Date: 15/09/2023

EXPERIMENT – 1

Aim:

Introduction to computer networks.

Q-1: What are computer networks?

Ans: Computer networks are interconnected systems of computers and other devices that facilitate the sharing of data and resources. These networks can be as small as a local area network (LAN) within a single home or office, or as vast as the global internet. They are fundamental to modern communication and data exchange.

Networks rely on a combination of hardware and software components. Devices such as computers, servers, routers, and switches are linked through various technologies like Ethernet, Wi-Fi, or cellular connections. The software, including protocols and operating systems, ensures the seamless transmission and reception of data.

Computer networks serve numerous purposes. They enable the sharing of files, printers, and internet access, making collaboration and resource utilization efficient. They also support email communication, video conferencing, and online services. The internet itself is the largest and most well-known computer network, connecting billions of devices worldwide.

Security is a crucial concern in computer networks, with measures like firewalls and encryption used to protect data from unauthorized access. The study of computer networks encompasses various fields, including network design, administration, and troubleshooting. Understanding network concepts is vital in our increasingly digital world, as it underpins the functioning of many aspects of modern life.

Q-2: What is a system?

Ans: A system is a structured, interconnected set of components or elements that work together to achieve a specific purpose or function. These components can include people, hardware, software, processes, and data. Systems are designed to process inputs, perform operations, and produce outputs, all within a defined framework.

Here's a simple table illustrating the components of a system:

Component	Description
Inputs	Data, information, or materials that enter the system.
Processes	Activities or operations that transform inputs.
Outputs	The results or products generated by the system.
Feedback	Information about the system's performance.

Q-3: What is a simulator?

Ans: A simulator is a software or hardware tool designed to mimic the behavior of a real- world system, process, or environment. Simulators are used for various purposes, including training, testing, experimentation, and analysis. They allow users to interact with a simulated version of a system without the risks or costs associated with the real thing. Simulators are commonly used in fields such as aviation, automotive engineering, and computer science.

Q-4: What is an emulator?

Ans: An emulator is similar to a simulator but typically focuses on replicating the hardware and software environment of a specific system or device, such as a gaming console, mobile phone, or computer. Emulators are often used for running software or applications designed for one platform on another, allowing compatibility between different systems. For example, an Android emulator can run Android apps on a Windows computer.

Q-5: What is the difference between continuous and discrete systems?

Ans: Continuous and discrete systems are two fundamental types of systems in the context of mathematics, engineering, and science. They differ in terms of the nature of their variables and how they evolve over time.

Here's a simple table summarizing the key differences:

Aspect	**Continuous Systems**	**Discrete Systems**
Variable Type	Continuous	Discrete
Evolution Over Time	Continuous	Discrete
Modeling Tools	Differential Equations	Recurrence Relations, Difference Equations
Examples	Fluid flow, Analog Circuits, Physical Motion	Digital Circuits, Computer Programs, Discrete-Time Signals

Q-6: What is discrete event simulation?

Ans: Discrete event simulation is a computational modeling technique used to study and analyze the dynamic behavior of complex systems, especially those involving discrete events or processes that occur at distinct points in time. In this method, a system is represented by a set of discrete events that trigger changes in the system's state. These events can represent various actions, such as the arrival of customers in a queue, the completion of a task, or the scheduling of maintenance activities.

Key characteristics of discrete event simulation include:

1. Event-driven modeling: The simulation progresses in response to specific events, which determine when and how the system's state changes.
2. Time advancement: The simulation advances from one event to the next, allowing for the modeling of asynchronous and dynamic systems.

3. Modeling complexity: It is particularly useful for systems with complex interactions, limited resources, and queuing phenomena.

Q-7: What are the various types of simulators available?

Ans: Simulators come in various types, depending on their applications and purposes. Here are some common types of simulators:

Type of Simulator	Description
Flight Simulators	Replicate aircraft flight for training and testing, used in aviation for pilot training and aircraft design.
Driving Simulators	Emulate driving conditions for training and testing, used in the automotive industry and for driver education.
Medical Simulators	Simulate medical procedures or scenarios for training and skill development among healthcare professionals.
Military Simulators	Replicate military scenarios and equipment for training and tactical planning, including flight, tank, and infantry simulators.
Gaming Simulators	Designed for entertainment, providing immersive experiences in various genres, including racing, sports, and role-playing games.
Construction Simulators	Simulate construction equipment and environments for training operators and testing construction plans.
Computer Network Simulators	Replicate computer network configurations and traffic for network design, testing, and training in IT.

Q-8: Explain at least seven networking simulators.

Ans: Here are seven popular networking simulators, along with a brief description of each:

1. **NS-2 (Network Simulator 2)**:
   - NS-2 is an open-source discrete event network simulator used for simulating both wired and wireless networks.
   - It provides a comprehensive platform for network research and protocol development.
   - NS-2 uses a script-based configuration and supports various network protocols and traffic models.
   - Widely used in academia and research to evaluate network protocols, routing algorithms, and performance.
2. **NS-3 (Network Simulator 3)**:
   - NS-3 is another open-source network simulation tool that offers a more modern and modular architecture compared to NS-2.

- It is designed for research, development, and testing of network protocols and applications.
- NS-3 is written in C++ and provides a flexible framework for creating custom network simulations.
- Used in academia and industry to study emerging networking technologies and protocols.

3. **Cisco Packet Tracer**:
   - Cisco Packet Tracer is a proprietary network simulation tool developed by Cisco Systems.
   - It is primarily used for teaching and learning about Cisco networking equipment and configurations.
   - Packet Tracer allows users to design, configure, and simulate network topologies, making it a valuable educational resource.
4. **GNS3 (Graphical Network Simulator-3)**:
   - GNS3 is an open-source network emulator that focuses on simulating complex network topologies using real or virtual devices.
   - It is commonly used for testing and developing network configurations, including Cisco and other vendor devices.
   - GNS3's graphical interface simplifies network design and allows for integration with real hardware.
5. **EVE-NG (Emulated Virtual Environment - Next Generation)**:
   - EVE-NG is a commercial network emulation platform used for designing and testing network topologies.
   - It supports both real and virtual network devices and is widely used by network professionals for certification exam preparation and lab testing.
6. **OpNet (now part of Riverbed SteelCentral)**:
   - OpNet was a commercial network simulation and performance management tool, but it has been integrated into Riverbed SteelCentral.
   - It is used for analyzing and optimizing the performance of complex networks, applications, and systems.
   - OpNet focuses on network management and performance monitoring, particularly in enterprise environments.
7. **OMNeT++**:
   - OMNeT++ is an open-source discrete event simulation framework primarily designed for modeling and simulating communication networks and distributed systems.
   - It provides a modular and extensible platform for creating custom simulations, making it popular in academia and research.
   - OMNeT++ supports a variety of protocols and communication technologies, making it versatile for network and distributed systems research.

