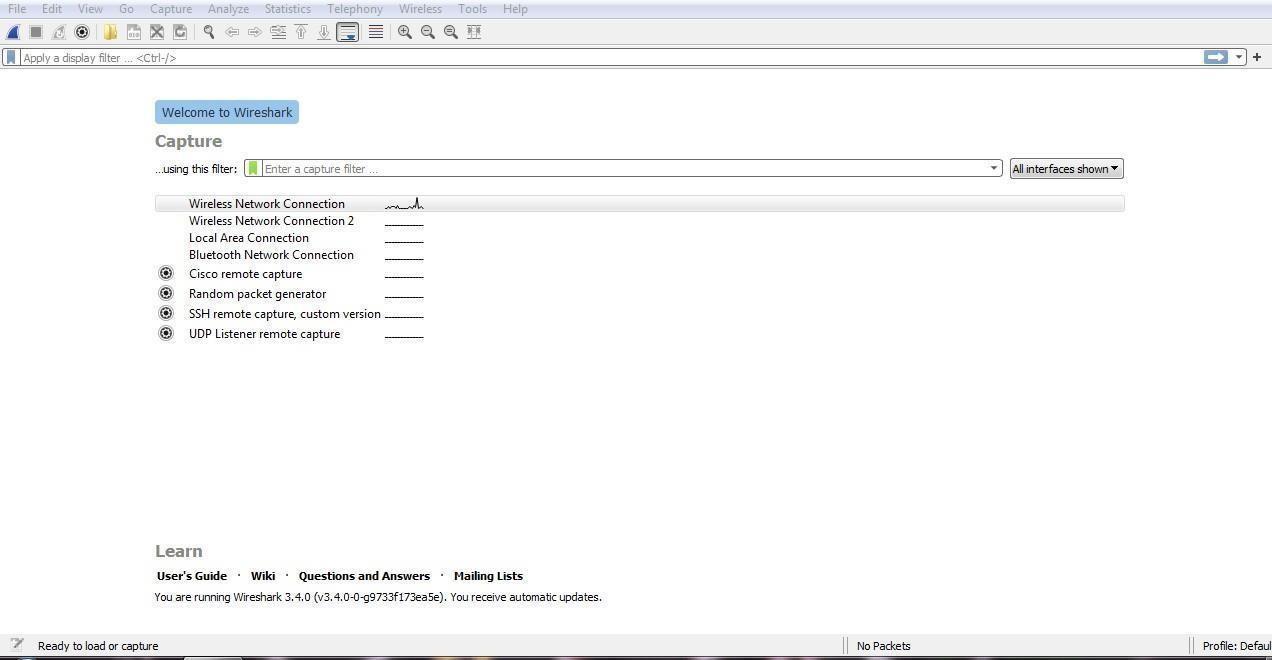
Select the Windows installer according to your system configuration, either 32-bt or 64-bit. Save the program and close the browser.

Now, open the software, and follow the install instruction by accepting the license. The Wireshark is ready for use.

On the network and Internet settings option, we can check the interface connected to our computer.

If you are Linux users, then you will find Wireshark in its package repositories.

By selecting the current interface, we can get the traffic traversing through that interface. The version used here is 3.0.3. This version will open as:



The screen/interface of the Wireshark is divided into five parts:

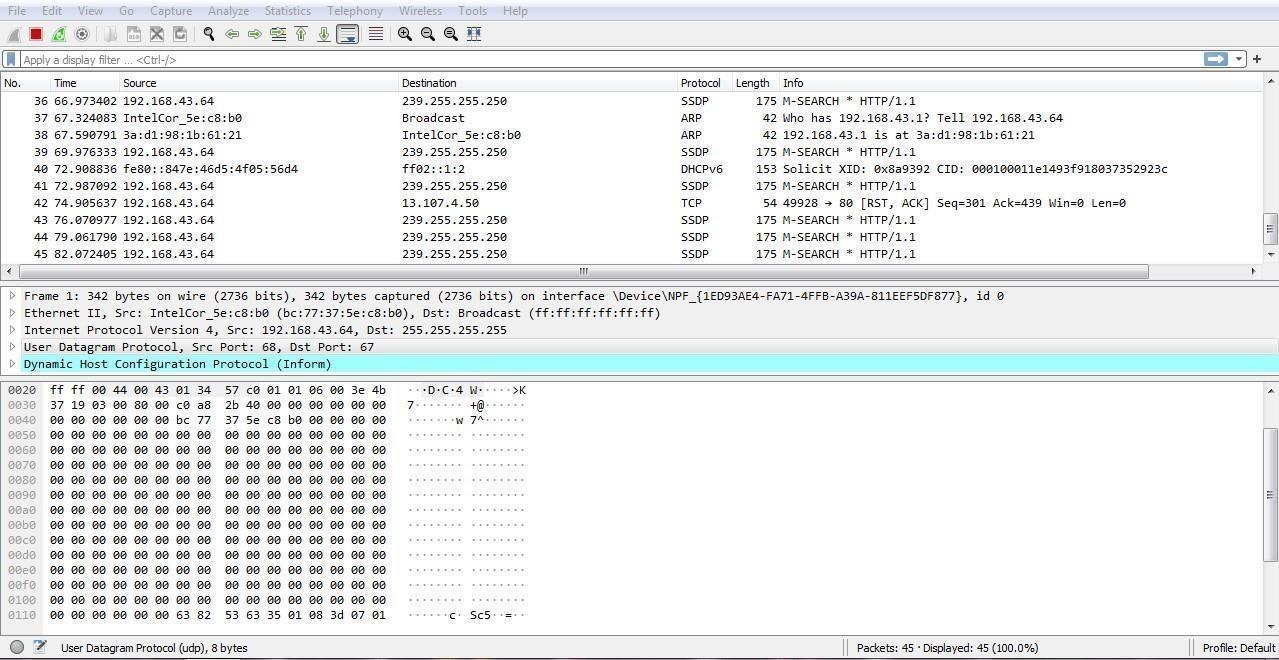
First part contains a menu bar and the options displayed below it. This part is at the top of the window. File and the capture menus options are commonly used in

Wireshark. The capture menu allows you to start the capturing process. And the File menu is used to open and save a capture file.