Q-9: What is the difference between NS-2 and NS-3?

Ans: NS-2 and NS-3 are both network simulators, but they have notable differences:

Feature	**NS-2**	**NS-3**
Development	Older, mature, and less flexible.	Modern, versatile, and actively developed.
Programming Language	TCL-based scripting.	C++ with Python scripting, offering more flexibility.
Modeling Capability	Primarily wired networks.	Both wired and wireless networks, more versatile.
User-Friendliness	Less user-friendly, complex scripting.	More user-friendly, graphical interface.
Realism Performance	Limited wireless realism. Slower simulations.	Improved wireless realism and faster simulations.
Protocol Integration	Limited protocol support and integration.	Enhanced protocol support and better integration.
Licensing	GNU Public License (open-source).	GNU General Public License (open-source), offering flexibility.

Q-10: Explain in detail with all the available functionality about Packet Tracer and Wireshark.

Ans: Packet Tracer:

Description: Cisco Packet Tracer is a network simulation and visualization tool developed by Cisco Systems. It is primarily used for teaching and learning networking concepts, especially in Cisco's networking courses.

Key Features:

- **Network Topology Simulation**: Users can create, configure, and simulate network topologies, including routers, switches, PCs, and other networking devices.
- **Packet Simulation**: Packet Tracer allows users to generate and track network packets, making it a valuable tool for understanding how data flows within a network.
- **Device Configuration**: Users can configure devices using a command-line interface (CLI) similar to Cisco's real networking devices.
- **Packet Capture**: Packet Tracer provides basic packet capture and analysis capabilities, allowing users to inspect network traffic.
- **Protocols Supported**: It supports a range of network protocols, including TCP/IP, DHCP, HTTP, and more.
- **Collaboration**: Packet Tracer offers collaboration features, enabling multiple users to work on the same network project simultaneously.
- **IoT Simulation**: It includes support for simulating Internet of Things (IoT) devices and scenarios.

Use Cases:

- Education: Packet Tracer is widely used by educators and students to teach and learn networking concepts, Cisco commands, and network design.
- Network Prototyping: It can be used for quickly prototyping network configurations and testing Cisco device configurations in a safe virtual environment.
- Certification Preparation: Individuals preparing for Cisco certification exams (e.g., CCNA) often use Packet Tracer to practice hands-on networking tasks.

Wireshark:

Description: Wireshark, formerly known as Ethereal, is a powerful open-source packet analysis tool used for network troubleshooting, analysis, and protocol development.

Key Features:

- **Packet Capture**: Wireshark can capture and display packets from a network interface in real-time.
- **Protocol Analysis**: It provides detailed protocol analysis, allowing users to dissect and analyze network traffic at a granular level.
- **Filtering and Searching**: Users can apply filters and search for specific packets or packet attributes, making it easy to isolate and examine relevant data.
- **Packet Decoding**: Wireshark can decode various network protocols, making it an invaluable tool for diagnosing network issues.
- **Statistics**: It offers statistics and summary information about captured packets, such as protocol distribution and bandwidth usage.
- **Export and Save**: Users can save captured packets in various file formats or export them for further analysis.
- **Scripting and Automation**: Wireshark supports scripting and automation through tools like TShark and Lua.
- **Cross-Platform**: Available on multiple operating systems, including Windows, macOS, and Linux.

Use Cases:

- Network Troubleshooting: Wireshark is commonly used by network administrators and engineers to diagnose network problems and identify the root causes of issues.
- Security Analysis: It can be used to detect and investigate network security incidents, such as malware infections and suspicious network traffic.
- Protocol Development: Wireshark is essential for developers working on new network protocols or troubleshooting existing ones.
- Educational and Training: It is used in networking courses and security training programs to teach students about network analysis and forensics.
- Both Packet Tracer and Wireshark serve important roles in networking, with Packet Tracer focusing on network simulation and learning, while Wireshark excels in packet analysis and troubleshooting.

Date: 22/09/2023

EXPERIMENT-2

Aim:

Installation of Cisco Packet Tracer.

Theory:

Cisco Packet Tracer is a network simulation and visualization tool developed by Cisco Systems. It is primarily used for teaching and learning networking concepts, allowing users to create virtual network environments and simulate network behaviour.

Packet Tracer provides a graphical interface that enables users to design, configure, and troubleshoot networks without needing physical hardware. Key features of the Cisco Packet Tracer include:

1. Network topology creation: Users can create network topologies by dragging and dropping devices such as routers, switches, PCs, servers, and more onto a virtual workspace.

2. Device configuration: Users can configure the devices in the network, including setting IP addresses, enabling routing protocols, configuring security features, and implementing advanced network configurations.

3. Network simulation: Packet Tracer simulates network behaviors and allows users to observe the flow of data packets, inspect network traffic, and analyze network performance.

4. Protocols and technologies: Packet Tracer supports a wide range of networking protocols and technologies, including Ethernet, TCP/IP, routing protocols (e.g., OSPF, EIGRP), switching protocols (e.g., VLANs, STP), wireless networking, and security features (e.g., firewalls, VPNs).

5. Collaboration and learning: Packet Tracer offers collaborative features that enable users to work together on network projects and share their work. It is widely used in educational institutions to teach networking concepts and facilitate hands-on learning experiences.

6. Assessment and evaluation: Packet Tracer includes built-in assessment tools that allow instructors to create and distribute activities, quizzes, and exams to evaluate students' understanding of networking concepts and ability to configure and troubleshoot networks.

7. Multi-platform support: Cisco Packet Tracer is available for Windows, macOS, and Linux operating systems, making it accessible to many users.

Packet Tracer is widely used by networking students, instructors, and professionals to gain practical experience in designing, configuring, and troubleshooting network environments. It helps users develop their networking skills in a virtual, risk-free environment before working with physical network equipment.

Installing Packet Tracer on Windows:

We have to follow some steps:

1: Visit the official website of Netacad using any web browser.

2: Press the login button and select log In option.

3: Next screen will appear, click on the sign-up option.

4: Next screen will appear and will ask for email and password and other simple details, fill them and click on Register

5: Now the login screen appears again so fill in the Email id.

6: On the next screen enter the password and press the Login button.

7: Dashboard will initialize, now click on Resources and choose Download Packet Tracer Option.

8: On the next web page choose the operating system to download the packet tracer. Downloading will start automatically.

9: Check for the executable file in your system and run it. Next screen is of License Agreement so Click on I accept the license. Choose the installing location which has sufficient space.

10: Now packet tracer is ready to install so click on the Install button. Click on the Finish button to complete the installation

Date: 22/09/2023

EXPERIMENT-3

Aim:

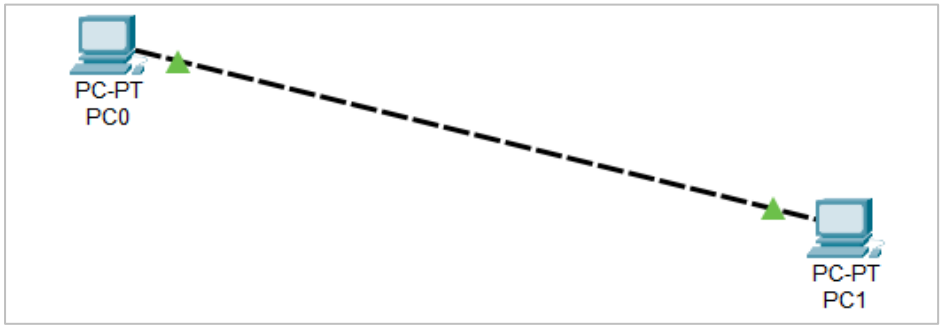
To implement the static routing using the Cisco packet trace.

Theory:

Static routing in Cisco Packet Tracer is a fundamental networking concept where network administrators manually configure the routing table of a router, specifying the next hop or exit interface for each destination network. This approach is suitable for smaller networks with relatively simple topologies, where routing decisions remain constant or change infrequently. Administrators define static routes by specifying the destination network and the associated next-hop router's IP address or directly connected interface.

Static routing offers simplicity and predictability, making it easier to troubleshoot and maintain, as it doesn't involve the complexities of dynamic routing protocols like OSPF or EIGRP. However, it is less adaptive to network changes, making it less suitable for large and dynamic networks. In Cisco Packet Tracer, network professionals can practice and experiment with static routing configurations, gaining a hands-on understanding of routing principles and helping them become proficient in managing network traffic efficiently within a controlled environment.

Snapshots of Cisco Packet Tracer:



Output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time=4ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time=4ms TTL=128