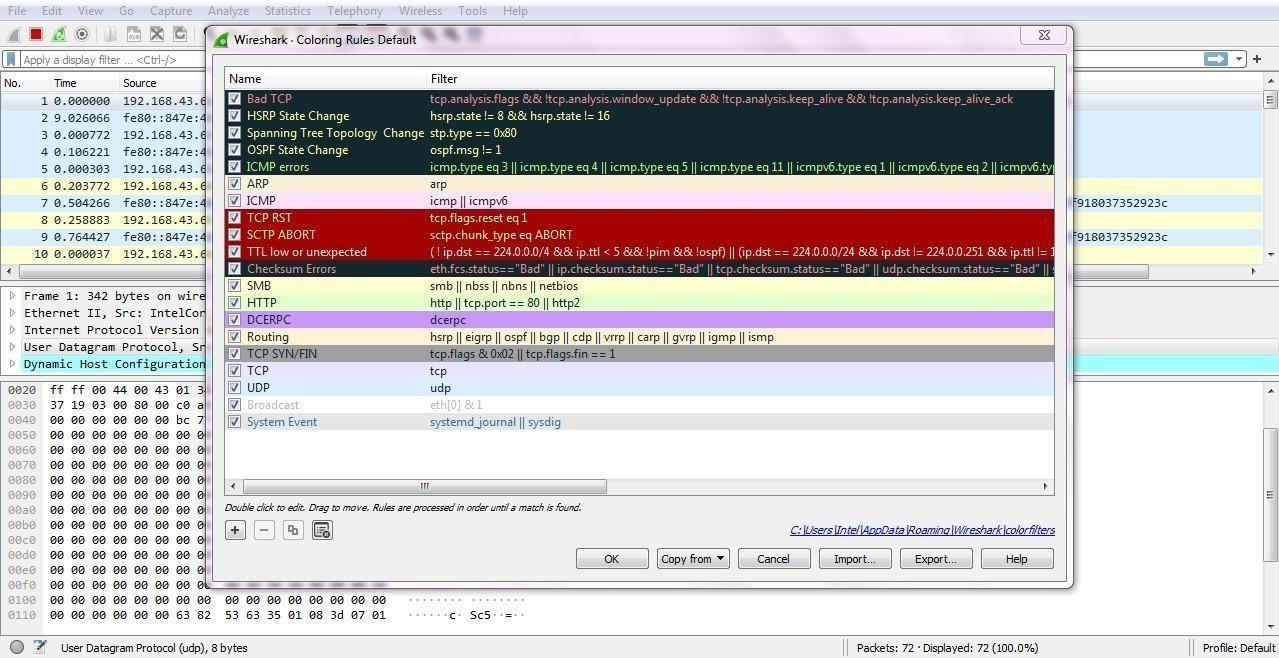
The second part is the packet listing window. It determines the packet flow or the captured packets in the traffic. It includes the packet number, time, source, destination, protocol, length, and info. We can sort the packet list by clicking on the column name. Next comes the packet header- detailed window. It contains detailed information about the components of the packets. The protocol info can also be expanded or minimized according to the information required.

The bottom window is called the packet contents window, which displays the content in ASCII and hexadecimal format.

At last, is the filter field which is at the top of the display. The captured packets on the screen can be filtered based on any component according to your requirements. For example, if we want to see only the packets with the HTTP protocol, we can apply filters to that option. All the packets with HTTP as the protocol will only be displayed on the screen, shown below:



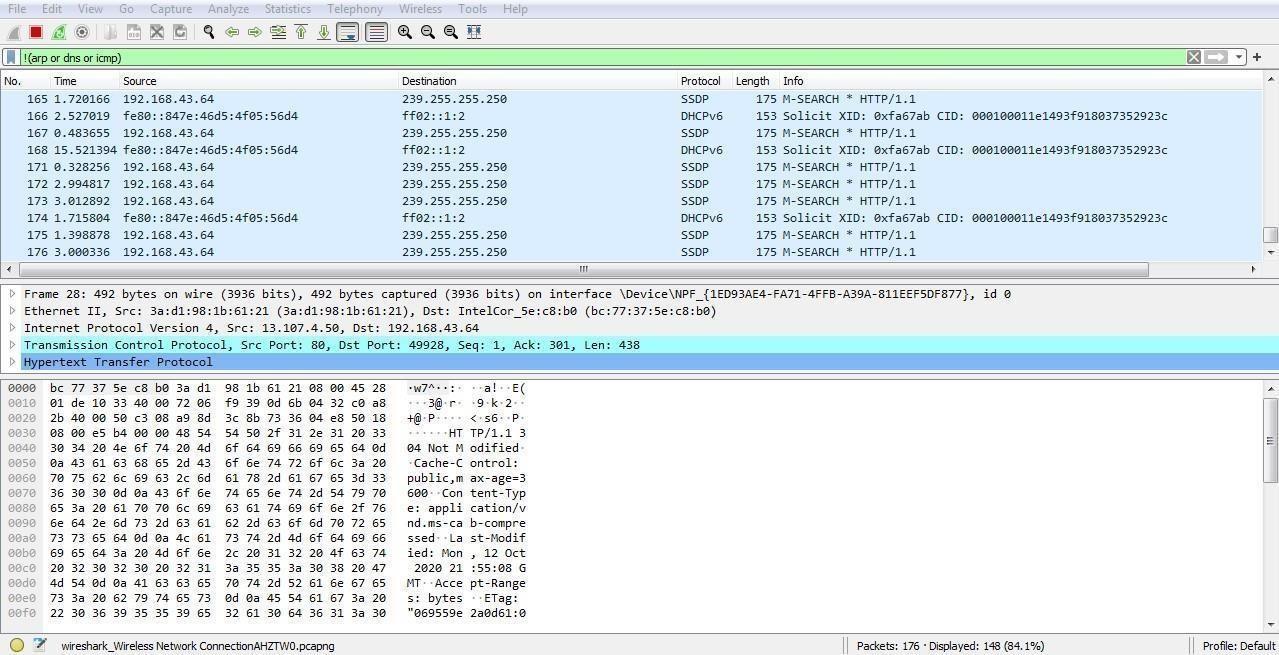
If you want to filter according to the source, right-click on the source you want to filter and select 'Apply as Filter' and choose '...and filter.' Steps for the permanent colorization are: click on the 'View' option on the menu bar and select 'Coloring Rules.' The table will appear like the image shown below:

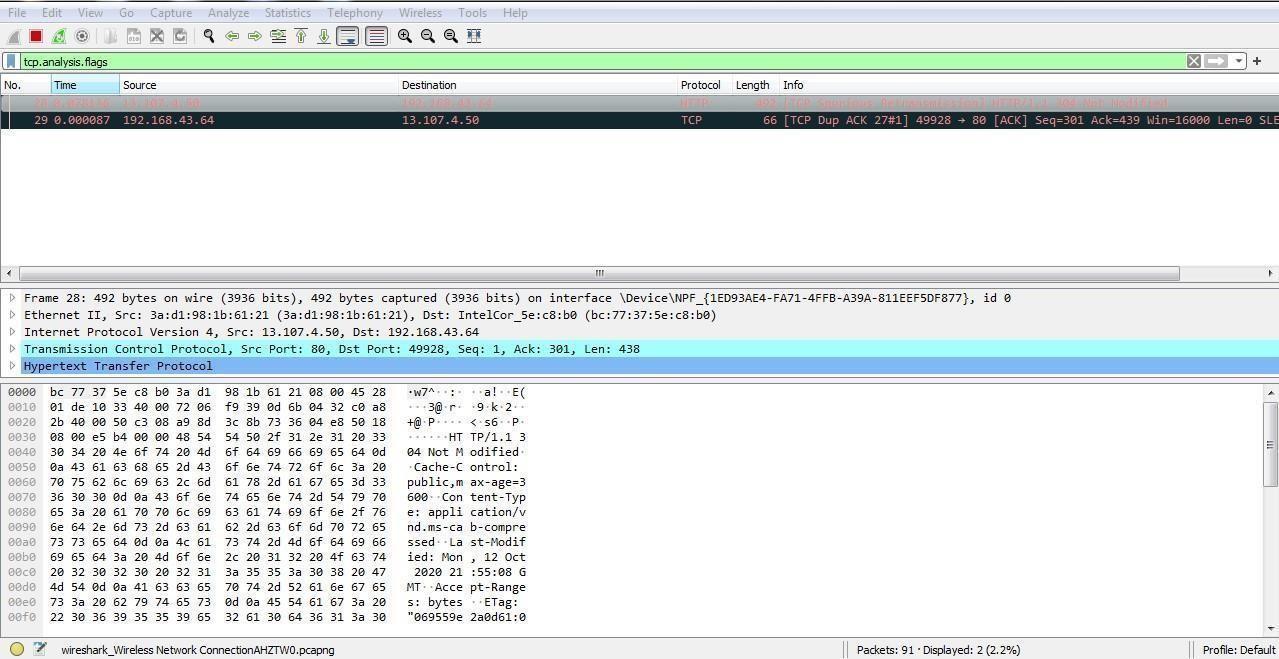


For the network administrator job, advanced knowledge of Wireshark is considered as the requirements. So, it is essential to understand the concepts of the software. It contains these 20 default coloring rules which can be added or removed according to the requirements. Select the option 'View' and then choose 'Colorize Packet List,' which is used to toggle the color on and off.

## MOST USED FILTER IN WIRESHARK:

Whenever we type any commands in the filter command box, it turns green if your command is correct. It turns red if it is incorrect or the Wireshark does not recognize your command.





**CONCLUSION:**

Wireshark is a powerful tool for capturing and analyzing network traffic. Through experiments like inspecting protocols (HTTP, DNS, TCP, etc.) and monitoring traffic patterns, it helps users understand network behavior, troubleshoot issues, and identify security threats effectively. It’s invaluable for both learning and professional network analysis.

**Practical: 3**

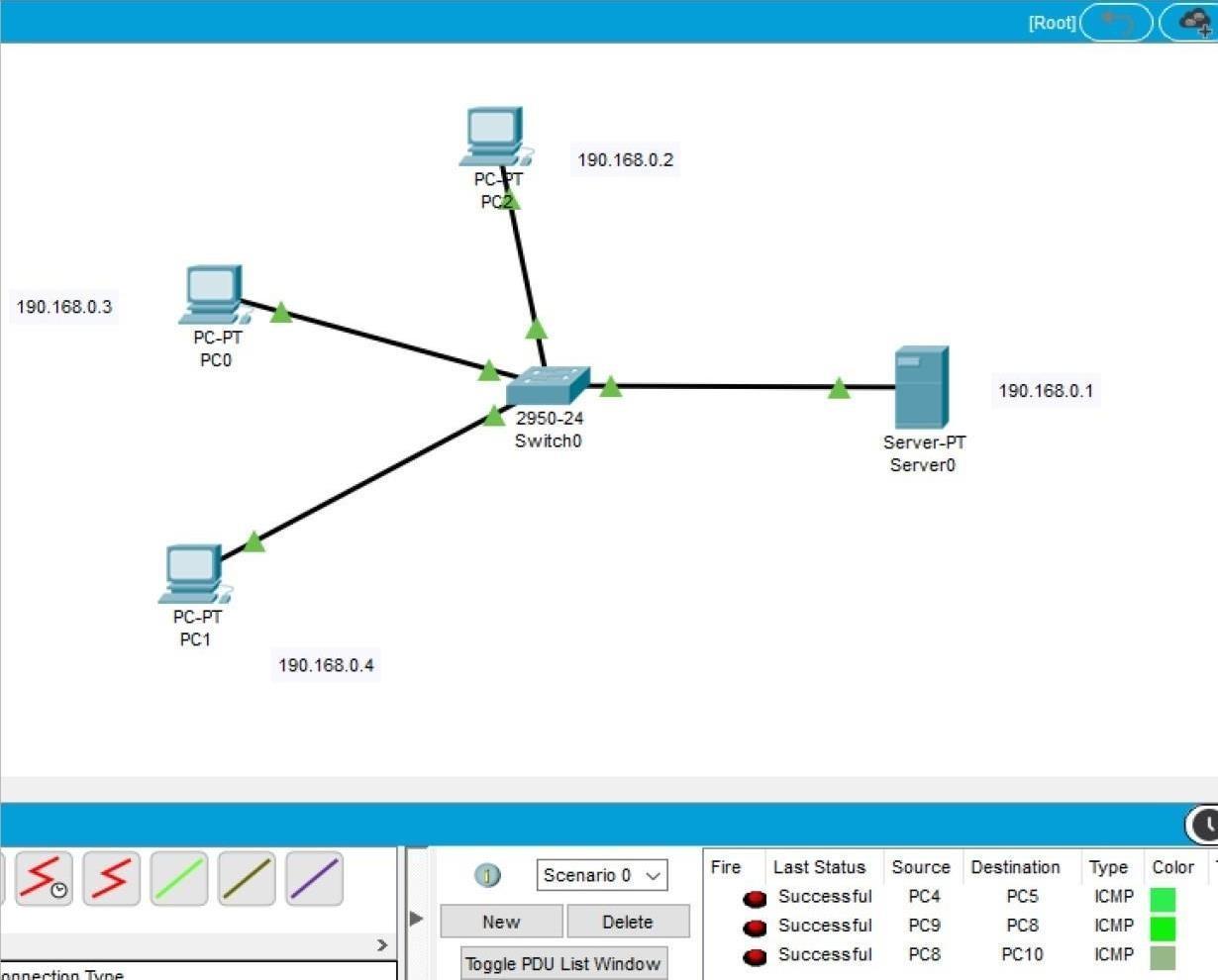
## Aim: To study behaviour of generic devices used for networking: (cisco packet tracer).