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 2ms
```

Date: 22/09/2023

EXPERIMENT-4

Aim:

To implement inter LAN communication using the Cisco packet tracer.

Theory:

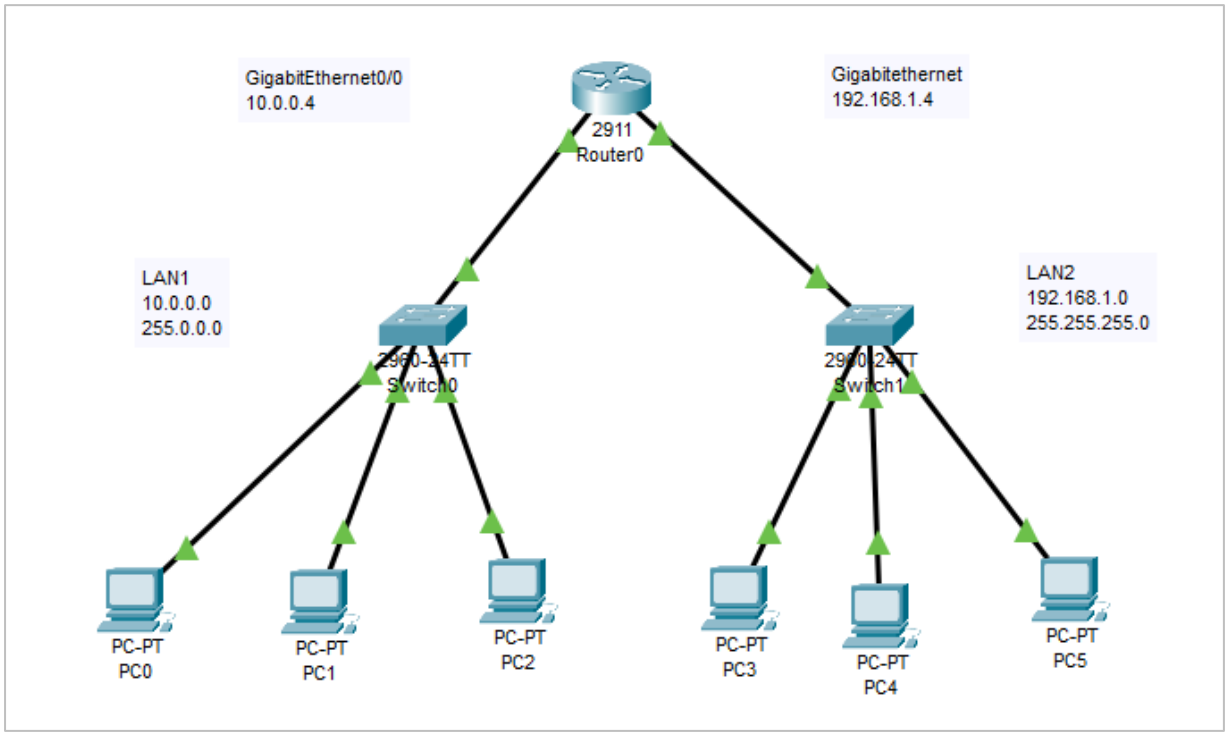
Inter-LAN communication, short for "Inter-Local Area Network communication," refers to the exchange of data and information between different local area networks (LANs). A LAN is a network of computers and devices that are interconnected within a limited geographic area, such as a home, office, or campus. Inter-LAN communication allows these separate LANs to communicate and share resources with each other, enabling data transfer and collaboration across different network segments. Inter-LAN communication is crucial for organizations with multiple office locations or complex network setups. It allows for the efficient sharing of resources, data, and services while ensuring security and control over the traffic between LANs.

Procedure:

1. Open Cisco Packet Tracer and create a new project.
2. Drag and drop 2 switches (type: 2960).
3. Connect 3 PCs to each of the switches.
4. Configure IP addresses of PCs connected to first switch (10.0.0.1, 10.0.0.2 and 10.0.0.3) and PCs connected to second switch (192.168.1.1, 192.168.1.2 and 192.168.1.3).
5. Take a router and connect the two switches to it through GigabitEthernet0/0 and GigabitEthernet0/1 ports of the router.
6. Configure IP addresses of the ports as 10.0.0.4 and 192.168.1.4 respectively.
7. Now, open the command prompt of any one PC of LAN1 and ping the IP address of any PC of LAN2 to check the connection.

Date: 22/09/2023

Visual Representation of Inter LAN Communication:



Output:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

EXPERIMENT-5

Aim:

To implement the DHCP using the Cisco packet tracer

Theory:

Dynamic Host Configuration Protocol (DHCP) is a networking protocol used to automatically assign IP addresses and related configuration information to devices on a network. In Cisco Packet Tracer, DHCP plays a crucial role in simplifying the management of IP addresses and other network parameters. This protocol enables network administrators to automate the IP address allocation process, making it efficient and scalable for both small and large networks.

DHCP eliminates the need for manually configuring IP addresses on each device by centralizing the administration of IP leases. When a device, such as a computer or smartphone, connects to the network, it sends a DHCP request. A DHCP server, typically a router or dedicated server, responds with an available IP address and other network settings, including subnet mask, gateway, DNS servers, and lease duration.

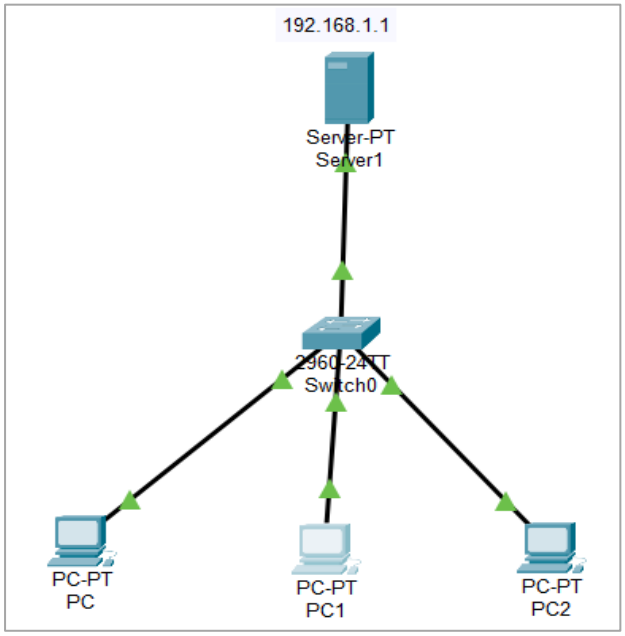