**THEORY:**

In this Practical we are going to learn the generic devices of Computer Networking.

## WEB SERVER:

A server is a computer connected to a network of other workstations called 'clients'. Client computers request information from the server over the network. Servers tend to have more storage, memory and processing power than a normal workstation.



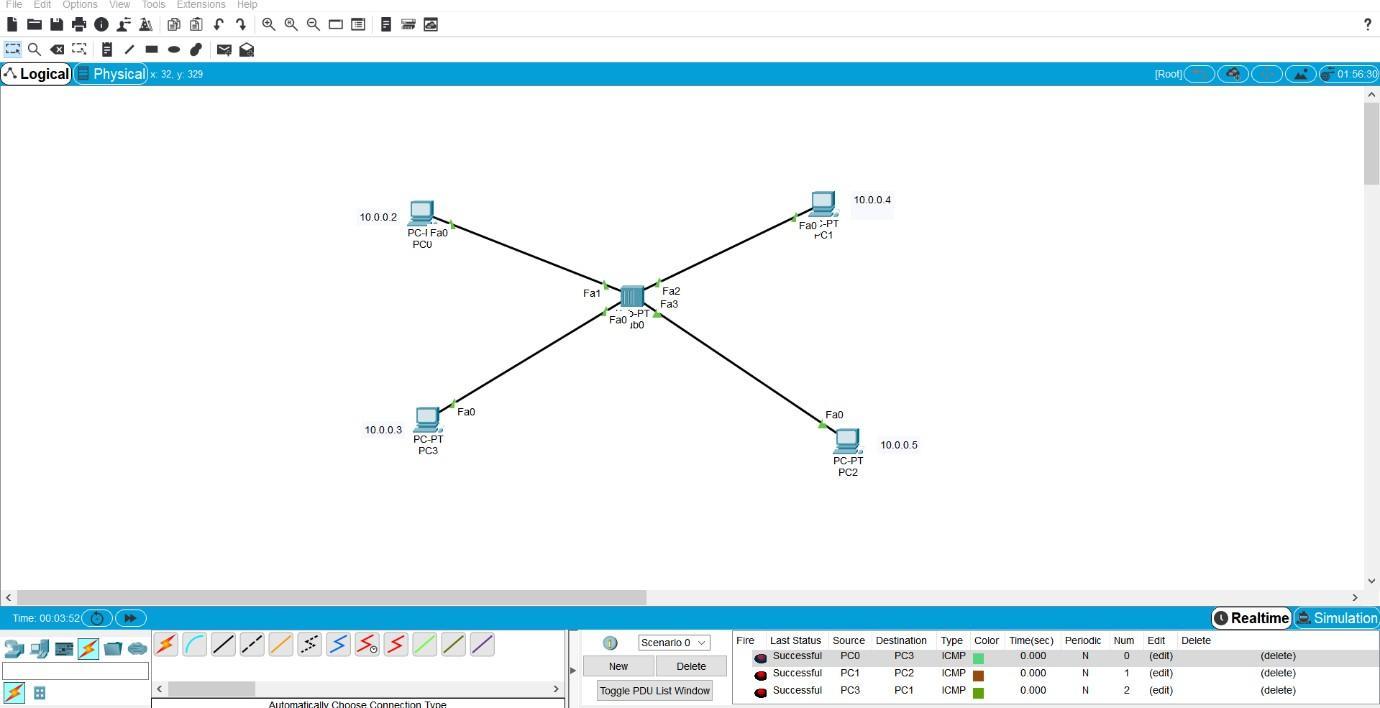
### USES:

A server is a computer connected to a network of other workstations called ‘clients. Client computers request information from the server over the network. Servers tend to have more

storage, memory and processing power than a normal workstation.

## 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. A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports.



### USES:

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. A computer which intends to be connected to the network is plugged in to one of these ports.

## ROUTERS:

A router receives and sends data on computer networks. Routers are sometimes confused with network hubs, modems, or network switches. However, routers can combine the functions of these components, and connect with these devices, to improve Internet access or help create business networks.

### USES:

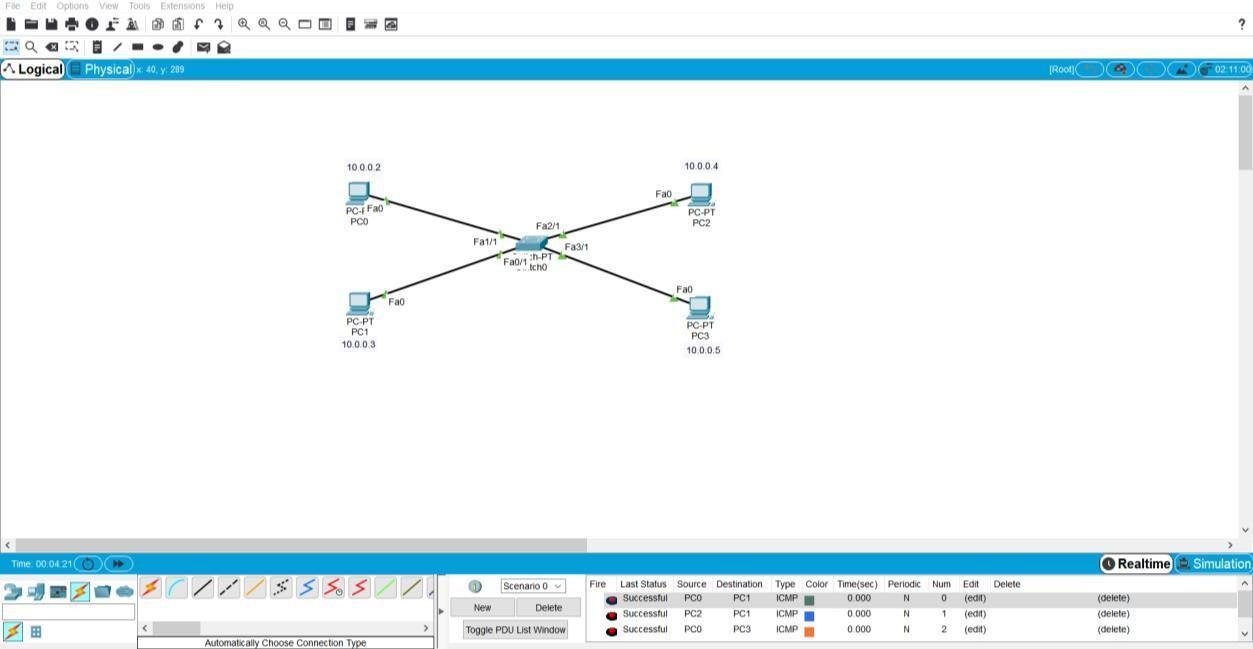
A router receives and sends data on computer networks. Routers are sometimes confused with network hubs, modems, or network switches. However, routers can combine the functions of these components, and connect with these devices, to improve Internet access or help create business networks.

## SWITCHES:

A switch is a device in a computer network that connects other devices together. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches may also operate at higher layers of the OSI model, including the network layer and above.

### USES:

Switches are key building blocks for any network. They connect multiple devices, such as computers, wireless access points, printers, and servers; on the same network within a building or campus. A switch enables connected devices to share information and talk to each other.



## BRIDGE:

A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network.

### USES:

A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments. Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network.

## SERVER:

A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, whenever computers share resources with client machines, they are considered servers.

## WIRELESS DEVICES:

Devices such as computers, tablets, and phones are common Clients on a network. Access Points (Master) most wireless networks are made using Access Points – devices that host and control the wireless connection for laptops, tablets, or smart phones.

## LAPTOP:

A laptop computer, sometimes called a notebook computer by manufacturers, is a battery- or AC powered personal computer generally smaller than a briefcase that can easily be transported and conveniently used in temporary spaces such as on airplanes, in libraries, temporary offices, and at meetings.

## 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.

## Modem:

Modem is a device or program that enables a computer to transmit data over telephone or cable lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analogy waves.

## Host:

Host is a computer or other devices connected to a network. A host may work as a server offering information resources, services and application to users or other hosts.

## Repeater:

A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.

## Automatically chose connection:

lead to automatic connect and disconnect actions on Wi-Fi, in the Windows user interface but can be configured by using the at least one active Internet connection to a preferred type of network.

## Console:

The console is a connection over serial port connection that allows a person access to a computer or network device console. Usually, a console is accessed over an SSH connection.

## Copper straight-through:

Straight-through cable is a type of twisted pair copper wire cable for local area network (LAN) use for which the RJ-45 connectors at each end have the same pinout (i.e., arrangement of conductors).

## Copper Crossover:

A crossover cable is a type of twisted pair copper wire cable for LANs (local area network) in which the wires on the cable are crossed over so that the receive signal pins on the RJ-45 connector on one end are connected to the transmit signal pins on the RJ-45 connector on the other end.

## Fiber cable:

Fiber cables transmit pulses of light instead of electrical signals, so the terminations must be much more precise. Instead of merely allowing pins to make metal-to-metal contact, fiber optic connectors must align microscopic glass fiber perfectly in order to allow for communication.

## Phone:

Phone a standard specifies both the physical connector and how it is wired, when modulator connectors are used, the latch release of the connector should be on the ridge side of flat phone wire in order to maintain polarity.

1. **Coaxial cable: **

Coaxial cable is **used as** a transmission line for radio frequency signals, taking a round cross section of the cable, one would find a signal centre solid wire symmetrically surrounded by a foil conductor.

## Serial DCE data:

circuit training, data communications or data carrier equipment this is a modem or more generally adapter. It has to transmit the clock signal which controls the data rate.



## DTE

DTE stands for data terminal equipment which is generally a terminal or a computer. It is a device that acts as an information source or an information sink for the binary digital data.

## Octal:

Octal is a term that describes a base 8 number system. It consists of eight single digit numbers:0,1,2,3,4,5,6 and 7. It can connect and access server to several different Cisco devices so that it can configure without plugging and unplugging.

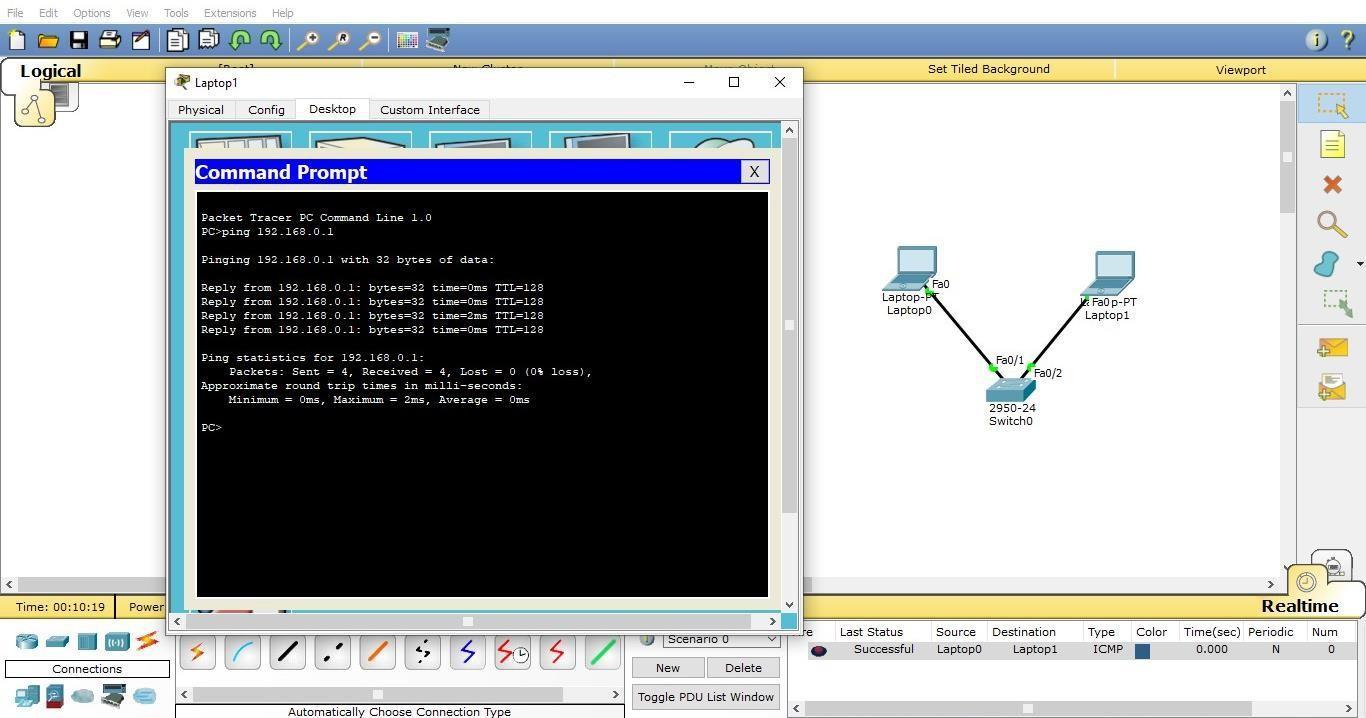
## USB:

USB is an industry standard that establishes specifications for cables and connectors and protocols for connection, communication and power supply between computers, peripheral devices and other computers.