Cisco Packet Tracer allows users to simulate the deployment of DHCP servers and clients, offering a practical platform for understanding and configuring DHCP settings within a controlled network environment. By using Packet Tracer, network administrators and students can experiment with different DHCP configurations, such as setting address pools, lease times, and reservation of specific IP addresses for devices, thereby gaining a deep understanding of how DHCP streamlines IP management, enhances network efficiency, and simplifies the provisioning and maintenance of IP configurations in real-world networking scenarios.

Procedure:

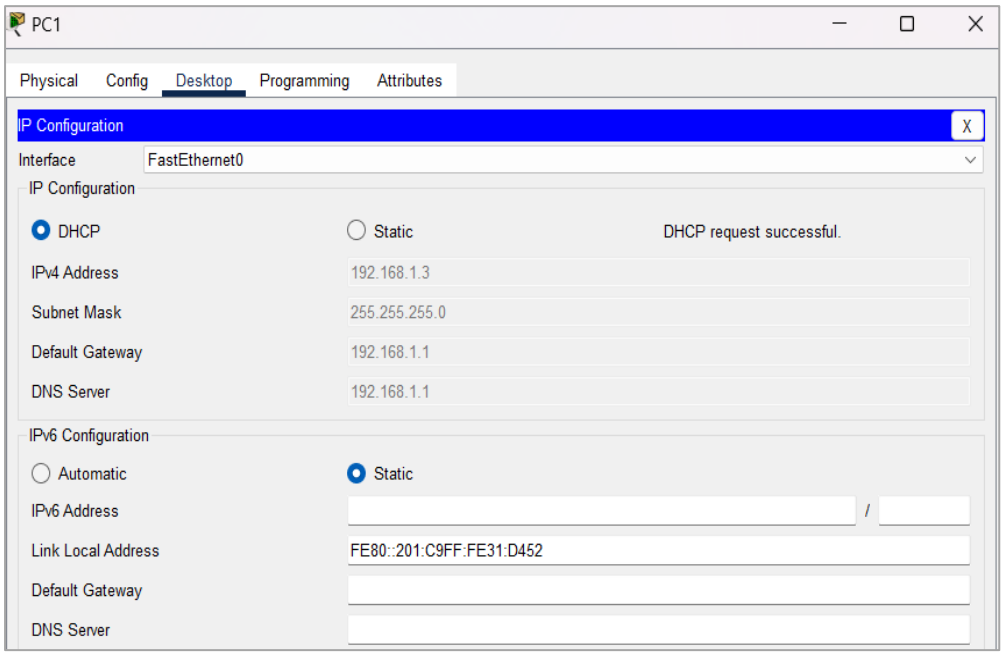
1. Open Cisco Packet Tracer and create a new project.
2. Drag and drop three “PCs” from and one Server from “End Devices”
3. Drag and drop the “2960” Switch from “Switches” and place it in between the server and the three PCs.
4. Now connect the server and the PCs to the switch using the “Copper Straight Through” wire.
5. Double-click on the Server and go to “Desktop”.
6. Now in the “IP Configuration”, click on static and put it in the IPv4 address as 192.168.1.1 and click on the subnet mask(255.255.255.0)
7. Now go to the “Services” section in the Server and click on DHCP.
8. Now turn on the service by pressing the toggle button

9. Put the “Default Gateway”, “DNS Server”, “Start Address” and “Subnet Mask” as 192.168.1.1, 192.168.1.1, 192.168.1.2, and 255.255.255.0 respectively
10. Click on save.
11. Now click on PC0, go to “IP Configuration” in the “Desktop” Section and click on DHCP.
12. You shall see the message “DHCP Request Successfully”
13. Do the same for the remaining two PCs.

Visual Representation of DHCP:



DHCP Configuration:



Date: 06/10/2023

EXPERIMENT-6

Aim:

To implement DNS using the Cisco packet tracer

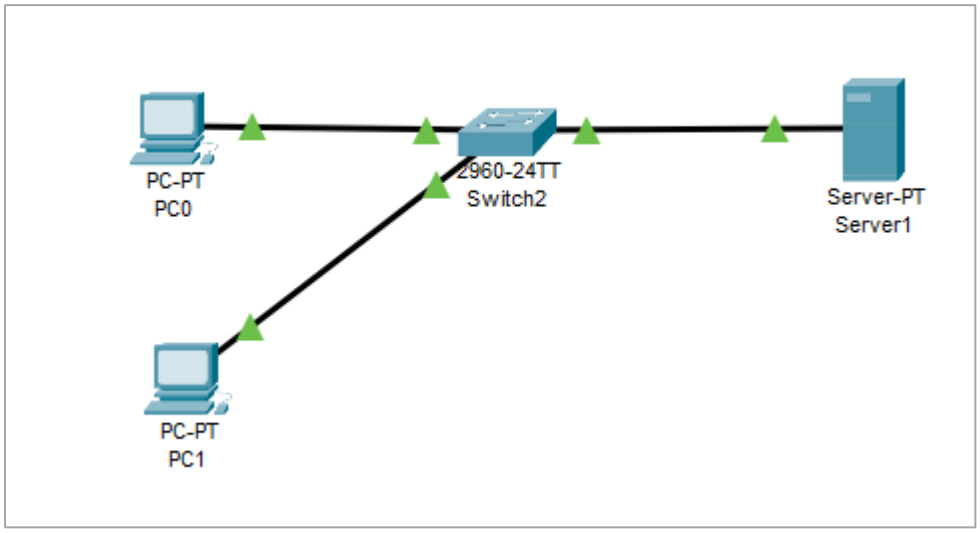
Theory:

DNS, which stands for Domain Name System, is a fundamental component of the internet and a system used to translate human-readable domain names into IP addresses. This translation is essential for the functioning of the internet because computers and network devices communicate with each other using IP addresses, which are numerical representations (e.g., 192.168.1.1) of the locations of servers, websites, and other resources on the internet. DNS helps users access websites and other resources using user-friendly domain names (e.g., www.example.com) rather than having to remember the corresponding IP addresses. DNS is a distributed and hierarchical system that ensures the efficiency, scalability, and reliability of internet communication. It plays a critical role in helping users easily access websites and services by using human-friendly domain names rather than having to remember complex numerical IP addresses.

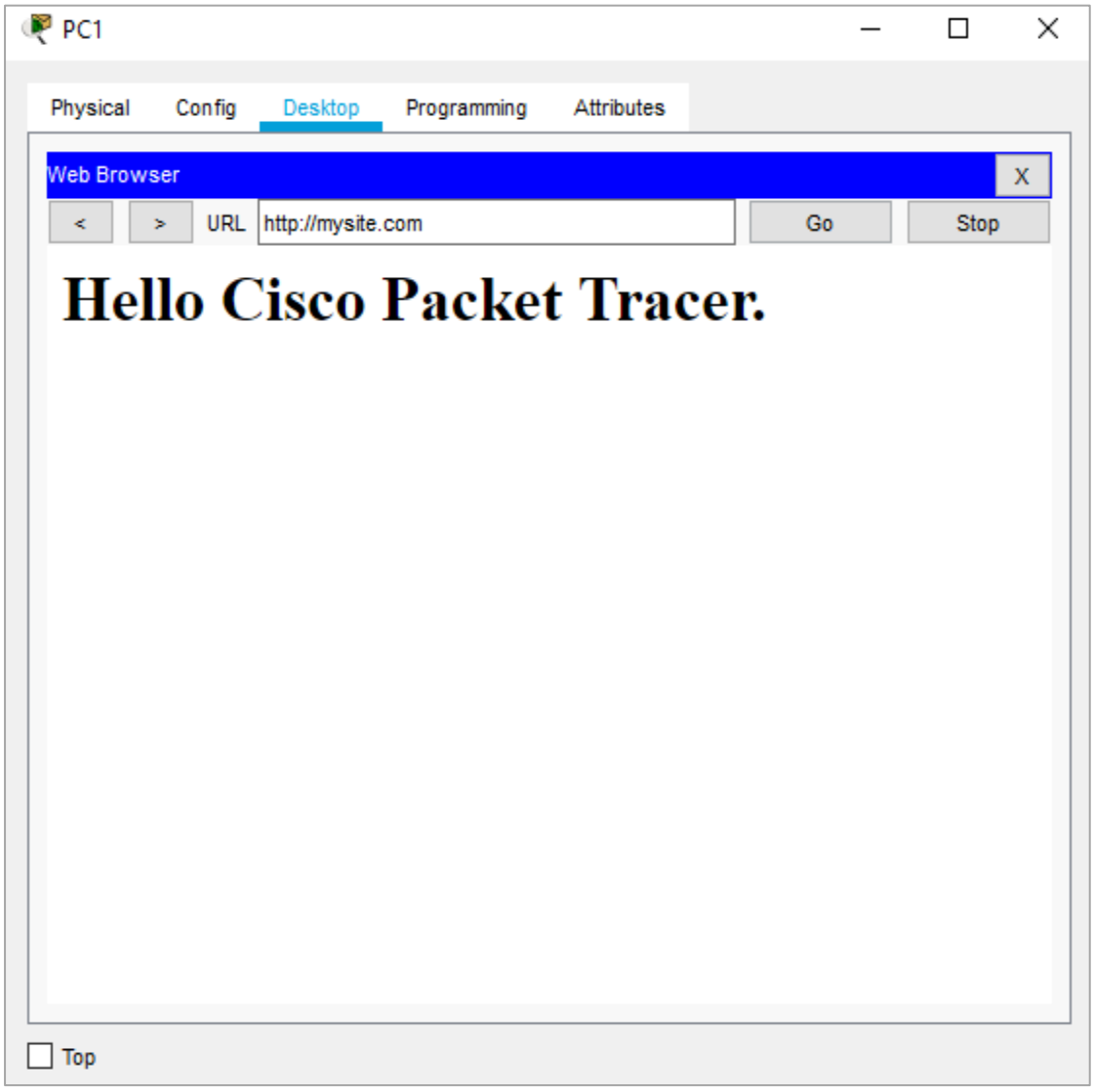
Procedure:

1. Open Cisco Packet Tracer and create a new project.
2. Drag and drop two "PC" devices from the "End Devices" section onto the workspace.
3. Drag and drop a switch (type: 2960) and connect the PCs to it by straight-through wires.
4. Drag and drop a server and connect it to switch.
5. Configure the IP address of the server (192.168.1.1).
6. Configure the IP addresses of the PCs (192.168.1.2 and 192.168.1.3).
7. Go to IPconfig section in desktop of server and set the DNS address to same as its IP address.
8. Then go to HTTP section inside services section and make a web page (index.html).
9. Go to DNS section below HTTP section, switch it ON and give a name to your webpage and add it.
10. Go to desktop of your PC and inside IPconfig set the DNS (192.168.1.1).
11. Then go to Web Browser section of the desktop section of PC.
12. Type the name of the web page or the DNS IP address to view your web page.

Visual Representation of DNS:



Output:



Date: 20/10/2023

EXPERIMENT-7

Aim:

To implement Email services using Cisco Packet Tracer.

Theory:

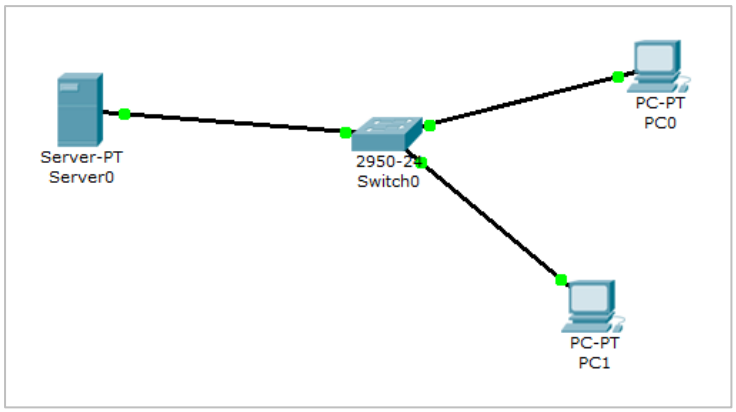
Electronic mail is one of the most well-known network services. Electronic mail is a computer-based service that allows users to communicate with one another by exchanging messages. Email information is transmitted via email servers and uses a variety of TCP/IP protocols. For example, the simple mail transfer protocol (SMTP) is a protocol that is used to send messages. Similarly, IMAP or POP receives messages from a mail server.

Procedure:

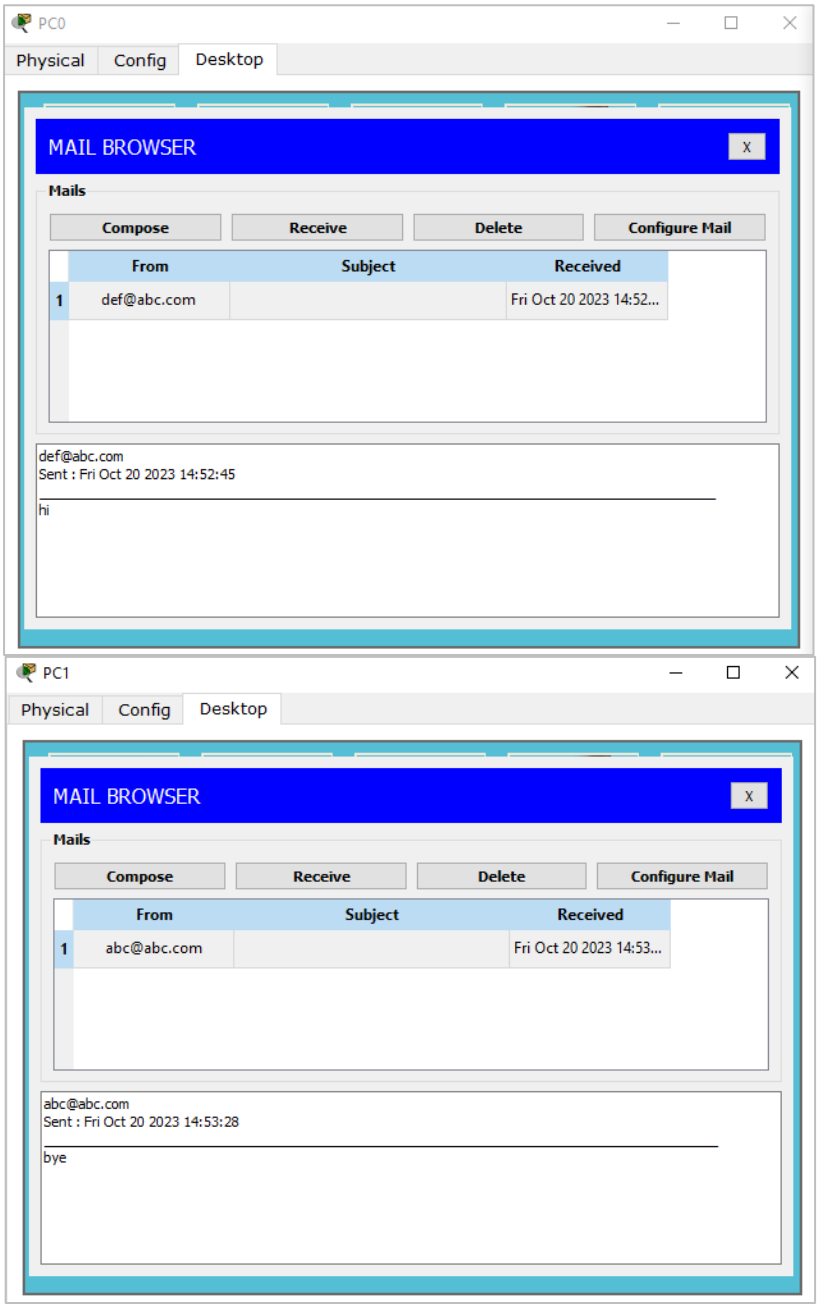
1. Open Cisco Packet Tracer and create a new project.
2. Drag and drop two "PC" devices from the "End Devices" section onto the workspace.
3. Drag and drop a switch (type: 2950T) and connect the PCs to it by straight-through wires.
4. Drag and drop a server and connect it to switch.
5. Configure the IP address of the server (192.168.1.1).
6. Configure the IP addresses of the PCs (192.168.1.2 and 192.168.1.3).
7. Set the default gateway and DNS to (192.168.1.1).
8. Go to IPconfig section in desktop of server and set the Default Gateway address to same as its IP address.
9. Then go to Email section inside services section and make a domain name (gmail.com).
10. Switch on the SMTP service and add 2 users
11. After entering a username and password, click on Add(+) to add the user to the server. (pc0@gmail.com and pc1@gmail.com).
12. Go to PC0 email client, compose an email and send its to PC1 email address (pc1@gmail.com)
13. to see whether the email from PC0 is received on PC1. On the email client of PC1, click on Receive.

Date: 20/10/2023

Snapshots of Cisco Packet Tracer:



Mail Browser Snapshots:



EXPERIMENT-8

Aim:

Create Bus, Star, Mesh, and hybrid topology using Cisco Packet Tracer.

Theory:

Network topology refers to the arrangement of nodes and the connections between them in a computer network. Four common topologies are Bus, Star, Mesh, and Hybrid.