### PC to PC Connection: Steps:

* + Drag 2 PC’s from end components.
  + Assign a unique IP address to each PC.
  + Drag a switch and connect 2 PC with a switch using copper straight through cable by fast ethernet ports.





CONCLUSION:

Cisco Packet Tracer is a versatile tool for simulating and studying the behavior of networking devices like routers, switches, and end devices. It helps learners understand network design, configuration, and troubleshooting in a risk-free virtual environment. By experimenting with various topologies and protocols, users gain practical insights into real-world networking scenarios.

**Practical: 4**

**Aim**: **To Perform the Data Link Layer (Error Detection) Hamming Code:** Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver. It is technique developed by R.W. Hamming for error correction.

## Redundant bits :

Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer. The number of redundant bits can be calculated using the following formula:

2^r ≥ m + r + 1

where, r = redundant bit, m = data bit

Suppose the number of data bits is 7, then the number of redundant bits can be calculated using:

= 2^4 ≥ 7 + 4 + 1

Thus, the number of redundant bits= 4

## Parity bits:

A parity bit is a bit appended to a data of binary bits to ensure that the total number of 1’s in the data is even or odd. Parity bits are used for error detection. There are two types of parity bits:

### Even parity bit:

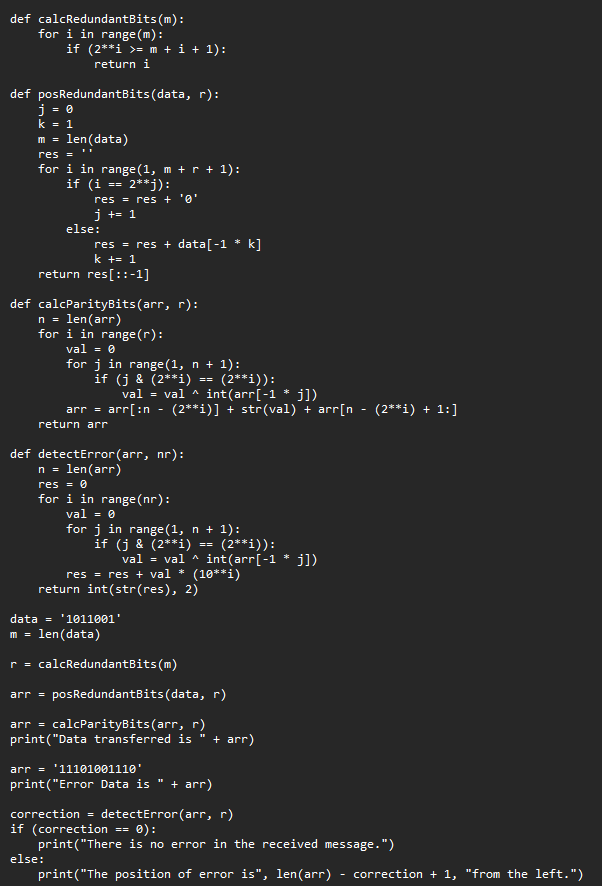
In the case of even parity, for a given set of bits, the number of 1’s are counted. If that count is odd, the parity bit value is set to 1, making the total count of occurrences of 1’s an even number. If the total number of 1’s in a given set of bits is already even, the parity bit’s value is 0.

### Odd Parity bit :

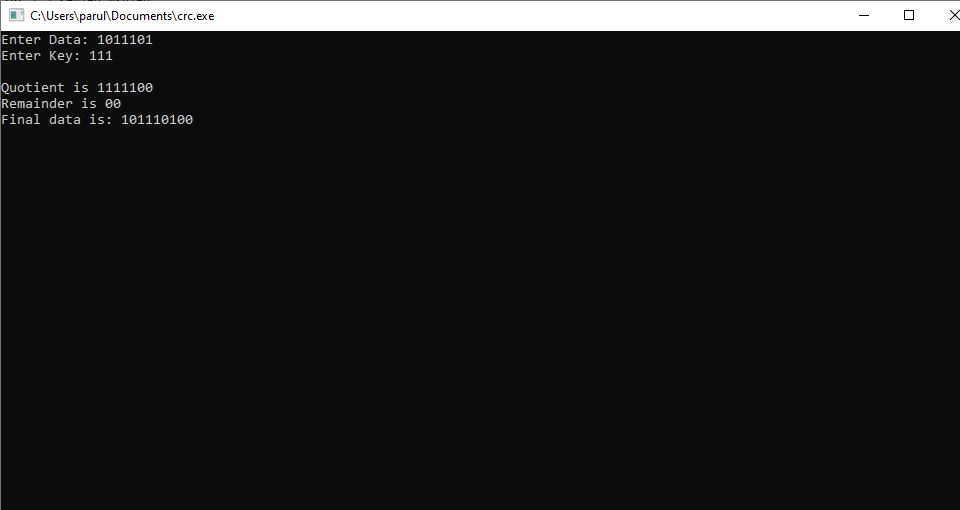
In the case of odd parity, for a given set of bits, the number of 1’s are counted. If that count is even, the parity bit value is set to 1, making the total count of occurrences of 1’s an odd number. If the total number of 1’s in a given set of bits is already odd, the parity bit’s value is 0.

### General Algorithm of Hamming code :

The Hamming Code is simply the use of extra parity bits to allow the identification of an error.

1. Write the bit positions starting from 1 in binary form (1, 10, 11, 100, etc).
2. All the bit positions that are a power of 2 are marked as parity bits (1, 2, 4, 8, etc).
3. All the other bit positions are marked as data bits.
4. Each data bit is included in a unique set of parity bits, as determined its bit position in binary form.
   1. Parity bit 1 covers all the bits positions whose binary representation includes a 1 in the least significant position (1, 3, 5, 7, 9, 11, etc).
   2. Parity bit 2 covers all the bits positions whose binary representation includes a 1 in the second position from the least significant bit (2, 3, 6, 7, 10, 11, etc).
   3. Parity bit 4 covers all the bits positions whose binary representation includes a 1 in the third position from the least significant bit (4–7, 12–15, 20–23, etc).
   4. Parity bit 8 covers all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit bits (8–15, 24–31, 40–47, etc).
   5. In general, each parity bit covers all bits where the bitwise AND of the parity position and the bit position is non-zero.
5. Since we check for even parity set a parity bit to 1 if the total number of ones in the positions it checks is odd.
6. Set a parity bit to 0 if the total number of ones in the positions it checks is even.****

**Output: -**



CONCLUSION:

The Data Link Layer ensures reliable communication by detecting and correcting errors in data frames using techniques like ARQ and FEC. These methods enhance data integrity and network reliability, ensuring smooth and error-free transmission.

**Practical: 5**

**Aim: Virtual LAN. DESCRIPTION:**

* A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).
* LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic.
* VLANs work by applying tags to network frames and handling these tags in networking systems – creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks.
* In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.
* VLANs allow network administrators to group hosts together even if the hosts are not directly connected to the same network switch. Because VLAN membership can be configured through software, this can greatly simplify network design and deployment. Without VLANs, grouping hosts according to their resource needs the labor of relocating nodes or rewiring data links
* VLANs allow networks and devices that must be kept separate to share the same physical cabling without interacting, improving simplicity, security, traffic management, or economy.
* For example, a VLAN could be used to separate traffic within a business due to users, and due to network administrators, or between types of traffic, so that users or low priority traffic cannot directly affect the rest of the network's functioning. Many Internet hosting services use VLANs to separate their customers' private zones from each other, allowing each customer's servers to be grouped together in a single network segment while being located anywhere in their data center. Some precautions are needed to prevent traffic "escaping" from a given VLAN, an exploit known as VLAN hopping.
* VLANs address issues such as [scalability,](https://en.wikipedia.org/wiki/Scalability) security, and network management. Network architects set up VLANs to provide [network segmentation](https://en.wikipedia.org/wiki/Network_segmentation). Routers between VLANs

filter [broadcast traffic,](https://en.wikipedia.org/wiki/Broadcasting_(networking)) enhance [network security,](https://en.wikipedia.org/wiki/Network_security) perform [address summarization](https://en.wikipedia.org/wiki/Supernetwork), and mitigate [network congestion](https://en.wikipedia.org/wiki/Network_congestion).

* In a network utilizing broadcasts for [service discovery](https://en.wikipedia.org/wiki/Service_discovery), address [assignment](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol) and [resolution](https://en.wikipedia.org/wiki/Address_Resolution_Protocol) and other services, as the number of peers on a network grows, the frequency of broadcasts also increases. VLANs can help manage broadcast traffic by forming multiple [broadcast domains.](https://en.wikipedia.org/wiki/Broadcast_domain) Breaking up a large network into smaller independent segments reduces the amount of broadcast traffic each network device and network segment has to bear. Switches may not bridge network traffic between VLANs, as doing so would violate the integrity of the VLAN broadcast domain.
* VLANs can also help create multiple [layer 3](https://en.wikipedia.org/wiki/Layer_3) networks on a single physical infrastructure. VLANs are [data link layer](https://en.wikipedia.org/wiki/Data_link_layer) (OSI layer 2) constructs, analogous to [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP) [subnets,](https://en.wikipedia.org/wiki/Subnetwork) which are [network layer](https://en.wikipedia.org/wiki/Network_layer) (OSI layer 3) constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, although it is possible to have multiple subnets on one VLAN.
* Without VLAN capability, users are assigned to networks based on geography and are limited by physical topologies and distances. VLANs can logically group networks to decouple the users' network location from their physical location. By using VLANs, one can control traffic patterns and react quickly to employee or equipment relocations. VLANs provide the flexibility to adapt to changes in network requirements and allow for simplified administration.[[2]](https://en.wikipedia.org/wiki/Virtual_LAN#cite_note-802.1Q_1.4-2)
* VLANs can be used to partition a local network into several distinctive segments, for instance.

**Cisco VLAN Trucking Protocol**

* VLAN Trucking Protocol (VTP) is a Cisco proprietary protocol that propagates the definition of VLANs on the whole local area network. VTP is available on most of the [Cisco Catalyst](https://en.wikipedia.org/wiki/Cisco_Catalyst) Family products. The comparable IEEE standard in use by other manufacturers is [GARP VLAN Registration Protocol](https://en.wikipedia.org/wiki/GARP_VLAN_Registration_Protocol) (GVRP) or the more recent [Multiple VLAN Registration Protocol](https://en.wikipedia.org/wiki/Multiple_VLAN_Registration_Protocol) (MVRP).
* The two common approaches to assigning VLAN membership are as follows:
* Static VLANs
* Dynamic VLANs
* Static VLANs are also referred to as port-based VLANs. Static VLAN assignments are created by assigning ports to a VLAN. As a device enters the network, the device automatically assumes the VLAN of the port. If the user changes ports and needs access to the same VLAN, the network administrator must manually make a port-to-VLAN assignment for the new connection.
* Dynamic VLANs are created using software or by protocol. With a [VLAN Management Policy Server](https://en.wikipedia.org/wiki/VLAN_Management_Policy_Server) (VMPS), an administrator can assign switch ports to VLANs dynamically based on information such as the source MAC address of the device connected to the port or the username used to log onto that device. As a device enters the network, the switch queries a database for the VLAN membership of the port that device is connected to. Protocol methods include [Multiple VLAN Registration Protocol](https://en.wikipedia.org/wiki/Multiple_Registration_Protocol#Multiple_VLAN_Registration_Protocol) (MVRP) and the somewhat obsolete [GARP VLAN Registration Protocol](https://en.wikipedia.org/wiki/Multiple_Registration_Protocol#History) (GVRP).
* In a switch that supports protocol-based VLANs, traffic is handled on the basis of its protocol. Essentially, this segregates or forwards traffic from a port depending on the particular protocol of that traffic; traffic of any other protocol is not forwarded on the port.
* For example, it is possible to connect the following to a given switch:
* A host generating Address Resolution Protocol (ARP) traffic to port 10
* A network with Internetwork Packet Exchange (IPX) traffic to port 20

## Make a Network:

We took router, switch, PC’s.