The Bus Topology is a linear arrangement where all devices share a common communication medium. Devices transmit data along the bus, and all nodes receive the data, but only the intended recipient processes it.

In the Star Topology, all devices are connected to a central hub or switch. The hub acts as a repeater, amplifying and forwarding signals to the connected devices. This structure enhances reliability and simplifies troubleshooting but relies heavily on the central hub.

Mesh Topology involves each device being connected to every other device in the network. This redundancy ensures multiple paths for data transmission, improving fault tolerance and reliability. However, it requires more cabling and is complex to implement.

Hybrid Topology is a combination of two or more different topologies. For example, a network might integrate elements of both Star and Mesh. This approach provides a balance between redundancy and simplicity, allowing for customization based on specific needs, optimizing performance, and addressing potential drawbacks of individual topologies.

Procedure:

To create different network topologies using Cisco Packet Tracer, follow these steps:

Bus Topology

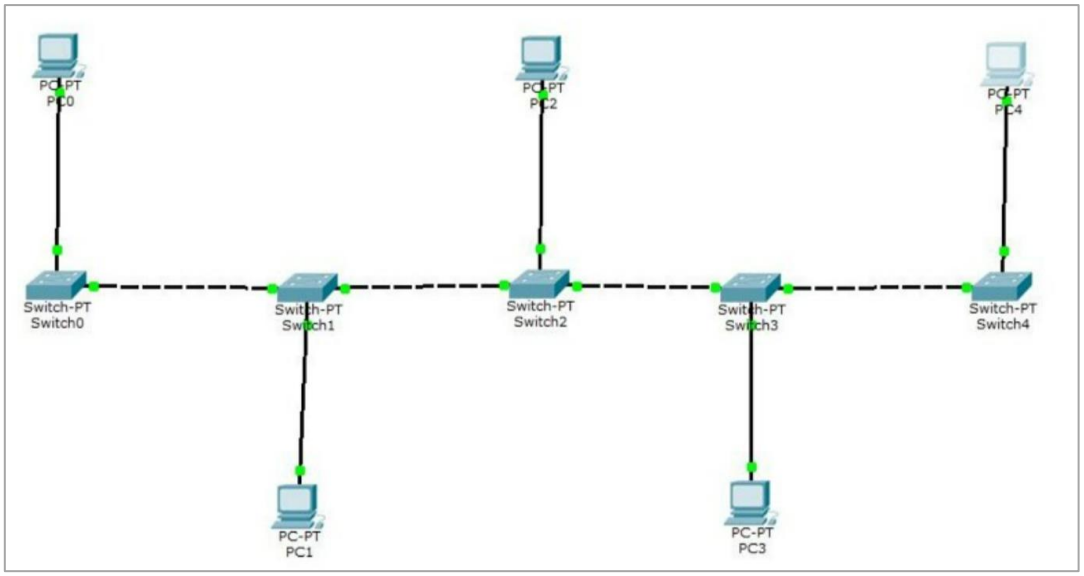
1. Open Cisco Packet Tracer and create a new project.

2. Drag and drop a "Switch" device from the "End Devices" section onto the workspace.

3. Connect multiple PCs to the Hub by dragging and dropping them onto the workspace and then connecting them to the Hub using Ethernet cables.

4. Arrange the PCs and Hub in a linear fashion to represent the bus topology.

5. Configure IP addresses and other necessary settings for each PC if required.



Star Topology

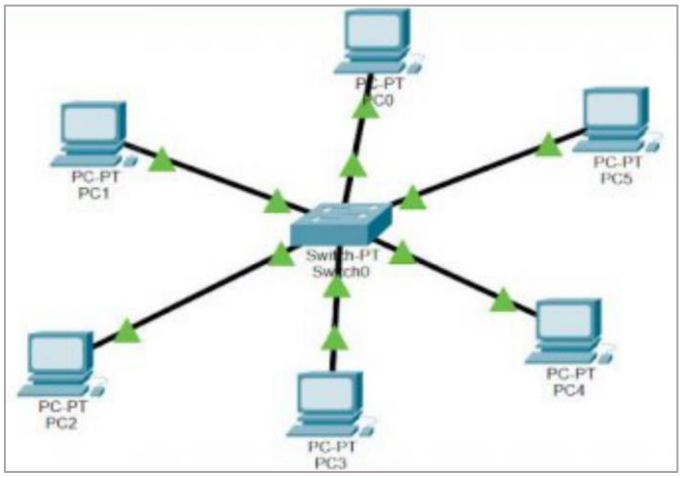
1. Create a new project in Cisco Packet Tracer.

2. Drag and drop a "Switch" device from the "Switches" section onto the workspace.

3. Connect multiple PCs to the Switch by dragging and dropping them onto the workspace and then connecting them to the Switch using Ethernet cables.

4. Arrange the PCs around the Switch in a star-like pattern, with each PC connected directly to the Switch.

5. Configure IP addresses and other necessary settings for each PC if required.



Mesh Topology

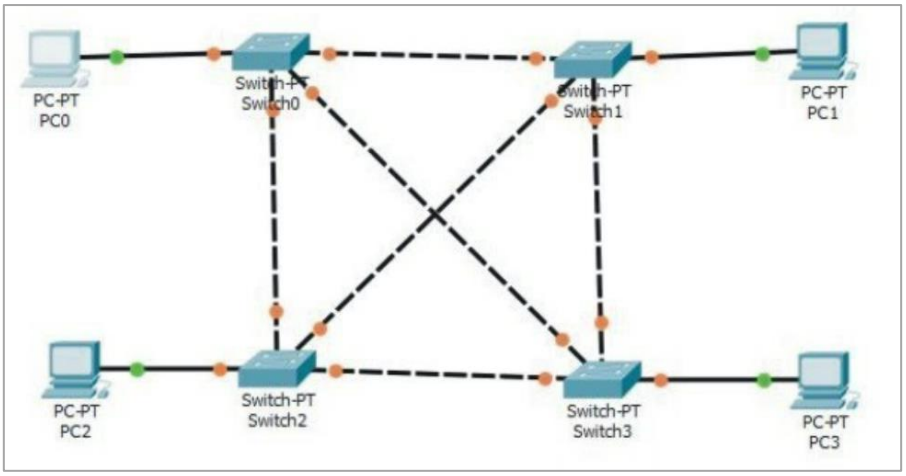
1. Begin a new project in Cisco Packet Tracer.

2. Drag and drop multiple "Switch" devices onto the workspace.

3. Connect the Switches to each other using Ethernet cables to create a fully connected mesh.

4. Drag and drop PCs onto the workspace and connect them to the Switches as required.

5. IF REQUIRED, Configure IP addresses and other necessary settings for each PC and Switch.



Hybrid Topology

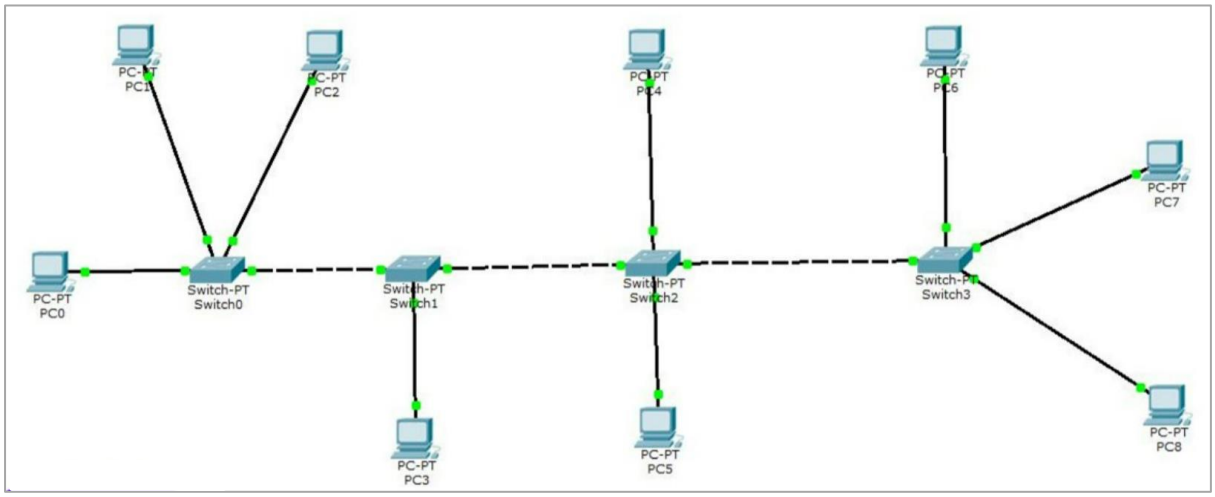
1. Open Cisco Packet Tracer and create a new project.

2. Combine elements from different topologies to create a hybrid topology that suits your requirements.