We have 1 router, 1 switch, 3 PC’s: PC0, PC1, PC2. Router address: gig 0/0.10 VLAN 10

Ip Address :192.168.10.1/24

gig 0/0.20 VLAN 20

Ip Address:192.168.20.1/24

gig 0/0.30 VLAN 30

Ip Address:192.168.30.1/24 PC0 Address: VLAN 10

192.168.10.2/24

192.168.10.1

PC1 Address: VLAN 20

192.168.10.2/24

192.168.10.1

PC2 Address: VLAN 30

192.168.30.2/24

192.168.30.1

## configure VLAN to switch:

1. switch>enable
2. switch# configure terminal
3. switch(config)# interface gigabitethernet 0/1
4. switch(config-if)# switchport access vlan 10
5. switch(config-if)# switchport mode trunk 6.switch(config-if)# no shutdown
6. switch(config-if)# exit
7. switch(config)# Interface FastEthernet0/1
8. switch(config-if)# switchport access vlan 10
9. switch(config-if)# switchport mode access 11.switch(config-if)# no shutdown 12.switch(config-if)# exit
10. switch(config)# Interface FastEthernet0/2
11. switch(config-if)# switchport access vlan 20
12. switch(config-if)# switchport mode access
13. switch(config-if)# no shutdown
14. switch(config-if)# exit
15. switch(config)# Interface FastEthernet0/3
16. switch(config-if)# switchport access vlan 30
17. switch(config-if)# switchport mode access 21.switch(config-if)# no shutdown

22. switch(config-if)# exit

## 3. configure Switch to Router:

1. router>enable
2. router# configure terminal
3. router(config)# interface gigabitethernet 0/0.10
4. router(config-if)# encapsulation dot1Q 10

5. router(config-if)# ip address 192.168.10.1 255.255.255.0

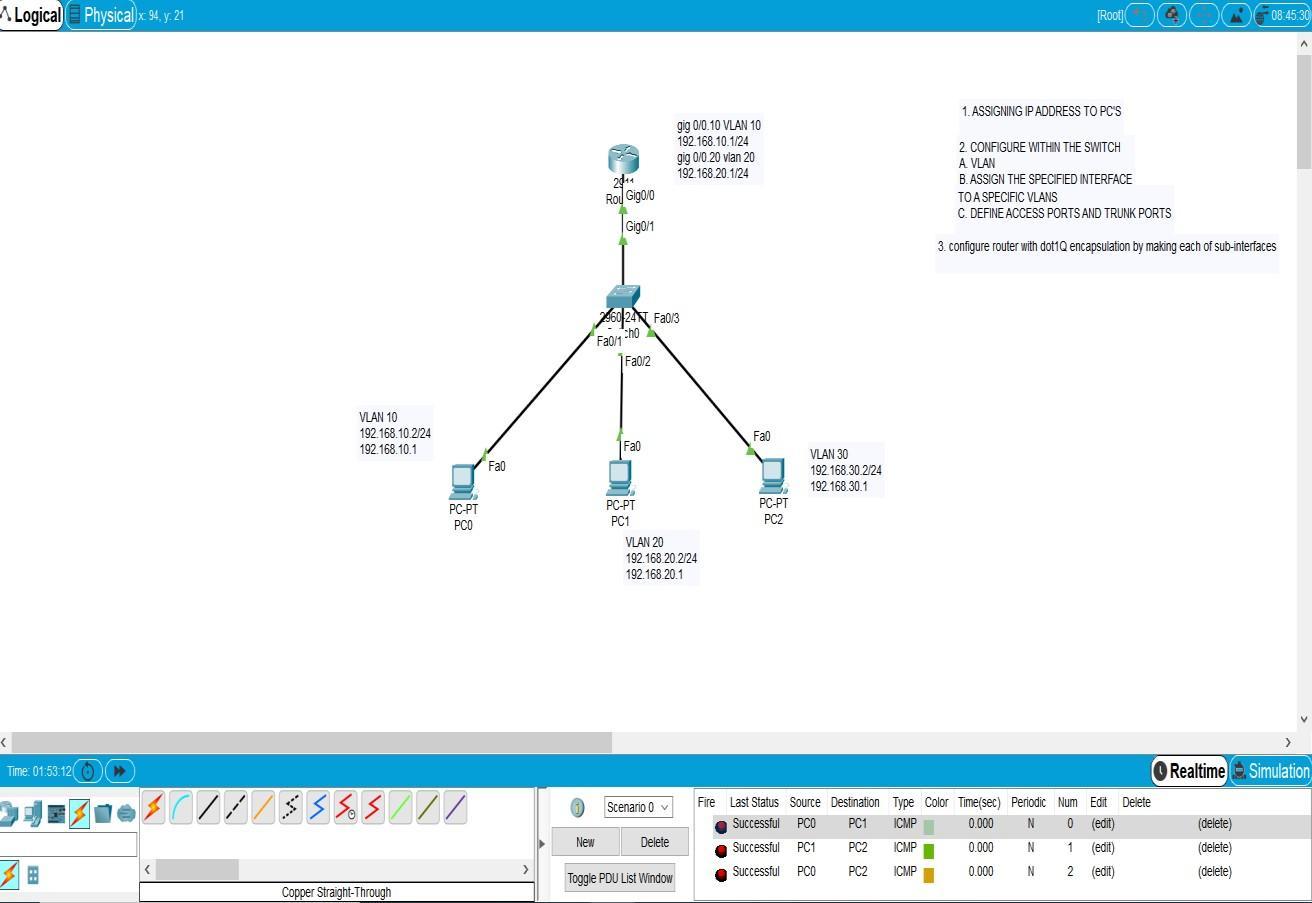
1. router(config-if)# no shutdown
2. router(config-if)# exit
3. router(config-if)# interface gigabitethernet 0/0.20
4. router(config-if)# encapsulation dot1Q 20

10. router(config-if)# ip address 192.168.20.1 255.255.255.0

1. router(config-if)# no shutdown
2. router(config-if)# exit
3. router(config-if)# interface gigabitethernet 0/0.30
4. router(config-if)# encapsulation dot1Q 30

15. router(config-if)# ip address 192.168.30.1 255.255.255.0

1. router(config-if)# no shutdown
2. router(config-if)# exit



CONCLUSION:

VLANs logically segment networks to improve performance, security, and scalability by isolating traffic and reducing broadcast domains, making network management more efficient.