For example, you can connect multiple Switches in a mesh configuration, and then click a few PCs to one Switch to form a star topology.

3. Drag and drop the required devices onto the workspace and connect them using the appropriate cables.

4. Configure IP addresses and other necessary settings for each device as required.



EXPERIMENT-9

Aim:

To implement the Network Address Resolution (NAT) using Cisco Packet Tracer.

Theory:

Network Address Resolution (NAT) is a crucial networking concept designed to address the scarcity of IPv4 addresses. Acting as a mediator between a private network and the public internet, NAT translates private IP addresses to a single public IP. This process allows multiple devices within a local network to share a common outward-facing address, enhancing security and conserving IP resources. NAT operates at the network layer, transparently altering packet headers during transmission. It facilitates smoother communication by concealing internal addresses from external networks. While effective for conserving IPv4 addresses, NAT can pose challenges for certain applications, leading to the adoption of IPv6 as a long-term solution.

Types of NAT:

Static NAT: Maps a private IP address to a specific public IP address.
Dynamic NAT: Maps private IP addresses to a pool of public IP addresses.
PAT (Port Address Translation): Maps multiple private IP addresses to a single public IP address using different port.

Components involved:

Inside Local Address: Private IP addresses used within the internal network.
Inside Global Address: Public IP address visible to the external network.
Outside Local Address: IP address as seen from the external network (typically a public IP).
Outside Global Address: IP address assigned to the device in the external network

Procedure:

1. Open Cisco Packet Tracer and create a network topology with at least two routers and two networks (one internal private network and one external public network).

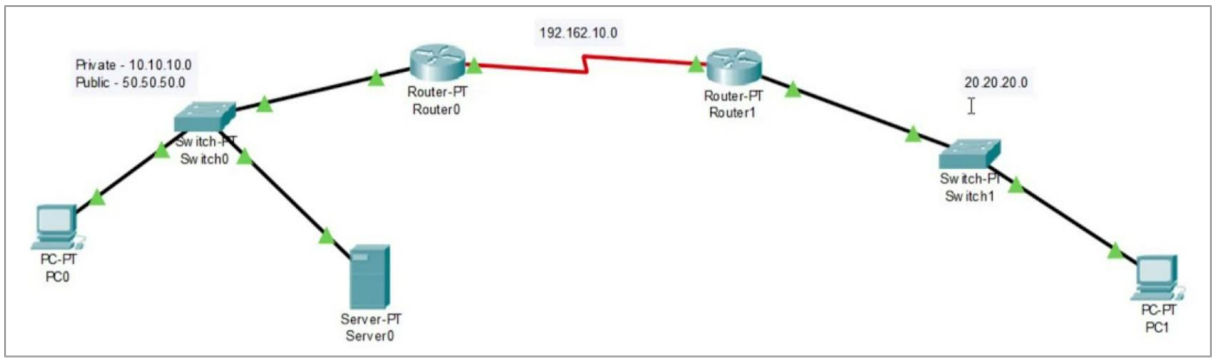
2. Connect the routers and networks appropriately using copper straight through cables.

3. Assign IP addresses to the devices in your network. Make sure to use private IP addresses for the internal network and a public IP address for the external network.

4. Access the CLI (Command Line Interface) of each router by clicking on it and selecting the "CLI" tab.

5. Test connectivity from devices on the internal network to external resources. Ensure that devices on the internal network can access the internet.

Snapshot of Topology:



IP Configurations:

PC-0	PC-1	Server-0
IP Address: 10.10.10.2 Gate Way: 10.10.10.1	IP Address: 20.20.20.2 Gate Way: 20.20.20.1	IP Address: 10.10.10.3 Gate Way: 10.10.10.1

Router-0	Router-1
IP Addresses: FastEthernet 0/0: 10.10.10.1 Serial 2/0: 192.162.10.1	IP Addresses: FastEthernet 0/0: 20.20.20.1 Serial 2/0: 192.162.10.2

Output: